Auftrag für die *Corporate*World Mastercard (Kreditkarte).

BW BANK
Ein Unternehmen der LBBW-Gruppe

corporate WORLD

Ich möchte gerne die Vorteile einer *Corporate*World Mastercard (Kreditkarte) nutzen! (Gewünschte Karte bitte ankreuzen!)

☐ Classic* ☐ Premium*

* Der Jahrespreis für die gewünschte Karte wird zu Beginn des jeweiligen Kreditkartenjahres Ihrem Kreditkartenkonto belastet und vom Girokonto der nebenstehend genannten Bankverbindung eingezogen. Von diesem Jahrespreis abweichende Konditionen können sich aufgrund eines Rahmenvertrages zwischen der BW-Bank und dem Arbeitgeber ergeben. Der Arbeitgeber teilt diese Sonderkonditionen im Namen der BW-Bank dem Karteninhaber vor oder bei Vertragsabschluss mit.

Bitte füllen Sie diesen Auftrag komplett aus.
Wenn Sie noch Fragen zur *Corporate*World Mastercard (Kreditkarte) haben, rufen Sie uns einfach an: Telefon 0711 124-45858.

Rahmenvereinbarungsnummer ☐☐☐☐☐

Baden-Württembergische Bank
Kleiner Schlossplatz 11
70173 Stuttgart
Gläubiger-Identifikationsnummer: DE39ATS00000000043

So soll mein Name auf der Karte erscheinen:
(max. 19 Stellen einschließlich Zwischenräume)

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
(Vorname, Name)

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
(z. B. Firmenname)

Persönliche Angaben des Kartenantragstellers

☐ Frau ☐ Herr

Name

Vorname | weitere Vornamen | Geburtsdatum

Geburtsort | Geburtsland

Familienstand | Anzahl Kinder | ☐ keine 2. Staatsang.

Staatsangehörigkeit | 2. Staatsangehörigkeit

Steuer-Identifikationsnummer (11-stellig) | ☐ Miete ☐ Eigentum

Straße, Hausnummer

PLZ, Ort

Telefon privat | Telefon geschäftlich

Wohnhaft seit

Wenn dort noch keine 3 Jahre wohnhaft, hier bitte auch frühere Anschrift angeben

Besitzen Sie eine Bankkundenkarte? ☐ Ja ☐ Nein
Besitzen Sie andere Kreditkarten? Wenn ja, welche? _____ ☐ Nein

Berufliche Angaben

Beruf / Position | beschäftigt seit

Firma / Branche

Straße, Hausnummer

PLZ, Ort

E-Mail

Monatseinkommen netto
☐ unter 1.250 EUR, bitte genauen Betrag angeben: _____
☐ über 1.250 EUR ☐ über 2.000 EUR ☐ über 2.500 EUR ☐ über 3.500 EUR

Bankverbindung/SEPA-Basis-Lastschriftmandat

Der Rechnungsausgleich soll erfolgen von: ☐ **Privatkonto** ☐ **Firmenkonto**

IBAN

Name der Bank | BIC

Kontoinhaber | Bankverbindung seit

Ich/Wir ermächtige(n) den oben genannten Zahlungsempfänger, wiederkehrende Zahlungen von meinem/unserem Konto mittels SEPA-Basis-Lastschrift einzuziehen.
Zugleich weise(n) ich/wir mein/unser Kreditinstitut an, die von oben genanntem Zahlungsempfänger auf mein/unser Konto gezogene(n) Lastschrift(en) einzulösen.
Hinweis: Ich kann/Wir können innerhalb von 8 Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem/unserem Kreditinstitut vereinbarten Bedingungen. Die Kartenabrechnung mit der Prenotification wird dem Karteninhaber mindestens 4 Geschäftstage vor Vornahme der Belastungsbuchung zugehen. Handelt es sich bei der hier angegebenen Bankverbindung um ein Girokonto der BW-Bank, werden die im Zusammen-hang mit der hier genannten Kreditkarte geschuldeten Zahlungen im Wege interner Umbuchungen durch die BW-Bank eingezogen (bankinterne Umbuchung). Die Erteilung eines SEPA-Mandats ist vorliegend nicht notwendig, es erfolgt auch keine Prenotification.

Rechnung Online/Elektronisches Postfach

Ich erhalte bequem und kostenfrei den Saldo, die Umsätze und alle rechtsverbindlichen Mitteilungen der Bank zu meinem Kreditkartenvertrag, insbesondere die monatliche Umsatzabrechnung sowie Änderungsmitteilungen zu den Kreditkartenbedingungen oder zum Preis- und Leistungsverzeichnis, ausschließlich über das mir bereitgestellte elektronische Postfach im Kartenservice Online. Es gelten die beigefügten Bedingungen für BW Kartenservice Online und die Bedingungen für die Nutzung des Elektronischen Postfachs im BW Kartenservice Online. Bitte senden Sie mir die Anmeldedaten zu. Ausnahme: Karteninhaber mit Firmenkontoabrechnung erhalten Ihre Rechnung per Post an die Firmenanschrift.

Wunsch-PIN

Sie wählen die Karten-PIN für Bargeldauszahlungen und Zahlungen im Handel frei aus (Wunsch-PIN). Diese erste Wunsch-PIN ist für Sie kostenlos.

Bitte beachten Sie, dass nach Zusendung des Briefes für die Einrichtung der Wunsch-PIN die darin enthaltene Transaktionsnummer zeitlich begrenzt ist.

Die Kreditkarte kann auch für Internetzahlungen genutzt werden. Das Limit für Internetzahlungen entspricht dabei dem allgemeinen Verfügungsrahmen Ihrer Kreditkarte. Bei Bedarf kann die Internetbezahlfunktionalität deaktiviert werden. Bitte wenden Sie sich dazu an den Kartenservice.

Für den Kreditkartenvertrag gelten die Bedingungen für die Nutzung des BW-Secure-Verfahrens (BW-Secure-App mit 3D-Secure-Verfahren), die Bedingungen für die *Corporate*World Mastercard (Kreditkarte), die Bedingungen für die digitale Mastercard (Kreditkarte) mit individualisierten Authentifizierungsverfahren sowie das Preis- und Leistungsverzeichnis der *Corporate*World Mastercard (Kreditkarte). Diese in Textform beigefügten Dokumente habe ich zustimmend zur Kenntnis genommen. Ich handle auf eigene Rechnung. Das Kreditkartenkonto wird nicht im Auftrag eines anderen eröffnet. Die ausführlichen Versicherungsbedingungen erhalte ich auf Wunsch im Voraus. Mir ist bekannt, dass ich die Classic-Karte (Kreditkarte) auch ohne Versicherungsschutz erhalten kann. Ich ermächtige die Baden-Württembergische Bank, die für die Ausstellung und Benutzung der Karte erforderlichen banküblichen Auskünfte bei meiner genannten Bank oder Kreditkartengesellschaft, die ich zur Auskunftserteilung an die BW-Bank ermächtige, einzuholen. Die Kreditkarte wird mir per Post an meine Privatanschrift bzw. Firmenanschrift zugesandt.

Hinweise zur Datenübermittlung

Hinweis zur Übermittlung und Verarbeitung von personenbezogenen Daten in die USA und in Länder, in denen das Datenschutzniveau nicht demjenigen in der Bundesrepublik Deutschland entspricht:
Die Mastercard ist ein Produkt der Mastercard International Incorporated, 2000 Purchase Street, New York 10577-2509 in den USA. Es kann daher nicht ausgeschlossen werden, dass personenbezogene Daten des Karteninhabers (Name, Vorname, Kartennummer, Kartenlaufzeit, Daten zum Karteneinsatz) zur Abwicklung von Kartenzahlungsvorgängen an diese oder deren Dienstleister in die USA übermittelt und dort verarbeitet werden. Dieses kann auch beim Karteneinsatz in der Bundesrepublik Deutschland nicht ausgeschlossen werden. Darüber hinaus ist – je nachdem, in welchem Land und gegenüber wem die Karte eingesetzt wird und wie der jeweilige Vertragspartner Kartenzahlungen abwickelt, nicht ausgeschlossen, dass die genannten personenbezogenen Daten zur Abwicklung von Kartenzahlungen auch in andere Länder, deren Datenschutzniveau nicht demjenigen in der Bundesrepublik entspricht, übermittelt und dort verarbeitet werden. Die BW-Bank hat hierauf keinen Einfluss.

Versicherungsleistungen *Corporate*World Mastercard (Kreditkarte):
Sofern Versicherungsleistungen in Anspruch genommen werden, werden sämtliche für die Schadensabwicklung erforderlichen Daten an die Europäische Reiseversicherungs AG, Vogelweidestraße 5, 81677 München, und die D. A. S. Allgemeine Rechtschutz-Versicherungs-AG, Thomas-Dehler-Straße 2, 81728 München, übermittelt und durch diese gespeichert und verarbeitet.

Einwilligungen in die Einholung von Bankauskünften
Einwilligung in die Datenübermittlung zum Zwecke der Bonitätsprüfung:
Ich/Wir willige(n) ein, dass die BW-Bank die für die Ausstellung und Benutzung der Karte erforderlichen banküblichen Auskünfte bei meiner/unserer Bank oder Kreditkartengesellschaft, die ich zur Auskunftserteilung an die BW-Bank ermächtige, einholen wird.

Einwilligungen in die Übermittlung personenbezogener Daten
Einwilligung in die Übermittlung personenbezogener Daten zu Zwecken der Teilnahme am Managementinformationssystem CorporateWorld DataOnline in die USA:
Ich willige ein, dass meine personenbezogenen Daten im Zusammenhang mit der Verwendung der *Corporate*World Mastercard (Kreditkarte), insbesondere Kartenumsätze einschließlich Zeit und Ort der Verwendung und des Kartenakzeptanten, Mahnungen, Personalnummer und Kartennummer durch die Mastercard International Incorporated, 2000 Purchase Street, Purchase, New York in den USA zu Zwecken der Erstellung von Managementinformationen in *Corporate*World *Data*Online gespeichert und verarbeitet werden und an meinen Arbeitgeber übermittelt sowie von diesem ebenfalls gespeichert und verarbeitet werden. Ein Widerruf berührt die Rechtmäßigkeit der auf Grund der Einwilligung bis zur Erklärung des Widerrufs erfolgten Verarbeitung nicht. Er führt dazu, dass von mir keine personenbezogenen Daten in das von Mastercard betriebene Managementinformationssystem eingegeben werden dürfen.

Datenübermittlung an infoscore Consumer Data GmbH
Wir übermitteln Ihre Daten (Name, Adresse und ggf. Geburtsdatum) zum Zweck der Bonitätsprüfung, dem Bezug von Informationen zur Beurteilung des Zahlungsausfallrisikos auf Basis mathematisch-statistischer Verfahren unter Verwendung von Anschriftendaten sowie zur Verifizierung Ihrer Adresse (Prüfung auf Zustellbarkeit) an die infoscore Consumer Data GmbH, Rheinstraße 99, 76532 Baden-Baden.
Rechtsgrundlagen dieser Übermittlungen sind Artikel 6 Absatz 1 Buchstabe b und Artikel 6 Absatz 1 Buchstabe f der DSGVO. Übermittlungen auf der Grundlage dieser Bestimmungen dürfen nur erfolgen, soweit dies zur Wahrnehmung berechtigter Interessen unseres Unternehmens oder Dritter erforderlich ist und nicht die Interessen der Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Detaillierte Informationen zur ICD i. S. d. Art. 14 Europäische Datenschutzgrundverordnung (»EU DSGVO«), d. h. Informationen zum Geschäftszweck, zu Zwecken der Datenspeicherung, zu den Datenempfängern, zum Selbstauskunftsrecht, zum Anspruch auf Löschung oder Berichtigung etc. finden Sie in der Anlage beziehungsweise unter folgendem Link: https://finance.arvato.com/icdinfoblatt

Datenübermittlung an die* SCHUFA *und Befreiung vom Bankgeheimnis (nur bei Abrechnung über ein Privatkonto)
Die Bank übermittelt im Rahmen dieses Vertragsverhältnisses erhobene personenbezogene Daten über die Beantragung, die Durchführung und Beendigung dieser Geschäftsbeziehung sowie Daten über nicht vertragsgemäßes Verhalten oder betrügerisches Verhalten an die SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden. Rechtsgrundlagen dieser Übermittlungen sind Artikel 6 Absatz 1 Buchstabe b und Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DSGVO). Übermittlungen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO dürfen nur erfolgen, soweit dies zur Wahrung berechtigter Interessen der Bank oder Dritter erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der Datenaustausch mit der SCHUFA dient auch der Erfüllung gesetzlicher Pflichten zur Durchführung von Kreditwürdigkeitsprüfungen von Kunden (§ 505a des Bürgerlichen Gesetzbuches, § 18a des Kreditwesengesetzes).
Der Kunde befreit die Bank insoweit auch vom Bankgeheimnis.
Die SCHUFA verarbeitet die erhaltenen Daten und verwendet sie auch zum Zwecke der Profilbildung (Scoring), um ihren Vertragspartnern im Europäischen Wirtschaftsraum und in der Schweiz sowie ggf. weiteren Drittländern (sofern zu diesen ein Angemessenheitsbeschluss der Europäischen Kommission besteht oder Standardvertragsklauseln vereinbart wurden, die unter www.schufa.de eingesehen werden können) Informationen unter anderem zur Beurteilung der Kreditwürdigkeit von natürlichen Personen zu geben. Nähere Informationen zur Tätigkeit der SCHUFA können dem SCHUFA-Informationsblatt nach Art. 14 DSGVO entnommen oder online unter www.schufa.de/datenschutz eingesehen werden.

Die BW-Bank ist unselbstständige Anstalt der Landesbank Baden-Württemberg. Sämtliche Erklärungen und Rechtsgeschäfte berechtigen und verpflichten ausschließlich die Landesbank Baden-Württemberg.

Rücklauf dieses Auftrags (Seite 1, 2 und 3), für die *Corporate*World Mastercard an Ihren Berater bzw. Ihre BW-Bank Filiale

Unterschrift(en) zwecks Auftragserteilung für die *Corporate*World Mastercard (Kreditkarte) und zwecks Erteilung eines SEPA-Basis-Lastschriftmandates

Ort, Datum	Unterschrift des Antragstellers

Rechtsverbindliche Unterschrift der Firma und Firmenstempel	EUR Verfügungsrahmen

Bearbeitungsvermerke (werden von der BW-Bank ausgefüllt)

Personen-Nr.	Legitimation oder Identifikation	Datum
Beratende OE/Abt.	bew. Datum/Unterschrift	Beratername in Druckbuchstaben
Kompetenzstufe	OE/Ber.Nr.	OE-Stempel
Kartenlimit	Konzernlimit	Konzern-ID

—Ausfertigung für die Bank—

Bitte ausfüllen und unterschreiben, sofern das Abrechnungskonto das Privatkonto ist.

Baden-Württembergische Bank
Kleiner Schlossplatz 11
70173 Stuttgart
Steuer-Nr. 2899/014/09009
UST-IDNr. DE 147 800 343

BW BANK
Ein Unternehmen der LBBW-Gruppe

Meine persönlichen Angaben

Vorname, Name ☐ Frau ☐ Herr	Personen-Nr.
	Geburtsdatum, ggf. Geburtsname

Informationsbogen für den Einleger

Einlagen bei der Landesbank Baden-Württemberg (LBBW) sind geschützt durch:	Sicherungssystem der Sparkassen-Finanzgruppe(1)
Sicherungsobergrenze:	100.000 EUR pro Einleger pro Kreditinstitut(2) Die folgende Marke ist Teil Ihres Kreditinstituts: Baden-Württembergische Bank (BW-Bank)
Falls Sie mehrere Einlagen bei demselben Kreditinstitut haben:	Alle Ihre Einlagen bei demselben Kreditinstitut werden „aufaddiert“, und die Gesamtsumme unterliegt der Obergrenze von 100.000 EUR(2)
Falls Sie ein Gemeinschaftskonto mit einer oder mehreren anderen Personen haben:	Die Obergrenze von 100.000 EUR gilt für jeden einzelnen Einleger(3)
Erstattungsfrist bei Ausfall eines Kreditinstituts:	7 Arbeitstage
Währung der Erstattung:	Euro (EUR)
Kontaktdaten:	Sicherungssystem der Sparkassen-Finanzgruppe Adresse: Deutscher Sparkassen- und Giroverband e.V. Charlottenstraße 47 10117 Berlin Telefon: +49 30 20225-0 E-Mail: sicherungssystem@dsgv.de
Weitere Informationen:	http://www.dsgv.de
Empfangsbestätigung durch den Einleger:	✗

Zusätzliche Informationen:
(1) Ihr Kreditinstitut ist Teil eines institutsbezogenen Sicherungssystems, das als Einlagensicherungssystem amtlich anerkannt ist. Das heißt, alle Institute, die Mitglied dieses Einlagensicherungssystems sind, unterstützen sich gegenseitig, um eine Insolvenz zu vermeiden. Im Falle einer Insolvenz werden Ihre Einlagen bis zu 100.000 EUR erstattet.

(2) Sollte eine Einlage nicht verfügbar sein, weil ein Kreditinstitut seinen finanziellen Verpflichtungen nicht nachkommen kann, so werden die Einleger von dem Einlagensicherungssystem entschädigt. Die betreffende Deckungssumme beträgt maximal 100.000 Euro pro Kreditinstitut. Das heißt, dass bei der Ermittlung dieser Summe alle bei demselben Kreditinstitut gehaltenen Einlagen addiert werden. Hält ein Einleger beispielsweise 90.000 EUR auf einem Sparkonto und 20.000 EUR auf einem Girokonto, so werden ihm lediglich 100.000 EUR erstattet.

Diese Methode wird auch angewandt, wenn ein Kreditinstitut unter unterschiedlichen Marken auftritt. Die LBBW ist auch unter dem Namen BW-Bank tätig. Das heißt, dass die Gesamtsumme aller Einlagen bei einem oder mehreren dieser Marken in Höhe von bis zu 100.000 EUR gedeckt ist.

(3) Bei Gemeinschaftskonten gilt die Obergrenze von 100.000 EUR für jeden Einleger.
Einlagen auf einem Konto, über das zwei oder mehrere Personen als Mitglieder einer Personengesellschaft oder Sozietät, einer Vereinigung oder eines ähnlichen Zusammenschlusses ohne Rechtspersönlichkeit verfügen können, werden bei der Berechnung der Obergrenze von 100.000 EUR allerdings zusammengefasst und als Einlage eines einzigen Einlegers behandelt. In den Fällen des § 8 Absätze 2 bis 4 des Einlagensicherungsgesetzes sind Einlagen über 100.000 EUR hinaus gesichert. Weitere Informationen sind erhältlich über: http://www.dsgv.de.

(4) Erstattung:
Das zuständige Einlagensicherungssystem ist das Sicherungssystem der Sparkassen-Finanzgruppe
Adresse: Deutscher Sparkassen- und Giroverband e.V.
Charlottenstraße 47
10117 Berlin
Telefon: +49 30 20225-0
E-Mail: sicherungssystem@dsgv.de
Website: http://www.dsgv.de

Es werden Ihnen Ihre Einlagen (bis zu 100.000 EUR) innerhalb von 7 Arbeitstagen erstattet.

Haben Sie die Erstattung innerhalb dieser Fristen nicht erhalten, sollten Sie mit dem Einlagensicherungssystem Kontakt aufnehmen, da der Gültigkeitszeitraum für Erstattungsforderungen nach einer bestimmten Frist abgelaufen sein kann. Weitere Informationen sind erhältlich über: http://www.dsgv.de

Weitere wichtige Informationen:
Einlagen von Privatkunden und Unternehmen sind im Allgemeinen durch Einlagensicherungssysteme gedeckt. Für bestimmte Einlagen geltende Ausnahmen werden auf der Website des zuständigen Einlagensicherungssystems mitgeteilt. Ihr Kreditinstitut wird Sie auf Anfrage auch darüber informieren, ob bestimmte Produkte gedeckt sind oder nicht. Wenn Einlagen entschädigungsfähig sind, wird das Kreditinstitut dies auch auf dem Kontoauszug bestätigen.

LB BW

BW BANK

Hiermit informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten durch uns 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 jeweils von Ihnen beantragten bzw. mit Ihnen vereinbarten Dienstleistungen.

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?	Verantwortliche Stelle ist: Landesbank Baden-Württemberg Am Hauptbahnhof 2 70173 Stuttgart 0711 127-0 0711 127-43544 kontakt@lbbw.de
	Sie erreichen unseren Datenschutzbeauftragten unter: Landesbank Baden-Württemberg Datenschutzbeauftragter Am Hauptbahnhof 2 70173 Stuttgart 0711 127-0 datenschutz@lbbw.de
2. Welche Quellen und Daten nutzen wir?	Wir verarbeiten personenbezogene Daten, die wir im Rahmen unserer Geschäftsbeziehung von Ihnen erhalten. Zudem verarbeiten wir – soweit für die Erbringung unserer Dienstleistung erforderlich – personenbezogene Daten, die wir von anderen Unternehmen der Sparkassen-Finanzgruppe (SFG)[1] 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. Zum anderen verarbeiten wir personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen (z. B. Schuldnerverzeichnisse, Grundbücher, Handels- und Vereinsregister, Presse, Medien) zulässigerweise gewonnen haben und verarbeiten dürfen. Relevante personenbezogene Daten sind Personalien (z.B. Name, Adresse und andere Kontaktdaten, Geburtstag und -ort und Staatsangehörigkeit), Legitimationsdaten (z. B. Ausweisdaten) und Authentifikationsdaten (z. B. Unterschriftprobe). Darüber hinaus können dies auch Auftragsdaten (z. B. Zahlungsauftrag, Wertpapierauftrag), Daten aus der Erfüllung unserer vertraglichen Verpflichtungen (z. B. Umsatzdaten im Zahlungsverkehr), Kreditrahmen, Produktdaten (z. B. Einlagen-, Kredit- und Depotgeschäft), Informationen über Ihre finanzielle Situation (Bonitätsdaten, Scoring-/ Ratingdaten, Herkunft von Vermögenswerten), Werbe- und Vertriebsdaten (inklusive Werbescores), Dokumentationsdaten (z. B. Geeignetheitserklärung), Registerdaten, Daten über Ihre Nutzung von unseren angebotenen Telemedien (z. B. Zeitpunkt des Aufrufs unserer Webseiten, Apps oder Newsletter, angeklickte Seiten von uns bzw. Einträge) sowie andere mit den genannten Kategorien vergleichbare Daten sein. In begrenztem Umfang verarbeiten wir auch Tonaufnahmen von Telefongesprächen, z. B. im Rahmen des Telefon-Bankings oder im Zusammenhang mit der Erbringung von Wertpapierdienstleistungen. Dies erfolgt in der Regel auf gesetzlicher oder vertraglicher Grundlage sowie wenn Sie uns zuvor Ihre Einwilligung dazu erteilt haben. Bei der Aufzeichnung werden neben dem eigentlichen Gesprächsinhalt auch technische Informationen aus dem Telefonsystem verarbeitet, die entweder dort erzeugt oder durch Übermittlung der Telefongesellschaft bereitgestellt wurden (z. B. Rufnummern, Gesprächsbeginn und die Dauer des Gesprächs). [1] *Unsere Verbundpartner finden Sie auch unter* *www.lbbw.de/rechtlichehinweise*
3. Wofür verarbeiten wir Ihre Daten (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage?	Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG).
3.1 Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 Buchst. b DS-GVO)	Die Verarbeitung personenbezogener Daten (Art. 4 Nr. 2 DS-GVO) erfolgt zur Erbringung und Vermittlung von Bankgeschäften, Finanzdienstleistungen sowie Versicherungs- und Immobiliengeschäften, insbesondere zur Durchführung unserer Verträge oder vorvertraglichen Maßnahmen mit Ihnen und der Ausführung Ihrer Aufträge 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 konkreten Produkt (z. B. Konto, Kredit, Bausparen, Wertpapiere, Einlagen, Vermittlung) und können unter anderem Bedarfsanalysen, Beratung, Vermögensverwaltung und -betreuung, die Durchführung von Transaktionen, Vermittlung von Geschäften zwischen Ihnen und Dritten (z.B. Förderbanken, Versicherungen, Immobiliengesellschaften) umfassen. Die weiteren Einzelheiten zum Zweck der Datenverarbeitung können Sie den jeweiligen Vertragsunterlagen und Geschäftsbedingungen entnehmen.
3.2 Im Rahmen der Interessenabwägung (Art. 6 Abs. 1 Buchst. f DS-GVO)	Soweit erforderlich, verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von uns oder Dritten. Beispiele: - Konsultation von und Datenaustausch mit Auskunfteien (z. B. SCHUFA) zur Ermittlung von Bonitäts- bzw. Ausfallrisiken und des Bedarfs beim Pfändungsschutzkonto oder Basiskonto; - Kreditkarten-Aktualisierungsservice von Visa bzw. Mastercard, soweit beim teilnehmenden Händler, die Kreditkarteninformationen in einen Token umgewandelt werden; - Prüfung und Optimierung von Verfahren zur Bedarfsanalyse und direkter Kundenansprache; - Werbung oder Markt- und Meinungsforschung, soweit Sie der Nutzung Ihrer Daten nicht widersprochen haben; - Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten; - Gewährleistung der IT-Sicherheit und des IT-Betriebs der Bank; - 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 Kunden und Mitarbeitern sowie der Wahrnehmung des Hausrechts; - Maßnahmen zur Gebäude- und Anlagensicherheit (z.B. Zutrittskontrollen); - Maßnahmen zur Sicherstellung des Hausrechts; - Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten.

3.3 Aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 Buchst. a DS-GVO)	Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z. B. Weitergabe von Daten im Verbund[2], 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 DS-GVO, 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. Wir verwenden eine standardisierte Einwilligungserklärung, um individuelle und möglichst passgenaue Beratung, Betreuung und Information über Produkte und Aktionen zu ermöglichen. Die Einwilligung ermöglicht uns beispielsweise komplexe Datenanalysen, inwiefern ein bestimmtes Produkt für gewisse Kunden von Interesse sein könnte. Beispielsweise könnten wir durch die Auswertung zahlreicher Datenfelder zu den persönlichen finanziellen Verhältnissen bestimmen, für welche unserer Kunden ein Angebot zu einem Konsumentenkredit oder einem Anlageprodukt besonders interessant sein dürfte, und gezielt diese Kunden auf dieses Angebot aufmerksam machen. Sollten Sie diese Einwilligung nicht erteilen, ist es uns trotzdem möglich, unsere vertraglichen Leistungen Ihnen gegenüber zu erfüllen. Die Rechtsgrundlage für die entsprechende Datenverarbeitung ist dann die Erfüllung unseres Vertrags mit Ihnen (s. Ziffer 3.1 dieser Datenschutzhinweise). Ebenso können wir ohne diese Einwilligung in gewissen Fällen noch einfache Datenverarbeitungen vornehmen, um jenseits des Vertrags Ihre Daten zu verarbeiten (s. dazu Ziffer 3.2 dieser Datenschutzhinweise). [2] *Unsere Verbundpartner finden Sie auch unter www.lbbw.de/rechtlichehinweise*
3.4 Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 Buchst. c DS-GVO) oder im öffentlichen Interesse (Art. 6 Abs. 1 Buchst. e DS-GVO)	Zudem unterliegen wir als Bank diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen (z. B. Kreditwesengesetz, Geldwäschegesetz, Wertpapierhandelsgesetz, Steuergesetze) sowie bankenaufsichtsrechtlichen Vorgaben (z. B. der Europäischen Zentralbank, der Europäischen Bankenaufsicht, der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht sowie die nach dem Gesetz über die Landesbank Baden-Württemberg zuständige Aufsichtsbehörde). Zu den Zwecken der Verarbeitung gehören unter anderem die Kreditwürdigkeitsprüfung, die Identitäts- und Altersprüfung, Betrugs- und Geldwäscheprävention, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie die Bewertung und Steuerung von Risiken.
4. Wer bekommt meine Daten?	Innerhalb der Bank erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten brauchen. Auch von uns eingesetzte Auftragsverarbeiter (Art. 28 DS-GVO) können zu diesen genannten Zwecken Daten erhalten. Dies sind Unternehmen in den Kategorien kreditwirtschaftliche Leistungen, IT-Dienstleistungen, Logistik, Druckdienstleistungen, Telekommunikation, Inkasso, Beratung und Consulting sowie Vertrieb und Marketing. Im Hinblick auf die Datenweitergabe an Empfänger außerhalb der Bank ist zunächst zu beachten, dass wir nach den zwischen Ihnen und uns vereinbarten Allgemeinen Geschäftsbedingungen zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet sind, von denen wir Kenntnis erlangen (Bankgeheimnis). Informationen über Sie dürfen wir nur weitergeben, 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, Europäische Bankenaufsichtsbehörde, 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 (je nach Vertrag: z. B. Förderbanken, Versicherungen, Korrespondenz-Institute, Depotbanken, Börsen, Auskunfteien). Weitere Datenempfänger können diejenigen Stellen sein, für die Sie uns Ihre Einwilligung zur Datenübermittlung erteilt haben bzw. für die Sie uns vom Bankgeheimnis gemäß Vereinbarung oder Einwilligung befreit haben.
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 Vertrages 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), dem Geldwäschegesetz (GwG) und dem Wertpapierhandelsgesetz (WpHG) ergeben. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen zwei bis zehn Jahre. Schließlich beurteilt sich die Speicherdauer auch nach den gesetzlichen Verjährungsfristen, die z. B. nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) in der Regel 3 Jahre, in gewissen Fällen aber auch bis zu dreißig Jahre betragen können. Telefonaufzeichnungen, die im Rahmen des Telefon-Bankings erfolgen, werden spätestens nach 13 Monaten gelöscht. Für Telefonaufnahmen, die im Zusammenhang mit Wertpapierdienstleistungen erfolgen, gelten Speicherpflichten von 5 bis zu 7 Jahren. Sonstige Telefonaufzeichnungen werden spätestens nach 6 Monaten gelöscht.
6. Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?	Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums – EWR) findet nur statt, soweit dies zur Ausführung Ihrer Aufträge (z. B. Zahlungsaufträge, Wertpapieraufträge und Kreditkarten) erforderlich, gesetzlich vorgeschrieben ist oder Sie uns Ihre Einwilligung erteilt haben. *www.lbbw.de/datenschutz*
7. Welche Datenschutzrechte habe ich?	Jede betroffene Person hat 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, das Recht auf **Einschränkung der Verarbeitung** nach Art. 18 DS-GVO sowie das Recht auf **Datenübertragbarkeit** aus Art. 20 DS-GVO. Beim Auskunftsrecht und beim Löschungs- recht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DS-GVO i. V. m. § 19 BDSG).

8. Besteht für mich 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 oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel den Abschluss des Vertrages oder die Ausführung des Auftrages 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 beispielsweise anhand Ihres Personalausweises zu identifizieren und dabei Ihren Namen, Ihren Geburtsort, Ihr Geburtsdatum, Ihre 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?	Zur Begründung und Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine automatisierte Entscheidungsfindung gemäß Art. 22 DS-GVO. Sollten wir diese Verfahren in einzelnen Geschäftsbereichen (z.B. Festlegung von Kreditlinien, Zulassung von Kontoüberziehungen) 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. - 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 sowie zur Vergabe von Konditionen nutzen wir für Privatkunden das Scoring bzw. für Firmenkunden das Rating. 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, Zahlungsverhalten (z. B. Kontoumsätze, Salden), Erfahrungen aus der bisherigen Geschäftsverbindung, vertragsgemäße Rückzahlung früherer Kredite sowie Informationen von Kreditauskunfteien einfließen. Bei Firmenkunden fließen zusätzlich weitere Daten mit ein, wie Branche, Jahresergebnisse sowie Vermögensverhältnisse. Das Scoring und das Rating beruhen beide auf einem mathematisch-statistisch anerkannten und bewährten Verfahren. Die errechneten Scorewerte und Bonitätsnoten unterstützen uns bei der Entscheidungsfindung im Rahmen von Produktabschlüssen und gehen in das laufende Risikomanagement mit ein.

LB≡BW BW≡BANK

Information über Ihr Widerspruchsrecht nach Art. 21 DSGVO

1. Einzelfallbezogenes Widerspruchsrecht

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstabe e der DS-GVO (Datenverarbeitung im öffentlichen Interesse) und Artikel 6 Absatz 1 Buchstabe f der DS-GVO (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 DS-GVO, 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. Widerspruchsrecht gegen eine Verarbeitung von Daten für Zwecke der Direktwerbung

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 gerichtet werden an:

Landesbank Baden-Württemberg
Am Hauptbahnhof 2
70173 Stuttgart
0711 127-0
0711 127-43544
kontakt@lbbw.de

Information gem. Art. 14 EU-DSGVO über die infoscore Consumer Data GmbH (»ICD«).

BW BANK
Ein Unternehmen der LBBW-Gruppe

1. Name und Kontaktdaten der ICD (verantwortliche Stelle) sowie des betrieblichen Datenschutzbeauftragten
infoscore Consumer Data GmbH, Rheinstraße 99, 76532 Baden-Baden
Der betriebliche Datenschutzbeauftragte der ICD ist unter der o.a. Anschrift, zu Hd. Abteilung Datenschutz, oder per E-Mail unter: ICD-Datenschutz@experian.com erreichbar.

2. Zwecke der Datenverarbeitung der ICD
Die ICD verarbeitet und speichert personenbezogene Daten, um ihren Vertragspartnern Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen und juristischen Personen sowie zur Prüfung der postalischen Erreichbarkeit von Personen zu geben. Hierzu werden auch Wahrscheinlichkeits- bzw. Scoringwerte errechnet und übermittelt. Solche Auskünfte sind notwendig und erlaubt, um das Zahlungsausfallrisiko z. B. bei einer Kreditvergabe, beim Rechnungskauf oder bei Abschluss eines Versicherungsvertrages vorab einschätzen zu können. Die Datenverarbeitung und die darauf basierenden Auskunftserteilungen der ICD dienen gleichzeitig der Bewahrung der Auskunftsempfänger vor wirtschaftlichen Verlusten und schützen Verbraucher gleichzeitig vor der Gefahr der übermäßigen Verschuldung. Die Verarbeitung der Daten erfolgt darüber hinaus zur Identitätsprüfung, Betrugsprävention, Anschriftenermittlung, Risikosteuerung, Festlegung von Zahlarten oder Konditionen sowie zur Tarifierung.

3. Rechtsgrundlagen für die Datenverarbeitung der ICD
Die ICD ist ein Auskunfteiunternehmen, das als solches bei der zuständigen Datenschutzaufsichtsbehörde gemeldet ist. Die Verarbeitung der Daten durch die ICD erfolgt auf Basis einer Einwilligung gemäß Art. 6 Abs. 1a i. V. m. Art. 7 Datenschutzgrundverordnung (DSGVO) oder auf Grundlage des Art. 6 Abs. 1f DSGVO, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und sofern die Interessen und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Die ICD stellt ihren Vertragspartnern die Informationen nur dann zur Verfügung, wenn eine Einwilligung des Betroffenen vorliegt oder von den Vertragspartnern 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 wirtschaftlichem Risiko gegeben (z. B. Rechnungskauf, Kreditvergabe, Abschluss eines Mobilfunk-, Festnetz- oder Versicherungsvertrages).

4. Kategorien der personenbezogenen Daten der ICD
Von der ICD werden personenbezogene Daten (Name, Vorname(n), Geburtsdatum, Anschrift(en), Telefonnummer(n), E-Mail-Adresse(n)), Informationen zum vertragswidrigen Zahlungsverhalten (siehe auch Ziff. 5), zu Schuldnerverzeichniseintragungen, (Privat-)Insolvenzverfahren und zur postalischen (Nicht-)Erreichbarkeit sowie entsprechende Scorewerte verarbeitet bzw. gespeichert.

5. Herkunft der Daten der ICD
Die Daten der ICD stammen aus den amtlichen Insolvenzveröffentlichungen sowie den Schuldnerverzeichnissen, die bei den zentralen Vollstreckungsgerichten geführt werden. Dazu kommen Informationen von Vertragspartnern der ICD über vertragswidriges Zahlungsverhalten, basierend auf gerichtlichen sowie außergerichtlichen Inkassomaßnahmen. Darüber hinaus werden personenbezogene Daten (s. Nr. 4) aus den Anfragen von Vertragspartnern der ICD gespeichert sowie Daten von Adressdienstleistern.

6. Kategorien von Empfängern der personenbezogenen Daten der ICD
Empfänger sind insbesondere Unternehmen, die ein wirtschaftliches Risiko tragen und ihren Sitz im Europäischen Wirtschaftsraum, in Großbritannien und in der Schweiz haben. Es handelt sich dabei im Wesentlichen um eCommerce-, Telekommunikations- und Versicherungsunternehmen, Finanzdienstleister (z. B. Banken, Kreditkartenanbieter), Energieversorgungs- und Dienstleistungsunternehmen. Darüber hinaus gehören zu den Empfängern solche Unternehmen, die Forderungen einziehen, wie etwa Inkassounternehmen, Abrechnungsstellen, Rechtsanwälte, Adressdienstleister sowie Dienstleister der ICD (z. B. Rechenzentrum, Postdienstleister).

7. Dauer der Datenspeicherung der ICD
Die ICD speichert Informationen über Personen nur für eine bestimmte Zeit, nämlich solange, wie deren Speicherung i. S. d. Art. 17 Abs. 1 lit. a) DSGVO notwendig ist.
Die bei der ICD zur Anwendung kommenden Prüf- und Löschfristen entsprechen einer Selbstverpflichtung (Code of Conduct) der im Verband »Die Wirtschaftsauskunfteien e.V.« zusammengeschlossenen Auskunfteiunternehmen.

- Informationen über fällige und unbestrittene Forderungen bleiben gespeichert, solange deren Ausgleich nicht bekannt gegeben wurde; die Erforderlichkeit der fortwährenden Speicherung wird jeweils taggenau nach drei Jahren überprüft. Wird der Ausgleich der Forderung bekannt gegeben, erfolgt eine Löschung der personenbezogenen Daten taggenau drei Jahre danach.
- Daten aus den Schuldnerverzeichnissen der zentralen Vollstreckungsgerichte (Eintragungen nach § 882c Abs. 1 Satz 1 Nr. 1 – 3 ZPO) werden taggenau nach drei Jahren gelöscht, jedoch vorzeitig, wenn der ICD eine Löschung durch das zentrale Vollstreckungsgericht nachgewiesen wird.
- Informationen über Verbraucher-/Insolvenzverfahren oder Restschuldbefreiungsverfahren werden taggenau drei Jahre nach Beendigung des Insolvenzverfahrens oder nach Erteilung oder Versagung der Restschuldbefreiung gelöscht.
- Informationen über die Abweisung eines Insolvenzantrages mangels Masse, die Aufhebung der Sicherungsmaßnahmen oder über die Versagung der Restschuldbefreiung werden taggenau nach drei Jahren gelöscht.
- Angaben über Anfragen werden spätestens taggenau nach drei Jahren gelöscht.
- Voranschriften bleiben taggenau drei Jahre gespeichert; danach erfolgt die Prüfung der Erforderlichkeit der fortwährenden Speicherung für weitere drei Jahre. Danach werden sie taggenau gelöscht, sofern nicht zum Zwecke der Identifizierung eine länger währende Speicherung erforderlich ist.

8. Betroffenenrechte gegenüber der ICD
Jede betroffene Person hat gegenüber der ICD 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. Darüber hinaus besteht die Möglichkeit, sich an die für die ICD zuständige Aufsichtsbehörde »Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Lautenschlagerstraße 20, 70173 Stuttgart« zu wenden. Einwilligungen können jederzeit gegenüber dem betreffenden Vertragspartner widerrufen werden. Dies gilt auch für Einwilligungen, die bereits vor Inkrafttreten der DSGVO erteilt wurden. Der Widerruf der Einwilligung berührt nicht die Rechtmäßigkeit der bis zum Widerruf verarbeiteten personenbezogenen Daten.

Nach Art. 21 Abs. 1 DSGVO kann der Datenverarbeitung aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, gegenüber der ICD widersprochen werden.

Sofern Sie wissen wollen, welche Daten die ICD zu Ihrer Person gespeichert und an wen sie welche Daten übermittelt hat, teilt Ihnen die ICD das gerne im Rahmen einer -unentgeltlichen- schriftlichen Selbstauskunft mit. Die ICD bittet um Ihr Verständnis, dass sie aus datenschutzrechtlichen Gründen keinerlei telefonische Auskünfte erteilen darf, da eine eindeutige Identifizierung Ihrer Person am Telefon nicht möglich ist. Um einen Missbrauch des Auskunftsrechts durch Dritte zu vermeiden, benötigt die ICD folgende Angaben von Ihnen: Name (ggf. Geburtsname), Vorname(n), Geburtsdatum, aktuelle Anschrift (Straße, Hausnummer, Postleitzahl und Ort), ggf. Voranschriften der letzten fünf Jahre (dies dient der Vollständigkeit der zu erteilenden Auskunft)
Wenn Sie – auf freiwilliger Basis – eine Kopie Ihres Ausweises beifügen, erleichtern Sie der ICD die Identifizierung Ihrer Person und vermeiden damit mögliche Rückfragen. Sie können die Selbstauskunft auch via Internet unter https://www.experian.de/selbstauskunft beantragen.

9. Profilbildung/Profiling/Scoring
Die ICD-Auskunft kann um sogenannte Scorewerte ergänzt werden. Beim Scoring der ICD wird anhand von Informationen und Erfahrungen aus der Vergangenheit eine Prognose insbesondere über Zahlungswahrscheinlichkeiten erstellt. Das Scoring basiert primär auf Basis der zu einer betroffenen Person bei der ICD gespeicherten Informationen. Anhand dieser Daten, von adressbezogenen Daten sowie von Anschriftendaten erfolgt auf Basis mathematisch-statistischer Verfahren (insbes. Verfahren der logistischen Regression) eine Zuordnung zu Personengruppen, die in der Vergangenheit ähnliches Zahlungsverhalten aufwiesen.
Folgende Datenarten werden bei der ICD für das Scoring verwendet, wobei nicht jede Datenart auch in jede einzelne Berechnung mit einfließt: Daten zum vertragswidrigen Zahlungsverhalten (siehe Nrn. 4 u. 5), zu Schuldnerverzeichnis-Eintragungen und Insolvenzverfahren (siehe Nrn. 4 u. 5), Geschlecht und Alter der Person, adressbezogene Daten (Bekanntsein des Namens bzw. des Haushalts an der Adresse, Anzahl bekannter Personen im Haushalt (Haushaltsstruktur), Bekanntsein der Adresse), Anschriftendaten (Informationen zu vertragswidrigem Zahlungsverhalten in Ihrem Wohnumfeld (Straße/Haus)), Daten aus Anfragen von Vertragspartnern der ICD.
Besondere Kategorien von Daten i. S. d. Art. 9 DSGVO (z. B. Angaben zur Staatsangehörigkeit, ethnischen Herkunft oder zu politischen oder religiösen Einstellungen) werden von der ICD weder gespeichert noch bei der Berechnung von Wahrscheinlichkeitswerten berücksichtigt. Auch die Geltendmachung von Rechten nach der DSGVO, also z. B. die Einsichtnahme in die bei der ICD gespeicherten Informationen nach Art. 15 DSGVO, hat keinen Einfluss auf das Scoring.
Die ICD selbst trifft keine Entscheidungen über den Abschluss eines Rechtsgeschäfts oder dessen Rahmenbedingungen (wie z. B. angebotene Zahlarten), sie unterstützt die ihr angeschlossenen Vertragspartner lediglich mit ihren Informationen bei der diesbezüglichen Entscheidungsfindung. Die Risikoeinschätzung und Beurteilung der Kreditwürdigkeit sowie die darauf basierende Entscheidung erfolgt allein durch Ihren Geschäftspartner.

Stand des Dokuments: August 2022

SCHUFA-Information nach Art. 14 DSGVO.

BW BANK
Ein Unternehmen der LBBW-Gruppe

Stand: Dezember 2023

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 datenschutz@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 zur Teilnahme an nationalen und internationalen externen Forschungsprojekten im Bereich der genannten Verarbeitungszwecke sowie Gewährleistung 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 DSGVO 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 DSGVO) sowie auf Grundlage des Art. 6 Abs. 1 Buchstabe f DSGVO, 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 DSGVO 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 oder Standardvertragsklauseln vereinbart wurden, die unter www.schufa.de eingesehen werden können) 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 etwa öffentlichen Verzeichnissen und amtlichen Bekanntmachungen (z. B. 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 sonstigem 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 DSGVO 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. Dieser sowie weitere Details zu unseren Löschfristen können unter www.schufa.de/loeschfristen eingesehen werden.

3. Betroffenenrechte
Jede betroffene Person hat gegenüber der SCHUFA das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO und das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO. 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 DSGVO kann der Datenverarbeitung aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, widersprochen werden. Das Widerspruchsrecht gilt auch für die nachfolgend dargestellte Profilbildung. Der Widerspruch kann formfrei erfolgen und z. B. an SCHUFA Holding AG, Privatkunden ServiceCenter, Postfach 10 34 41, 50474 Köln gerichtet werden.

4. Profilbildung (Scoring)
Neben der Erteilung von Auskünften über die zu einer Person gespeicherten Informationen unterstützt die SCHUFA ihre Vertragspartner durch Profilbildungen, insbesondere mittels sogenannter Scorewerte.
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 DSGVO 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 DSGVO (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 DSGVO, wie z. B. die Einsichtnahme in die zur eigenen Person bei der SCHUFA gespeicherten Daten nach Art. 15 DSGVO, 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 grundsätzlich keine Entscheidungen. Sie unterstützt die angeschlossenen Vertragspartner lediglich mit ihren Auskünften und Profilbildungen in ihrem Risikomanagement. Die Entscheidung für oder gegen ein Geschäft trifft hingegen allein der direkte Geschäftspartner. Verlässt sich ein Vertragspartner bei seiner Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses maßgeblich auf das Scoring der SCHUFA, gelten ergänzend die Bestimmungen des Art. 22 DSGVO. Das Scoring der SCHUFA kann in diesem Fall z. B. dabei helfen, alltägliche Kreditgeschäfte rasch abwickeln zu können; es kann unter Umständen aber auch dazu führen, dass ein Vertragspartner eine negative, möglicherweise ablehnende Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses trifft. Weiterführende Informationen, wie ein Vertragspartner das Scoring der SCHUFA verwendet, können beim jeweiligen Vertragspartner eingeholt werden. 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.

Sicheres Bezahlen im Internet.

Fassung: Dezember 2021

1. Allgemeine Hinweise

1.1 Geben Sie Ihre Kreditkartendaten nur bei Händlern an, die Ihnen absolut vertrauenswürdig erscheinen.
1.2 Achten Sie darauf, dass die Daten ausschließlich verschlüsselt übertragen werden. Dies erkennen Sie daran, dass die Internetadresse mit »https« beginnt.
1.3 Als Sicherheit bieten Händler das sogenannte 3D-Secure-Verfahren an (auch »Visa Secure« bzw. »Mastercard Identity Check™« genannt). Ob ein Händler hieran teilnimmt, können Sie der jeweiligen Bestellseite entnehmen.
1.4 Ihre Kreditkarte ist für den Einsatz im Internet ausgestattet. Der allgemeine Verfügungsrahmen Ihrer Kreditkarte gilt auch für Einkäufe im Internet. Sie können den Verfügungsrahmen nach Ihren Wünschen absenken lassen. Auch können Sie Ihre Kreditkarte für Internetzahlungen deaktivieren lassen. Zu den vorgenannten Fällen wenden Sie sich bitte an den BW-Bank Karten-Service.

2. Durchführen einer Transaktion

2.1 Um eine Transaktion durchzuführen, werden während des Kaufprozesses im Internet die Daten Ihrer Kreditkarte abgefragt. Bitte achten Sie darauf, dass Sie diese nur in einer sicheren Umgebung eingeben (siehe Punkt 1). Andernfalls besteht ein erhöhtes Risiko bei der Übermittlung Ihrer Daten.
2.2 Unterstützt ein Händler das 3D-Secure-Verfahren, ist es erforderlich, dass Ihre Kreditkarte ebenfalls hierfür aktiviert ist. Falls noch nicht geschehen, registrieren Sie sich bitte für die BW-Secure App oder SMS-mTAN mit 3D-Secure-Verfahren über die spezielle Internetseite Ihrer BW-Bank (https://sicheres-bezahlen.bw-bank.de). Sofern Sie sich nicht registrieren, kann die Transaktion nicht durchgeführt werden.
2.3 Die Genehmigung der Zahlung erfolgt mit Angabe der Kartendaten bzw. Auslösung der Zahlung über das 3D-Secure-Verfahren. Mit diesem Schritt ist die Zahlung über Ihre Kreditkarte abgeschlossen.

3. Achten Sie auf Auffälligkeiten

3.1 Kommt Ihnen im Bestellprozess etwas ungewöhnlich vor oder vermuten Sie den Missbrauch Ihrer Daten, kontaktieren Sie bitte umgehend den BW-Bank Karten-Service. Die Rufnummer finden Sie u. a. auf der Rückseite Ihrer Kreditkarte.
3.2 Bei Umsatzreklamationen wenden Sie sich bitte schriftlich an den BW-Bank Karten-Service. Die Kontaktdaten finden Sie auf Ihrer Kreditkartenabrechnung. Sie werden sodann schriftlich über die weitere Bearbeitung informiert. Je nach Fall wird von Ihrer BW-Bank eine Rückbuchung mit Gutschrift vorgenommen oder weitere Unterlagen (Belege etc.) von Ihnen angefordert. Die BW-Bank wird in Abstimmung mit Ihnen weitere Maßnahmen zur Sicherung Ihrer Kreditkarte ergreifen, z. B. die Sperrung der Karte oder Neuversand einer Karte.
3.3 Vorsicht vor Phishing
Es kommt vor, dass Betrüger E-Mails mit Links versenden oder Werbeanzeigen bei Suchdiensten schalten. Diese sehen aus wie von der BW-Bank versendet oder geschaltet, enthaltene Links führen aber auf Internetseiten der Betrüger. Achten Sie immer darauf, dass die Internetseite die Adresse »www.bw-bank.de« am Ende enthält. Es muss immer ein Punkt vor »bw-bank.de« stehen, damit es eine offizielle Seite der BW-Bank ist. Gültig sind beispielsweise auch »sicheres-bezahlen.bw-bank.de« oder »kso.bw-bank.de«.
Geben Sie nur dann Daten ein, wenn Sie sicher sind auf einer Internetseite der BW-Bank zu sein. Optik und Inhalte werden von den Betrügern imitiert und nur die gültige Internetadresse in der Adresszeile Ihres Browsers bietet Sicherheit. Wenn Sie nicht sicher sind, geben Sie keine Daten ein (!) und wenden Sie sich direkt an den Kundenservice der BW-Bank.

4. Präventivmaßnahmen beim Einsatz Ihrer Karte

4.1 Die BW-Bank ist berechtigt, die Kreditkarte bei Vorliegen der in den Kartenbedingungen genannten Voraussetzungen zu sperren oder eine bestimmte Transaktion aufgrund von Sicherheitsbedenken abzulehnen. Diese Maßnahmen verhindern Betrug und dienen Ihrem Schutz.
4.2 Über eine Sperre werden Sie von der BW-Bank unverzüglich telefonisch oder schriftlich informiert.
4.3 Für Informationen hierzu steht Ihnen der BW-Bank Karten-Service zur Verfügung. Dort können Sie zudem die Aufhebung der Sperre beantragen bzw. klären, warum es zur Ablehnung einer Transaktion kam. Sollten wir Sie durch unsere Maßnahme in Ihrem Einkauf behindert haben, können Ihnen unsere Mitarbeiter hierzu weiterhelfen.

5. Verlust der personalisierten Sicherheits-Berechtigungsnachweise

Wenn Ihr Passwort oder Ihre Zahlungsdaten (Kreditkartennummer, Prüfziffer, Gültigkeitsdatum) ausgespäht worden oder in falsche Hände geraten sind, wenden Sie sich unverzüglich an den BW-Bank Karten-Service. Dies gilt auch für Vorfälle während eines Zahlungsvorgangs oder in sozialen Medien (z. B. Anfrage nach Ihren Zahlungsdaten).

6. Betrugsfall

6.1 Informieren Sie bitte umgehend telefonisch den BW-Bank Karten-Service, wenn Sie vermuten, dass unbefugte Personen im Besitz Ihrer persönlichen Kreditkartendaten sind.
6.2 Wir stimmen mit Ihnen ab, ob die Sperrung Ihrer Kreditkarte erforderlich ist.
6.3 Sofern betrügerische Transaktionen mit Ihrer BW-Bank Kreditkarte erkannt werden, werden Sie durch die BW-Bank umgehend hierüber informiert.

7. Schutz Ihrer Daten

7.1 Passwörter, persönliche Angaben und sonstige vertrauliche Daten gehören nur Ihnen und müssen vor dem Zugriff Fremder geschützt werden. Auch Ihr Kundenberater kennt diese vertraulichen Informationen nicht und wird diese nicht von Ihnen erfragen.
7.2 Bei der Registrierung oder Neuregistrierung für das sichere Zahlverfahren 3D-Secure (»Visa Secure« oder »Mastercard Identity Check™«) werden Sie von Ihrer BW-Bank über den genauen Ablauf und die Voraussetzungen einer Zahlung nach diesem Verfahren informiert. Achten Sie bei der Registrierung oder Neuregistrierung darauf, dass diese im sicheren technischen Umfeld Ihrer BW-Bank erfolgt (https://sicheres-bezahlen.bw-bank.de).
7.3 Die BW-Bank setzt nur sichere und zertifizierte Hard- und Software ein. Achten Sie darauf, dass Sie ggf. Apps, die Sie von der BW-Bank zur Verfügung gestellt bekommen, über einen sicheren Download beziehen (Apple Store, Google Play Store etc.). Nur diese Programme sind geprüft und sicher. Genaue Hinweise erhalten Sie bei der Registrierung zum jeweiligen Verfahren.
7.4 Um die Kreditkarte für Zahlungen im Internet sicher verwenden zu können, achten Sie bitte auf eine sichere IT-Umgebung auf Ihrem Computer. Dazu gehören

- ein aktuelles Antivirenprogramm,
- eine konfigurierte Firewall,
- ein aktuelles Betriebssystem mit allen Sicherheitsupdates,
- eine sichere (verschlüsselte) Verbindung zur aufgerufenen Website (diese erkennen Sie am Schlosssymbol in Ihrem Browser sowie daran, dass die Internetadresse mit »https« beginnt) und
- eine sichere Verbindung zum Internet (unverschlüsselte WLAN-Verbindungen an öffentlichen Plätzen können von Angreifern kompromittiert werden).

Hinweis: Auch die korrekte Schreibweise der URL in der Adresszeile im Browser ist wichtig. Betrüger können sich Tippfehler zunutze machen, um Sie auf eine ähnliche Seite umzuleiten, wenn Sie Ihre Zahlungsdaten (Kreditkartennummer, Prüfziffer, Gültigkeitsdatum) eingeben.
7.5 Laden Sie Dateien und Programme aus dem Internet nur von vertrauenswürdigen Seiten und nur, wenn Sie mit hinreichender Sicherheit feststellen können, dass die Software echt ist und nicht manipuliert wurde.
7.6 Geben Sie Ihre Zahlungsdaten (Kreditkartennummer, Prüfziffer, Gültigkeitsdatum) nicht auf unbekannten oder nicht vertrauenswürdigen Seiten ein.

8. Regelmäßige Informationen

Die BW-Bank wird Sie über Änderungen im Internetzahlungsverkehr oder weitere Sicherheitshinweise nur über einen gesicherten Kommunikationsweg informieren. Dazu zählen Ihr elektronisches Postfach im BW Online-Banking oder im BW Kartenservice Online, eine gesicherte Website wie »www.bw-bank.de«, Nachrichten am Kontoauszugsdrucker oder der Postweg. Andere Nachrichten sind in der Regel nicht vertrauenswürdig. Wenn Ihnen eine Nachricht verdächtig vorkommt, setzen Sie sich bitte umgehend mit dem BW-Bank Karten-Service in Verbindung.

Bedingungen für die Nutzung des BW-Secure-Verfahrens.

BW-Secure-App mit 3D-Secure-Verfahren oder SMS-mTAN mit 3D-Secure-Verfahren.

Stand: 13. Juni 2022

Gegenstand

Die nachfolgenden Bestimmungen regeln das Verhältnis zwischen der Baden-Württembergischen Bank (nachfolgend als »Bank« bezeichnet) und dem Karteninhaber im Zusammenhang mit der Nutzung des BW-Secure-Verfahrens. Bei Nutzung des BW-Secure-Verfahrens hat der Kunde die Wahl zwischen der Mobile App »BW-Secure« (nachfolgend »BW-Secure-App« genannt) und dem SMS-mTAN-Verfahren mit statischem Passwort (nachfolgend »SMS-mTAN« genannt). Beide Techniken beinhalten das 3D-Secure-Verfahren. Die vorliegenden Bedingungen gelten in Ergänzung zu den übrigen für das Kredit-/Debitkartenverhältnis zwischen der Bank und dem Karteninhaber vereinbarten Bedingungen.

3D-Secure ist ein international anerkannter Standard für die Identifikation von Karteninhabern bei Kredit-/Debitkartenzahlungen im Internet (nachfolgend als »Transaktion/-en« bezeichnet). Das Verfahren wird von Mastercard als »Mastercard® Identity Check™« und von Visa als »Visa Secure« betrieben. Die BW-Secure-App und das SMS-mTAN-Verfahren beinhalten diesen 3D-Secure-Standard für die Freigabe von Kredit-/Debitkartenzahlungen im Internet. Darüber hinaus wird die BW-Secure-App und die SMS-mTAN für die Identifikation des Karteninhabers bei Online-Mitteilungen und Aufträgen des Karteninhabers an die Bank (nachfolgend als »Vorgänge« bezeichnet) eingesetzt. Informationen über die Handhabung von 3D-Secure finden Sie im Internet unter https://www.bw-bank.de.

1. Registrierung für das BW-Secure-Verfahren

Wenn der Karteninhaber sich nicht gem. den nachfolgenden Ziffern für das BW-Secure-Verfahren – entweder über die BW-Secure-App oder SMS-mTAN – registriert, können Transaktionen bei Händlern, die 3D-Secure fordern, nicht durchgeführt werden. Gleiches gilt für Vorgänge, die eine Identifikation des Karteninhabers erfordern. Die Registrierung für das BW-Secure-Verfahren erfolgt durch Anmeldung auf der Webseite https://sicheres-bezahlen.bw-bank.de/.

1.1 BW-Secure-App:

Für die Erstregistrierung benötigt der Karteninhaber ein sog. Einmal-Passwort (OTP), welches ihm auf sicherem Weg, z. B. per Post, bereitgestellt wird. Mit diesem Passwort belegt er eindeutig seine Identität. Nach der Verwendung ist das Passwort ungültig. Im Rahmen der Registrierung über die oben unter 1. genannte Webseite lädt der Karteninhaber die BW-Secure-App auf sein Smartphone, Tablet etc. (nachfolgend »Mobilgerät« genannt) herunter und verbindet diese durch Scannen des bei der Registrierung angezeigten QR-Codes mit seiner Kredit-/Debitkartennummer. Bei künftigen 3D-Secure-Transaktionen erhält der Karteninhaber auf seinem Mobilgerät die Aufforderung, die Transaktion freizugeben oder abzulehnen. Gleiches gilt für Vorgänge, die eine Identifikation des Karteninhabers erfordern. Wenn der Karteninhaber die BW-Secure-App nutzt und sein Mobilgerät wechselt oder weitere Geräte hinzufügen möchte, kann er das neue Gerät über die Geräteverwaltung im BW Secure Portal hinzufügen und alte Geräte löschen. Sollte dem Kunden kein Zugriff mehr auf das Portal möglich sein, ist die oben beschriebene Erstregistrierung mit Einmal-Passwort erneut durchzuführen. Hierzu wird ihm nach Anforderung ein neues Einmal-Passwort auf sicherem Weg zugesendet. Es können maximal 5 Geräte gleichzeitig für eine Kredit-/Debitkarte aktiviert werden. Die Deaktivierung des BW-Secure-Verfahrens für eine registrierte Kredit-/Debitkarte erfolgt durch die Löschung aller aktivierten Geräte bei Nutzung der BW-Secure-App über die Geräteverwaltung im BW Secure Portal: https://sicheres-bezahlen.bw-bank.de/

1.2 SMS-mTAN:

Für die Erstregistrierung benötigt der Karteninhaber ein sog. Einmal-Passwort (OTP), welches ihm auf sicherem Weg, z. B. per Post, bereitgestellt wird. Mit diesem Passwort belegt er eindeutig seine Identität. Nach der Verwendung ist das Passwort ungültig. Die Einrichtung der Mobilfunkrufnummer und des statischen Passwortes erfolgt im Rahmen der Registrierung auf der oben unter 1. genannten Webseite. Bei zukünftigen 3D-Secure-Transaktionen erhält der Karteninhaber eine SMS mit einer mTAN auf die hinterlegte Rufnummer und bestätigt die Transaktion durch Eingabe des statischen Passwortes und der für diesen Vorgang erhaltenen mTAN. Gleiches gilt für Vorgänge, die eine Identifikation des Karteninhabers erfordern. Bei Nutzung des SMS-mTAN-Verfahrens muss bei Wechsel der Mobilfunknummer die neue Rufnummer im BW Secure Portal hinterlegt werden. Hier kann auch das statische Passwort geändert werden. Sollte dem Kunden kein Zugriff mehr auf das Portal möglich sein, ist eine wie oben beschriebene erneute Erstregistrierung erforderlich. Hierzu wird ihm nach Anforderung ein neues Einmal-Passwort auf sicherem Weg zugesendet. Die Deaktivierung des BW-Secure-Verfahrens für eine registrierte Kredit-/Debitkarte erfolgt durch die Löschung der Mobilfunknummer im BW Secure Portal: https://sicheres-bezahlen.bw-bank.de/

2. Informationen zur BW-Secure-App und zur SMS-mTAN

2.1 Auf der unter 1. genannten Webseite steht dem Karteninhaber eine Schritt-für-Schritt-Anleitung und ein Erklär-Video für die Registrierung und Aktivierung der BW-Secure-App und der SMS-mTAN zur Verfügung.

2.2 Die Registrierung für das BW-Secure-Verfahren erfolgt über eine verschlüsselte Internetverbindung. Bei der Registrierung und Nutzung des BW Secure Internetportals können Gebühren für die Inanspruchnahme einer Internetverbindung anfallen. Gleiches gilt bei Herunterladen und Nutzung der BW-Secure-App. Bei Nutzung des SMS-mTAN-Verfahrens können Gebühren für die Inanspruchnahme des Mobilfunknetzes anfallen.

2.3. Wir weisen hiermit darauf hin, dass durch die Registrierung und Nutzung der BW-Secure-App Dritte (z. B. Apple Inc. oder Google Inc.) auf eine bestehende Kredit-/Debitkarteninhaberbeziehung mit der Bank schließen können.

2.4. Wir weisen des Weiteren darauf hin, dass bei der Registrierung und Nutzung der BW-Secure-App Daten (z. B. Registrierungscode, Informationen über den Händler, Transaktionsbetrag usw.) über das Internet transportiert werden. Hierbei werden die Datenpakete (außer Absender und Empfänger) verschlüsselt übermittelt. Dritte können auf bestehende Geschäftsbeziehungen schließen. Die Datenübermittlung kann im Internet über Drittstaaten erfolgen, auch wenn Absender und Empfänger im selben Land angesiedelt sind.

3. Karteneinsatz und Autorisierung

Durch die Freigabe einer Transaktion über die BW-Secure-App oder Freigabe mit SMS-mTAN und statischem Passwort gelten Transaktionen gem. den Bedingungen für die Mastercard/Visa Card (je nach Produkt Kreditkarte oder Debitkarte) der Bank als vom Karteninhaber autorisiert. Gleiches gilt für die Freigabe von Vorgängen an die Bank.

4. Pflichten des Kunden und der Bank

a) BW-Secure-App: Unverzügliche Meldung an die Bank, wenn auf dem Mobilgerät die Aufforderung zur Genehmigung einer Transaktion oder von Vorgängen erscheint, die der Karteninhaber nicht getätigt hat. SMS-mTAN: Unverzügliche Meldung an die Bank, wenn eine mTAN per SMS zugestellt wird, obwohl kein Vorgang vom Karteninhaber gestartet wurde. Die Meldung kann bei beiden Verfahren auch rund um die Uhr direkt an den Karten-Service erfolgen (Telefonnummer siehe Rückseite der Kredit-/Debitkarte).

b) Keine Weitergabe des persönlichen Einmal-Passwortes an Dritte.

c) Eingabe des Einmal-Passwortes nur auf der Webseite https://sicheres-bezahlen.bw-bank.de/.
d) Die Bank wird den Karteninhaber weder per E-Mail noch telefonisch zur (erneuten) Registrierung oder Bekanntgabe seiner Registrierungsdaten auffordern.
e) Das Mobilgerät, mit welchem die SMS-mTAN empfangen wird oder mit dem über die BW-Secure-App die Freigabe (Autorisierung) der Kredit-/Debitkartenzahlung bzw. des Vorgangs erfolgt, darf nicht gleichzeitig für die Online-Kartenzahlung genutzt werden (physische Trennung der Kommunikationskanäle).
f) Der Karteninhaber hat die ihm von der Bank mittels des BW-Secure-Verfahrens übermittelten Transaktionsdaten auf Übereinstimmung mit den von ihm für die Online-Kartenzahlung vorgesehenen Daten abzugleichen. Bei Unstimmigkeiten ist die Kredit-/Debitkartenzahlung abzubrechen und die Bank zu informieren.

5. Verfügbarkeit des Verfahrens

Die Bank leistet keine Gewähr für die ständige Verfügbarkeit des BW-Secure-Verfahrens und haftet nicht für Schäden infolge von Störungen, Unterbrechungen (inkl. systembedingter Wartungsarbeiten) oder Überlastungen der beteiligten IT- oder Mobilfunk-Systeme. Die Bank übernimmt außerdem keine Haftung bei Manipulationen des mobilen Endgeräts bzw. dessen Software (wie insbesondere dem sog. »Jailbreak« oder »Rooten« bzw. der Installation von vom Hersteller nicht freigegebener Betriebssystemvarianten). Die BW-Secure-App wird von der Bank herausgegeben. Die Bank kann weder den störungsfreien noch den ununterbrochenen Zugang zur BW-Secure-App gewährleisten.

6. Haftung

6.1 Die Haftung der Bank – auch bei Verschulden ihrer Vertreter bzw. Erfüllungsgehilfen – ist auf Vorsatz und grobe Fahrlässigkeit beschränkt.

6.2 Die Bank haftet nicht für den Fall, dass das durch den Karteninhaber genutzte Endgerät verloren, gestohlen oder weitergegeben wird und dadurch Dritte ggf. Zugriff auf die App und das Sicherheitsmerkmal erhalten und diese unberechtigt nutzen können.

6.3 Die Bank leistet keine Gewähr für die jederzeitige Verfügbarkeit von 3D-Secure.

6.4 Außerdem haftet sie nicht für Schäden, die von dritter Seite oder durch höhere Gewalt verursacht worden sind, insbesondere durch Systemausfall oder -fehler, Störungen, Unterbrechungen (inkl. systembedingter Wartungsarbeiten), es sei denn, die Drittverursachung ist ihr zuzurechnen.

6.5 Die in diesen Bedingungen genannten Haftungsbeschränkungen bzw. Haftungsausschlüsse gelten nicht

- bei vorsätzlicher oder grob fahrlässiger Pflichtverletzung durch die Bank,
- im Falle der Übernahme einer Garantie für die Beschaffenheit oder das Vorhandensein eines Leistungserfolges oder der Übernahme eines Beschaffungsrisikos durch die Bank,
- bei schuldhafter Verletzung wesentlicher Vertragspflichten durch die Bank; wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung dieser Vereinbarung überhaupt erst ermöglichen und auf deren Einhaltung die jeweils gegnerische Partei regelmäßig vertrauen darf. Im Falle der Verletzung wesentlicher Vertragspflichten ist die Haftung der Bank dem Umfang nach auf den bei Vertragsschluss vorhersehbaren Schaden beschränkt,
- für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit durch die Bank,
- im Falle des Verzugs seitens der Bank, soweit ein fixierter Liefertermin mit der Bank vereinbart wurde, oder
- bei der Verwirklichung gesetzlich zwingender Haftungstatbestände durch die Bank, z. B. aus Produkthaftungsgesetz.

6.6 Die Haftungsbestimmungen des zugrunde liegenden Kredit-/Debitkartenverhältnisses gelten im Übrigen unverändert.

7. Änderung dieser Bedingungen; Kündigung

7.1 Änderungsangebot

Änderungen dieser Bedingungen werden dem Karteninhaber spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform angeboten. Hat der Karteninhaber mit der Bank einen elektronischen Kommunikationsweg vereinbart, können die Änderungen auch auf diesem Wege angeboten werden.

7.2 Annahme durch den Karteninhaber

Die von der Bank angebotenen Änderungen werden nur wirksam, wenn der Karteninhaber diese annimmt, gegebenenfalls im Wege der nachfolgend geregelten Zustimmungsfiktion.

7.3 Annahme durch den Karteninhaber im Wege der Zustimmungsfiktion

Das Schweigen des Karteninhabers gilt nur dann als Annahme des Änderungsangebots (Zustimmungsfiktion), wenn

(1) das Änderungsangebot der Bank erfolgt, um die Übereinstimmung der vertraglichen Bestimmungen mit einer veränderten Rechtslage wiederherzustellen, weil eine Bestimmung dieser Bedingungen

- aufgrund einer Änderung von Gesetzen, einschließlich unmittelbar geltender Rechtsvorschriften der Europäischen Union, nicht mehr der Rechtslage entspricht oder
- durch eine rechtskräftige gerichtliche Entscheidung, auch durch ein Gericht erster Instanz, unwirksam wird oder nicht mehr verwendet werden darf oder
- aufgrund einer verbindlichen Verfügung einer für die Bank zuständigen nationalen oder internationalen Behörde (z. B. der Bundesanstalt für Finanzdienstleistungsaufsicht oder der Europäischen Zentralbank) nicht mehr mit den aufsichtsrechtlichen Verpflichtungen der Bank in Einklang zu bringen ist und

(2) der Karteninhaber das Änderungsangebot der Bank nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen abgelehnt hat. Die Bank wird den Karteninhaber im Änderungsangebot auf die Folgen seines Schweigens hinweisen.

7.4 Ausschluss der Zustimmungsfiktion

Die Zustimmungsfiktion findet keine Anwendung

- bei Änderungen dieser Regelungen in Ziff. 7 oder
- bei Änderungen, die die Hauptleistungspflichten des Vertrages und die Entgelte für Hauptleistungen betreffen, oder
- bei Änderungen von Entgelten, die auf eine über das vereinbarte Entgelt für die Hauptleistung hinausgehende Zahlung des Verbrauchers gerichtet sind, oder
- bei Änderungen, die dem Abschluss eines neuen Vertrages gleichkommen, oder
- bei Änderungen, die das bisher vereinbarte Verhältnis von Leistung und Gegenleistung erheblich zugunsten der Bank verschieben würden.

In diesen Fällen wird die Bank die Zustimmung des Karteninhabers zu den Änderungen auf andere Weise einholen.

7.5 Kündigungsrecht des Karteninhabers bei der Zustimmungsfiktion

Macht die Bank von der Zustimmungsfiktion Gebrauch, kann der Karteninhaber diese Geschäftsbeziehung vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen auch fristlos und kostenfrei kündigen. Auf dieses Kündigungsrecht wird ihn die Bank in ihrem Angebot besonders hinweisen.

7.6 Der Karteninhaber kann jederzeit die Vereinbarung über die Benutzung des BW-Secure-Verfahrens kündigen, indem er die Registrierung aller Geräte im BW Secure Portal unter »Geräteverwaltung« oder seine Mobilfunknummer löscht.

7.7 Die Bank kann die Vereinbarung über die Benutzung des BW-Secure-Verfahrens mit einer Frist von zwei Monaten kündigen.

7.8 Nach erfolgter Kündigung ist eine Online-Kartenzahlungen bei Kartenakzeptanzstellen, die eine Authentifizierung über Visa Secure und MasterCard® Identity Check™ erwarten, nicht mehr möglich. Um die Kredit-/Debitkarte bei diesen Kartenakzeptanzstellen einsetzen zu können, ist eine Neuregistrierung für das BW-Secure-Verfahren erforderlich.

Bedingungen für die *Corporate*World Mastercard (Kreditkarte).

BW BANK
Ein Unternehmen der LBBW-Gruppe

Fassung: Oktober 2021

1. Ausgabe der Kreditkarte
Die von der Bank ausgegebene *Corporate*World Mastercard ist eine Kreditkarte (nachfolgend Kreditkarte genannt). Die Kreditkarte kann als physische Karte und zusätzlich als digitale Karte zur Speicherung auf einem Telekommunikations-, Digital- oder IT-Gerät (mobiles Endgerät) ausgegeben werden. Diese Kundenbedingungen gelten für beide Kartenformen gleichermaßen, es sei denn, es ist ausdrücklich etwas anderes geregelt. Für die digitale Kreditkarte gelten ergänzend die Nutzungsvoraussetzungen und Hinweise für die digitale Kreditkarte.

2. Verwendungsmöglichkeiten und Leistungen
Die *Corporate*World Mastercard (nachfolgend Kreditkarte) wird dem Kreditkarteninhaber aufgrund eines Abkommens zwischen der BW-Bank (nachfolgend Bank) und seinem Arbeitgeber zur Verfügung gestellt. Die Bank gibt die Kreditkarte dabei nach Maßgabe der nachfolgenden Bedingungen an den Kreditkarteninhaber aus. Werden die Salden der vom Kreditkarteninhaber mit der Kreditkarte getätigten Kartenverfügungen, der Kartenjahrespreis sowie sonstige mit der Karte in Verbindung stehende Entgelte von einem Girokonto des Arbeitgebers abgebucht, so ist die Karte durch den Kreditkarteninhaber ausschließlich für dienstliche/geschäftliche Zwecke zu nutzen. Werden die Salden der vom Kreditkarteninhaber mit der Kreditkarte getätigten Kartenverfügungen, der Kartenjahrespreis sowie sonstige mit der Karte in Verbindung stehende Entgelte von einem Girokonto des Kreditkarteninhabers abgebucht, so ist die Nutzung der Kreditkarte für den Kreditkarteninhaber im Verhältnis zur Bank nicht zweckgebunden. Aus Vereinbarungen zwischen dem Kreditkarteninhaber und dessen Arbeitgeber können sich eingeschränkte Nutzungszwecke bezüglich der Kreditkarte ergeben.
Für selbständige natürliche Personen ist die Nutzung der Kreditkarte auf dienstliche/geschäftliche Zwecke begrenzt. Dabei werden die Salden der mit der Kreditkarte getätigten Kartenverfügungen, der Kartenjahrespreis sowie sonstige mit der Karte in Verbindung stehende Entgelte von einem Geschäftsgirokonto der selbständigen natürlichen Person abgebucht.
Der Karteninhaber kann die von der Bank ausgegebenen Kreditkarten, soweit diese und die Akzeptanzstellen entsprechend ausgestattet sind, für folgende Zahlungsdienste nutzen: Mit der Kreditkarte kann der Karteninhaber im Inland – und als weitere Dienstleistung auch im Ausland – im Mastercard-Verbund bei Vertragsunternehmen Waren und Dienstleistungen bargeldlos bezahlen und zusätzlich im Rahmen des Bargeldservices an Geldautomaten Bargeldauszahlungen vornehmen. Die Vertragsunternehmen und die Geldautomaten im Rahmen des Bargeldservices sind an den Akzeptanzsymbolen zu erkennen, die auf der Kreditkarte zu sehen sind. Die Bank behält sich das Recht vor, dem Karteninhaber eine Kreditkarte auf Guthabenbasis auszustellen. Soweit mit der Kreditkarte zusätzliche Leistungen (z. B. Versicherungen) verbunden sind, wird der Karteninhaber hierüber gesondert informiert. Die Bank bietet im Zusammenhang mit der Kreditkarte außerdem zusätzliche Dienstleistungen an oder vermittelt solche, insoweit sind Änderungen jederzeit ohne Zustimmung des Karteninhabers möglich.
Zusätzlich wird die Bank über Mastercard/Visa teilnehmenden Akzeptanzstellen, bei welchen der Karteninhaber zuvor Waren oder Dienstleistungen mit der Kreditkarte bezahlt hat, aktualisierte Kartendaten (die letzten vier Ziffern der Kartennummer und das Ablaufdatum) zur Verfügung stellen (Aktualisierungsservice), um z. B. Zahlungen für wiederkehrende Dienstleistungen und im Online-Handel auch nach einer Aktualisierung der Kartendaten automatisch zu ermöglichen.

3. Personalisiertes Sicherheitsmerkmal
3.1 Für die Nutzung an Geldautomaten und an automatisierten Kassen kann dem Karteninhaber für seine Kreditkarte eine persönliche Geheimzahl (PIN) als personalisiertes Sicherheitsmerkmal zur Verfügung gestellt werden.
3.2 Die Kreditkarte kann an Geldautomaten sowie an automatisierten Kassen, an denen im Zusammenhang mit der Verwendung der Kreditkarte die PIN eingegeben werden muss, nicht mehr eingesetzt werden, wenn die persönliche Geheimzahl dreimal hintereinander mit einer oder beiden Kartenformen falsch eingegeben wurde. Der Karteninhaber sollte sich in diesem Fall mit der Bank, möglichst mit der kontoführenden Stelle, in Verbindung setzen.

4. Verfügungsrahmen
Der Karteninhaber darf seine Kreditkarte nur innerhalb des vereinbarten monatlichen Verfügungsrahmens (zzgl. eines etwaigen Guthabens auf dem Kartenkonto) und nur in der Weise nutzen, dass ein Ausgleich der Kartenumsätze bei Fälligkeit gewährleistet ist (finanzielle Nutzungsgrenze). Innerhalb dieses Rahmens gilt für den Bargeldservice das im Preis- und Leistungsverzeichnis ausgewiesene tägliche Verfügungslimit. Der Karteninhaber/die Firma kann mit der Bank eine Änderung des Verfügungsrahmens vereinbaren. Die Bank ist berechtigt, den mitgeteilten Verfügungsrahmen mit einer Ankündigungsfrist von einem Monat nach billigem Ermessen (§ 315 BGB) zu reduzieren.

5. Autorisierung von Zahlungsaufträgen
5.1 Mit dem Einsatz der Kreditkarte erteilt der Karteninhaber die Zustimmung (Autorisierung) zur Ausführung des Zahlungsauftrags. Hierzu hat der Karteninhaber entweder
- an Geldautomaten die PIN einzugeben oder
- an automatisierten Kassen bei Vertragsunternehmen die PIN einzugeben oder – soweit erforderlich – bei Vertragsunternehmen die Unterschrift zu leisten oder
- an automatisierten Kassen die kontaktlose Bezahlfunktion mit PIN zu nutzen, indem die Kreditkarte vor das Empfangsgerät des Vertragshändlers gehalten wird. Der kontaktlose Einsatz der Kreditkarte an automatisierten Kassen kann bis maximal 50 EUR pro Bezahlvorgang ohne Eingabe der PIN erfolgen, soweit an den automatisierten Kassen für den jeweiligen kontaktlosen Einsatz nicht die Eingabe der PIN verlangt wird. Soweit für die Autorisierung zusätzlich eine PIN oder die Unterschrift erforderlich ist, erfolgt die Autorisierung erst mit deren Einsatz; oder
- bei elektronischen Fernzahlungsvorgängen über das Internet gegenüber Vertragsunternehmen die geforderten Kartendaten einzugeben. Soweit dabei besondere Authentifizierungsverfahren gefordert werden, sind diese zu nutzen. Weitere Informationen über die von der Bank unterstützten Authentifizierungsverfahren und Hinweise zum Bezahlen im Internet sind in den Geschäftsräumen der Bank verfügbar sowie auf deren Internetseiten abrufbar; oder
- gegenüber Vertragsunternehmen die geforderten Kartendaten anzugeben (z. B. am Telefon).

5.2 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.
5.3 Nach Erteilung der Zustimmung kann der Karteninhaber den Zahlungsauftrag nicht mehr widerrufen.

6. Ablehnung von Zahlungsaufträgen durch die Bank
Die Bank ist berechtigt, den Zahlungsauftrag abzulehnen, wenn
- der Karteninhaber die Autorisierung des Zahlungsauftrags nicht gemäß Nummer 5.1 erteilt hat,
- der für den Zahlungsauftrag geltende Verfügungsrahmen oder die finanzielle Nutzungsgrenze nicht eingehalten wurde oder
- die Kreditkarte gesperrt ist.

Hierüber wird der Karteninhaber während des Bezahlvorgangs bzw. über das Terminal, an dem die Karte eingesetzt wird, unterrichtet.

7. Sperrung eines verfügbaren Geldbetrags
Die Bank ist berechtigt, einen im Rahmen der finanziellen Nutzungsgrenze (Nummer 4) verfügbaren Geldbetrag auf dem Kreditkartenkonto des Karteninhabers zu sperren, wenn
- der Zahlungsvorgang vom Zahlungsempfänger ausgelöst worden ist und
- der Karteninhaber auch der genauen Höhe des zu sperrenden Geldbetrags zugestimmt hat.

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

8. Zahlungsverpflichtung des Karteninhabers
8.1 Die Bank wird die bei der Nutzung der Kreditkarte entstandenen sofort fälligen Forderungen der Vertragsunternehmen gegen den Karteninhaber bezahlen. Der Karteninhaber ist seinerseits verpflichtet, der Bank diese Forderungsbeträge zu erstatten. Entsprechendes gilt für im Rahmen des Bargeldservices entstandene Forderungen. Auch wenn der Karteninhaber die finanzielle Nutzungsgrenze bei seinen Zahlungsaufträgen nicht einhält, ist die Bank berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung der Kreditkarte entstehen. Die Genehmigung einzelner Kartenumsätze führt weder zur Einräumung eines Kredits noch zur Erhöhung eines zuvor eingeräumten Kredits, sondern erfolgt in der Erwartung, dass ein Ausgleich der Kartenumsätze bei Fälligkeit gewährleistet ist.
8.2 Der Karteninhaber ermächtigt die Bank, fällige Zahlungen aus dem Kreditkartenverhältnis, insbesondere die geschuldeten Erstattungsleistungen und Entgelte, dem auf dem Kartenantrag angeführten Girokonto (Abrechnungskonto) zu belasten bzw. per Lastschrift einzuziehen. Der Karteninhaber hat dafür Sorge zu tragen, dass auf diesem Abrechnungskonto bei Einzug des jeweiligen Forderungsbetrages ausreichend Deckung besteht.

9. Kreditkartenabrechnung
9.1 Mit der Kreditkarte ausgelöste Zahlungsaufträge werden sofort mit etwaigem Guthaben auf dem Kreditkartenkonto verrechnet (vgl. Nummer 10). Die Kreditkartenabrechnung über die mit der Karte ausgelösten Zahlungsaufträge, die anfallenden Entgelte sowie die sonstigen Umsätze im Zusammenhang mit der Kreditkarte erfolgt in der mit dem Karteninhaber/der Firma vereinbarten Weise (z. B. Abrechnung über das elektronische Postfach) einmal im Monat zum vereinbarten Abrechnungsstichtag (Rechnungsperiode). Für Kreditkarten mit Abrechnung über das Firmenkonto erhält die Firma die Kreditkartenabrechnung auf dem Postweg, es sei denn, mit der Firma wurde der Versand in ein elektronisches Postfach vereinbart. Mit erteilter Kreditkartenabrechnung wird der darin ausgewiesene Forderungsbetrag sofort fällig. Dieser Betrag wird dem vom Karteninhaber/von der Firma angegebenen Abrechnungskonto zum vereinbarten Zeitpunkt belastet. Wenn der Karteninhaber/die Firma die Abrechnung in der vereinbarten Weise nicht innerhalb der vereinbarten Frist abgerufen hat, kann zeitnah eine papierhafte Abrechnung erfolgen und dem Karteninhaber/der Firma gegen Portoersatz zugesandt werden. Der Karteninhaber/die Firma hat die Kreditkartenabrechnung unverzüglich auf nicht autorisierte oder fehlerhaft ausgeführte Kartenverfügungen zu überprüfen.
9.2 Besonderheiten zu *Corporate*World RechnungOnline: Sofern der Karteninhaber die elektronische Rechnung (Online-Rechnung) erhält, erhält er keine Papier-Sammelabrechnung. Der Karteninhaber ist verpflichtet, eine gültige E-Mail-Adresse zur Benachrichtigung über Rechnungseingänge in der Anwendung zu hinterlegen und umgehend nach Eingang einer Benachrichtigung, mindestens jedoch einmal monatlich, die im Onlinearchiv eingehenden Sammelabrechnungen zu prüfen. Sofern die Abrechnung vom Karteninhaber nicht innerhalb der vereinbarten Frist abgerufen wird, kann zeitnah eine papierhafte Abrechnung erfolgen und dem Karteninhaber gegen Portoersatz zugesandt werden. Der Karteninhaber kann über *Corporate*World RechnungOnline auch Informationen der Bank abrufen. Für die Nutzung des elektronischen Archivs erhält der Karteninhaber ein gesondertes Online-Passwort. Dieses ist beim erstmaligen Zugang zu ändern. Der Karteninhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von dem Online-Passwort erlangt, und hat beim Verdacht einer missbräuchlichen Nutzung unverzüglich dieses zu ändern oder die Bank zu unterrichten. Bei dreimaliger Falscheingabe des Online-Passworts sperrt die Bank automatisch den Zugang zu *Corporate*World RechnungOnline.
9.3 Prenotification (Vorankündigung des Lastschrifteinzugs) gemäß SEPA – Verkürzung der Vorlauffrist: Über die monatliche Kreditkartenabrechnung erhält der Karteninhaber/die Firma die Prenotification gemäß SEPA. Die Kartenabrechnung mit der Prenotification wird dem Karteninhaber/der Firma mindestens 4 Geschäftstage vor Vornahme der Belastungsbuchung zugehen. Handelt es sich bei der im Kartenantrag angegebenen Bankverbindung um ein Girokonto bei der BW-Bank, so bucht die BW-Bank von diesem Konto die im Zusammenhang mit der hier genannten Kreditkarte geschuldete Zahlungen ab. Die Erteilung eines SEPA-Mandats ist für den vorgenannten Fall nicht notwendig, es erfolgt auch keine Prenotification.
9.4 Wenn es sich bei dem Abrechnungskonto um ein Girokonto des Karteninhabers handelt, hat dieser dafür Sorge zu tragen, dass auf seinem Abrechnungskonto bei Einzug des jeweiligen Forderungsbetrags ausreichend Deckung besteht. Entsprechendes gilt für die Firma bei Abrechnung über ein Firmenkonto.

10. Guthaben
10.1 Der Karteninhaber kann auf seinem Kartenkonto Guthaben bis zu einer Grenze von 25.000 EUR bilden. Das jeweilige Guthaben auf dem Kartenkonto wird nicht verzinst und ist – je nach Kartenart – Privatvermögen bzw. Firmenvermögen. Das Kartenkonto darf nicht für den allgemeinen Zahlungsverkehr herangezogen werden.

10.2 Die der Bank aufgrund der Benutzung der Kreditkarte gegen den Karteninhaber zustehenden Zahlungsansprüche und Entgelte sowie die vom Karteninhaber auf das Kreditkartenkonto geleisteten Zahlungen werden auf dem Kreditkartenkonto in laufende Rechnung eingestellt. Die Kreditkartenabrechnung ist gleichzeitig der Rechnungsabschluss. Die Haftung nach Nummer 13.1.5 erhöht sich um das jeweils auf dem Kreditkartenkonto vorhandene Guthaben. Die auf dem Kreditkartenkonto gebuchten Kartenverfügungen werden mit etwaigem Guthaben taggleich verrechnet. Übersteigen diese Kartenverfügungen das Guthaben, wird der Differenzbetrag zum Abrechnungsstichtag dem vom Karteninhaber angegebenen Abrechnungskonto belas tet. Über ein Guthaben auf dem Kreditkartenkonto kann auch durch Überweisung auf das Abrechnungskonto verfügt werden.

11. Sorgfalts- und Mitwirkungspflichten des Karteninhabers

11.1 Unterschrift

Der Karteninhaber hat die physische Kreditkarte nach Erhalt unverzüglich auf dem Unterschriftsfeld zu unterschreiben.

11.2 Sorgfältige Aufbewahrung und Sicherung der Kreditkarte

11.2.1 Die Kreditkarte ist mit besonderer Sorgfalt aufzubewahren, um zu verhindern, dass sie abhanden kommt und missbräuchlich verwendet wird (z. B. um Transaktionen an automatisierten Kassen ohne PIN bis zur Sperre zu tätigen). Sie darf insbesondere auch nicht unbeaufsichtigt im Kraftfahrzeug aufbewahrt werden.

11.2.2 Soweit technisch möglich, soll der Karteninhaber den Zugang zu seinem mobilen Endgerät mit einer für das mobile Endgerät bestimmten persönlichen Geheimzahl (Endgeräte-PIN) oder auf andere geeignete Weise (z. B. durch Fingerabdruck) sichern.

11.3 Geheimhaltung der persönlichen Geheimzahl (PIN)

Der Karteninhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von seiner PIN erlangt. Die PIN darf insbesondere nicht auf der physischen Kreditkarte vermerkt, bei einer digitalen Kreditkarte nicht in dem mobilen Endgerät gespeichert werden, das für die Nutzung der digitalen Kreditkarte erforderlich ist, oder in anderer Weise zusammen mit der Kreditkarte aufbewahrt werden. Denn jede Person, die die PIN kennt und in den Besitz der Kreditkarte bzw. des mobilen Endgeräts, auf dem die digitale Kreditkarte gespeichert ist, kommt, hat die Möglichkeit, zusammen mit der PIN und der Kreditkarte missbräuchliche Kartenverfügungen zu tätigen (z. B. Bargeldabhebung am Geldautomat vorzunehmen). Sofern der Karteninhaber eine digitale Kreditkarte nutzt und der Zugriff auf das mobile Endgerät durch eine vom Karteninhaber wählbare Endgeräte-PIN abgesichert werden kann, darf der Karteninhaber zur Absicherung des Zugriffs nicht dieselbe PIN verwenden, die für die Nutzung der digitalen Kreditkarte erforderlich ist.

11.4 Anzeige-, Prüfungs- und Unterrichtungspflichten des Karteninhabers

11.4.1 Stellt der Karteninhaber den Verlust oder Diebstahl seiner Kreditkarte oder des mobilen Endgeräts mit digitaler Kreditkarte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung der Kreditkarte, Kartendaten oder PIN fest, hat er die Bank (Telefon 069 6657-1333) unverzüglich zu unterrichten (Sperranzeige). Der Karteninhaber hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei anzuzeigen. Im Notfall kann eine Ersatzkarte (emergency card) binnen 48 Stunden zur Verfügung gestellt werden. Für die Ausstellung einer emergency card für Kreditkarten fallen jeweils die im Preis- und Leistungsverzeichnis angegebenen Kosten an.

11.4.2 Durch die Sperre der digitalen Kreditkarte bei der Bank bzw. dem Zentralen Sperrannahmedienst wird nicht der Zugang zum mobilen Endgerät gesperrt. Eine Sperrung der sonstigen Funktionen auf dem mobilen Endgerät kann nur gegenüber dem jeweiligen Anbieter dieser Funktionen erfolgen.

11.4.3 Bei Nutzung besonderer Authentifizierungsverfahren gemäß Nummer 5.1 hat der Karteninhaber vor der Autorisierung die Übereinstimmung der zur Authentifizierung übermittelten Transaktionsdaten (z. B. Zahlbetrag, Datum) mit den für die Transaktion vorgesehenen Daten abzugleichen. Bei Feststellung von Abweichungen ist die Transaktion abzubrechen und der Verdacht auf missbräuchliche Verwendung der Bank anzuzeigen.

11.4.4 Hat der Karteninhaber den Verdacht, dass eine andere Person unberechtigt in den Besitz seiner Kreditkarte gelangt ist, eine missbräuchliche Verwendung oder eine sonstige, nicht autorisierte Nutzung von Kreditkarte, der Kartendaten oder der PIN vorliegt, muss er ebenfalls unverzüglich eine Sperranzeige abgeben.

12. Reklamationen und Beanstandungen

Der Karteninhaber hat die Bank unverzüglich nach Feststellung einer nicht autorisierten oder fehlerhaft ausgeführten Kartenverfügung zu unterrichten. Reklamationen und Beanstandungen aus dem Vertragsverhältnis zwischen dem Karteninhaber und dem Vertragsunternehmen sind unmittelbar zwischen diesen zu klären; sie berühren nicht die Zahlungsverpflichtung des Karteninhabers. Die Rechte des Karteninhabers nach Nummer 16 dieser Bedingungen bleiben unberührt.

13. Haftung des Karteninhabers für nicht autorisierte Kartenverfügungen

13.1 Haftung des Karteninhabers bis zur Sperranzeige

13.1.1 Verliert der Karteninhaber seine Kreditkarte oder PIN, werden sie ihm gestohlen, kommen sie ihm in sonstiger Weise abhanden oder wird die Kreditkarte sonst missbräuchlich verwendet und kommt es dadurch zu einer nicht autorisierten Kartenverfügung, z. B. im Rahmen der

- Bargeldauszahlung an einem Geldautomaten,
- Verwendung der Kreditkarte an automatisierten Kassen von Vertragsunternehmen,
- Nutzung der Kreditkarte bei elektronischen Fernzahlungsvorgängen über das Internet,

haftet der Karteninhaber für Schäden, die bis zum Zeitpunkt der Sperranzeige verursacht werden, in Höhe von maximal 50 EUR. Die Haftung nach Nummer 13.1.5 für Vorsatz und grobe Fahrlässigkeit sowie für Handeln in betrügerischer Absicht bleibt unberührt.

13.1.2 Der Karteninhaber haftet nicht nach Nr. 13.1.1, wenn

- es dem Karteninhaber nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung der Kreditkarte vor der nicht autorisierten Kartenverfügung zu bemerken, oder
- der Verlust der Kreditkarte durch einen Angestellten, einen Agenten, eine Zweigstelle/ Zweigniederlassung der Bank oder eine sonstige Stelle, an die Tätigkeiten der Bank ausgelagert wurden, verursacht worden ist.

Die Haftung nach Nummer 13.1.5 für Vorsatz und grobe Fahrlässigkeit sowie für Handeln in betrügerischer Absicht bleibt unberührt.

13.1.3 Die Bank verzichtet auf die Schadensbeteiligung des Karteninhabers in Höhe von 50 EUR gemäß Nummer 13.1.1 und übernimmt alle Schäden, die durch die nicht autorisierte Kartenverfügung bis zum Eingang der Sperranzeige entstanden sind, wenn der Karteninhaber seine ihm obliegenden Sorgfalts- und Mitwirkungspflichten gemäß Nummer 11 nicht in betrügerischer Absicht, vorsätzlich oder grob fahrlässig verletzt hat. Eine Übernahme des vom Karteninhaber zu tragenden Schadens erfolgt nur, wenn der Karteninhaber die Voraussetzungen der Haftungsentlastung glaubhaft darlegt und Anzeige bei der Polizei erstattet.

13.1.4 Der Karteninhaber ist nicht zum Ersatz des Schadens nach Nummer 13.1.1 verpflichtet, wenn er die Sperranzeige nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

13.1.5 Kommt es vor der Sperranzeige zu einer nicht autorisierten Kartenverfügung und hat der Karteninhaber seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Karteninhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Karteninhabers kann insbesondere dann vorliegen, wenn er

- den Verlust, Diebstahl oder die missbräuchliche Kartenverfügung der Bank oder dem Sperrannahmedienst schuldhaft nicht unverzüglich mitgeteilt hat, nachdem er hiervon Kenntnis erlangt hat,
- die persönliche Geheimzahl auf der physischen Kreditkarte vermerkt oder zusammen mit der physischen Kreditkarte verwahrt hat,
- die persönliche Geheimzahl auf dem mobilen Endgerät gespeichert hat oder
- die persönliche Geheimzahl einer anderen Person mitgeteilt hat und der Missbrauch dadurch verursacht worden ist.

Die Haftung für Schäden, die innerhalb des Zeitraums verursacht werden, für den der Verfügungsrahmen gilt, beschränkt sich jeweils auf den für die Kreditkarte vereinbarten monatlichen Verfügungsrahmen. Für Schäden im Rahmen des Bargeldservices haftet der Karteninhaber pro Kalendertag maximal in Höhe des im Preis- und Leistungsverzeichnis ausgewiesenen täglichen Verfügungslimits, jedoch begrenzt auf den monatlichen Verfügungsrahmen.

13.1.6 Hat die Bank durch eine Verletzung ihrer Pflichten zur Entstehung des Schadens beigetragen, haftet sie für den entstandenen Schaden im Umfang des von ihr zu vertretenden Mitverschuldens.

13.1.7 Hat die Bank beim Einsatz der Kreditkarte eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz (ZAG) nicht verlangt oder hat der Zahlungsempfänger oder sein Zahlungsdienstleister diese nicht akzeptiert, obwohl die Bank nach § 55 ZAG gesetzlich zur starken Kundenauthentifizierung verpflichtet ist, bestimmt sich die Haftung des Karteninhabers und der Bank abweichend von den Nummern 13.1.1 bis 13.1.6 nach § 675v Abs. 4 des Bürgerlichen Gesetzbuches.

13.2 Haftung des Karteninhabers ab Sperranzeige

Sobald der Bank oder dem Sperrannahmedienst der Verlust oder Diebstahl der Kreditkarte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Kreditkarte oder PIN angezeigt wurde, übernimmt die Bank alle danach durch Kartenverfügungen entstehenden Schäden. Handelt der Karteninhaber in betrügerischer Absicht, trägt der Karteninhaber auch die nach der Sperranzeige entstehenden Schäden.

14. Erstattungs-, Berichtigungs-, und Schadensersatzansprüche des Karteninhabers

14.1 Erstattung bei nicht autorisierter Kartenverfügung

Im Falle einer nicht autorisierten Kartenverfügung hat die Bank gegen den Karteninhaber keinen Anspruch auf Erstattung ihrer Aufwendungen. Die Bank ist verpflichtet, dem Karteninhaber den Betrag ungekürzt zu erstatten. Wurde der Betrag dem Abrechnungskonto belastet, wird die Bank dieses wieder auf den Stand bringen, auf dem es sich ohne die Belastung durch die nicht autorisierte Kartenverfügung befunden hätte.

Diese Verpflichtungen sind unverzüglich, spätestens bis zum Ende des Geschäftstags gemäß Preis- und Leistungsverzeichnis zu erfüllen, der auf den Tag folgt, an welchem der Bank angezeigt wurde, dass die Kartenverfügung nicht autorisiert ist, oder die Bank auf andere Weise davon Kenntnis erhalten hat. Hat die Bank einer zuständigen Behörde berechtigte Gründe für den Verdacht, dass ein betrügerisches Verhalten des Kunden vorliegt, schriftlich mitgeteilt, hat sie ihre Verpflichtung aus Satz 2 unverzüglich zu prüfen und zu erfüllen, wenn sich der Betrugsverdacht nicht bestätigt.

14.2 Erstattung bei nicht erfolgter oder fehlerhafter Ausführung einer autorisierten Kartenverfügung

14.2.1 Im Falle einer nicht erfolgten oder fehlerhaften Ausführung einer autorisierten Kartenverfügung kann der Karteninhaber von der Bank die unverzügliche und ungekürzte Erstattung des Kartenverfügungsbetrags insoweit verlangen, als die Kartenverfügung nicht erfolgte oder fehlerhaft war. Wurde der Betrag dem Abrechnungskonto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne die nicht erfolgte oder fehlerhafte Kartenverfügung befunden hätte.

14.2.2 Der Karteninhaber kann über Nummer 14.2.1 hinaus von der Bank die Erstattung der Entgelte und Zinsen insoweit verlangen, als ihm diese im Zusammenhang mit der nicht erfolgten oder fehlerhaften Ausführung der autorisierten Kartenverfügung in Rechnung gestellt oder seinem Konto belastet wurden.

14.2.3 Besteht die fehlerhafte Ausführung darin, dass eine autorisierte Kartenverfügung beim Zahlungsdienstleister des Zahlungsempfängers erst nach Ablauf der im Preis- und Leistungsverzeichnis geregelten Ausführungsfrist eingeht (Verspätung), sind die Ansprüche des Karteninhabers nach Nummer 14.2.1 und 14.2.2 ausgeschlossen. Ist dem Karteninhaber durch die Verspätung ein Schaden entstanden, so haftet die Bank nach Nummer 14.3. Wurde eine autorisierte Kartenverfügung nicht oder fehlerhaft ausgeführt, wird die Bank die Kartenverfügung auf Verlangen des Karteninhabers nachvollziehen und ihn über das Ergebnis unterrichten.

14.3 Schadensersatzansprüche des Karteninhabers

Im Falle einer nicht autorisierten Kartenverfügung oder im Falle einer nicht erfolgten oder fehlerhaften Ausführung einer autorisierten Kartenverfügung kann der Karteninhaber von der Bank einen Schaden, der nicht bereits von Nummer 14.1 oder 14.2 erfasst ist, ersetzt verlangen. Dies gilt nicht, wenn die Bank die Pflichtverletzung nicht zu vertreten hat. Die Bank hat hierbei ein Verschulden, das einer zwischengeschalteten Stelle zur Last fällt, wie eigenes Verschulden zu vertreten, es sei denn, dass die wesentliche Ursache bei einer zwischengeschalteten Stelle liegt, die der Karteninhaber vorgegeben hat. Handelt es sich bei dem Karteninhaber nicht um einen Verbraucher oder erfolgt der Einsatz der Kreditkarte in einem Land außerhalb Deutschlands und des Europäischen Wirtschaftsraums (EWR) (Drittstaat) oder in einer Währung eines Staates außerhalb des EWR (Drittstaatwährungszahlung), beschränkt sich die Haftung der Bank für das Verschulden einer an der Abwicklung 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. Die Haftung nach Nummer 14.3 ist auf 12.500 EUR je Kartenzahlung begrenzt. Diese betragsmäßige Haftungsbeschränkung gilt nicht

- für nicht autorisierte Zahlungsvorgänge,
- bei Vorsatz oder grober Fahrlässigkeit der Bank,
- für Gefahren, die die Bank besonders übernommen hat, und
- für den dem Karteninhaber entstandenen Zinsschaden, soweit der Karteninhaber Verbraucher ist.

14.4 Einwendungsausschluss
14.4.1 Der Karteninhaber kann Ansprüche und Einwendungen nach Nummer 14.1 bis 14.3 nicht mehr geltend machen, wenn er diese nicht spätestens 13 Monate nach dem Tag der Belastungsbuchung auf dem Abrechnungskonto gegenüber der Bank angezeigt hat. Der Lauf der 13-monatigen Frist beginnt nur, wenn die Bank den Karteninhaber über die aus der Kartenverfügung resultierende Belastungsbuchung entsprechend dem für Kontoinformationen vereinbarten Weg spätestens innerhalb eines Monats nach der Belastungsbuchung unterrichtet hat; anderenfalls ist für den Fristbeginn der Tag der Unterrichtung über die Kreditkartenabrechnung maßgeblich. Ansprüche und Einwendungen nach Nummer 14.1 bis 14.3 kann der Karteninhaber auch nach Ablauf der vorgenannten Frist geltend machen, wenn er ohne Verschulden an der Einhaltung dieser Frist verhindert war.
14.4.2 Ansprüche des Karteninhabers gegen die Bank nach Nummer 14.1 bis 14.3 sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände
- auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das die Bank keinen Einfluss hat und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten verhindert werden können, oder
- von der Bank aufgrund einer gesetzlichen Verpflichtung herbeigeführt wurden.

15. Sperre und Einziehung der Kreditkarte durch die Bank
Die Bank darf die Kreditkarte sperren und den Einzug der Kreditkarte (z. B. an Geldautomaten) veranlassen bzw. die Löschung der digitalen Kreditkarte verlangen oder selbst veranlassen, wenn
- sie berechtigt ist, den Kreditkartenvertrag bzw. die Nutzung der digitalen Kreditkarte aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Kreditkarte dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Kreditkarte besteht.

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

16. Anspruch des Karteninhabers bei einer von dem Vertragsunternehmen ausgelösten autorisierten Kartenverfügung
Im Falle einer von dem Vertragsunternehmen ausgelösten autorisierten Kartenverfügung hat der Karteninhaber einen Anspruch auf Erstattung des belasteten Zahlungsbetrags, wenn
- bei der Autorisierung der genaue Betrag nicht angegeben wurde und
- der Zahlungsbetrag den Betrag übersteigt, den der Karteninhaber entsprechend seinem bisherigen Ausgabeverhalten, den Bedingungen des Kreditkartenvertrags und den jeweiligen Umständen des Einzelfalls hätte erwarten können; mit einem etwaigen Währungsumtausch zusammenhängende Gründe bleiben außer Betracht, wenn der vereinbarte Referenzwechselkurs zugrunde gelegt wurde.

Der Karteninhaber muss gegenüber der Bank die Sachumstände darlegen, mit denen er seinen Erstattungsanspruch begründet. Ein Anspruch des Karteninhabers auf Erstattung ist ausgeschlossen, wenn er ihn nicht innerhalb von acht Wochen ab dem Zeitpunkt des Ausweises der Belastung des betreffenden Zahlungsbetrags auf der Kreditkartenabrechnung gegenüber der Bank geltend macht.

17. Rückgabe und Austausch der Kreditkarte
Die Kreditkarte bleibt Eigentum der Bank. Sie ist nicht übertragbar. Die Kreditkarte ist nur für den angegebenen Zeitraum gültig. Mit Aushändigung der neuen, spätestens aber nach Ablauf der Gültigkeit der Kreditkarte ist die Bank berechtigt, die alte Kreditkarte zurückzuverlangen bzw. die Löschung der digitalen Kreditkarte zu verlangen oder selbst zu veranlassen. Endet die Nutzungsberechtigung der Kreditkarte in den ausgegebenen Kartenformen bzw. der digitalen Kreditkarte früher (z. B. durch Kündigung des Kreditkartenvertrags), hat der Karteninhaber die Kreditkarte unverzüglich an die Bank zurückzugeben bzw. die digitale Kreditkarte zu löschen. Die Bank behält sich das Recht vor, auch während der Laufzeit einer Kreditkarte diese gegen eine neue auszutauschen; Kosten entstehen dem Karteninhaber hierdurch nicht.

18. Fremdwährungsumrechnung beim Auslandseinsatz
Nutzt der Karteninhaber die Kreditkarte für Zahlungsaufträge, die nicht auf Euro lauten, wird das Kartenkonto gleichwohl in Euro belastet. Die Bestimmung des Kurses bei Fremdwährungsgeschäften ergibt sich aus dem Preis- und Leistungsverzeichnis. Eine Änderung des in der Umrechnungsregelung genannten Referenzwechselkurses wird unmittelbar und ohne vorherige Benachrichtigung des Karteninhabers wirksam.

19. Entgelte und deren Änderung
19.1 Die vom Karteninhaber gegenüber der Bank geschuldeten Entgelte ergeben sich aus dem Preis- und Leistungsverzeichnis der Bank.
Für den Ersatz einer verlorenen, gestohlenen, missbräuchlich verwendeten oder sonst nicht autorisiert genutzten Kreditkarte ist die Bank berechtigt, dem Karteninhaber im Rahmen des § 675l Absatz 1 des Bürgerlichen Gesetzbuches das im Preis- und Leistungsverzeichnis der Bank ausgewiesene Entgelt zu berechnen, sofern der Karteninhaber die Umstände, die zum Ersatz der Kreditkarte geführt haben, zu vertreten hat und die Bank nicht zur Ausstellung einer Ersatzkarte verpflichtet ist. Ob darüber hinaus Entgelte für den Ersatz einer Kreditkarte in anderen Fällen durch die Bank erhoben werden, können Sie dem Preis- und Leistungsverzeichnis der Bank entnehmen.
19.2 Änderungen dieser Entgelte werden dem Karteninhaber spätestens zwei Monate vor dem Zeitpunkt ihres Wirksamwerdens in Textform angeboten. Hat der Karteninhaber mit der Bank im Rahmen der Geschäftsbeziehung einen elektronischen Kommunikationsweg (z. B. das Elektronische Postfach) vereinbart, können die Änderungen auch auf diesem Wege angeboten werden.
Die von der Bank angebotenen Änderungen werden nur wirksam, wenn der Karteninhaber diese annimmt. Eine Vereinbarung über die Änderung eines Entgelts, das auf eine über die Hauptleistung hinausgehende Zahlung des Karteninhabers gerichtet ist, kann die Bank mit dem Karteninhaber nur ausdrücklich treffen. Die Änderung von Entgelten für den Zahlungsdiensterahmenvertrag (Girovertrag) richtet sich nach Nummer 17 Abs. 6 AGB. Bei Entgelten und deren Änderung für Karteninhaber, die nicht Verbraucher sind, verbleibt es bei der Regelung in Nummer 17 Abs. 2 AGB.

20. Änderung der Bedingungen
20.1 Änderungsangebot
Änderungen dieser Bedingungen werden dem Karteninhaber spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform angeboten. Hat der Karteninhaber mit der Bank einen elektronischen Kommunikationsweg vereinbart, können die Änderungen auch auf diesem Wege angeboten werden.
20.2 Annahme durch den Karteninhaber
Die von der Bank angebotenen Änderungen werden nur wirksam, wenn der Karteninhaber diese annimmt, gegebenenfalls im Wege der nachfolgend geregelten Zustimmungsfiktion.
20.3 Annahme durch den Karteninhaber im Wege der Zustimmungsfiktion
Das Schweigen des Karteninhabers gilt nur dann als Annahme des Änderungsangebots (Zustimmungsfiktion), wenn
(1) das Änderungsangebot der Sparkasse/Landesbank erfolgt, um die Übereinstimmung der vertraglichen Bestimmungen mit einer veränderten Rechtslage wiederherzustellen, weil eine Bestimmung dieser Bedingungen
- aufgrund einer Änderung von Gesetzen, einschließlich unmittelbar geltender Rechtsvorschriften der Europäischen Union, nicht mehr der Rechtslage entspricht oder
- durch eine rechtskräftige gerichtliche Entscheidung, auch durch ein Gericht erster Instanz, unwirksam wird oder nicht mehr verwendet werden darf oder
- aufgrund einer verbindlichen Verfügung einer für die Bank zuständigen nationalen oder internationalen Behörde (z. B. der Bundesanstalt für Finanzdienstleistungsaufsicht oder der Europäischen Zentralbank) nicht mehr mit den aufsichtsrechtlichen Verpflichtungen der Bank in Einklang zu bringen ist und

(2) der Karteninhaber das Änderungsangebot der Bank nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen abgelehnt hat. Die Bank wird den Karteninhaber im Änderungsangebot auf die Folgen seines Schweigens hinweisen.
20.4 Ausschluss der Zustimmungsfiktion
Die Zustimmungsfiktion findet keine Anwendung
- bei Änderungen dieser Regelungen in Ziff. 20 oder
- bei Änderungen, die die Hauptleistungspflichten des Vertrages und die Entgelte für Hauptleistungen betreffen, oder
- bei Änderungen von Entgelten, die auf eine über das vereinbarte Entgelt für die Hauptleistung hinausgehende Zahlung des Verbrauchers gerichtet sind, oder
- bei Änderungen, die dem Abschluss eines neuen Vertrages gleichkommen, oder
- bei Änderungen, die das bisher vereinbarte Verhältnis von Leistung und Gegenleistung erheblich zugunsten der Bank verschieben würden.

In diesen Fällen wird die Bank die Zustimmung des Karteninhabers zu den Änderungen auf andere Weise einholen.
20.5 Kündigungsrecht des Karteninhabers bei der Zustimmungsfiktion
Macht die Bank von der Zustimmungsfiktion Gebrauch, kann der Karteninhaber diese Geschäftsbeziehung vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen auch fristlos und kostenfrei kündigen. Auf dieses Kündigungsrecht wird ihn die Bank in ihrem Angebot besonders hinweisen.

21. Kündigung
21.1 Sowohl der Kreditkartenvertrag als auch die Nutzung der digitalen Kreditkarte alleine kann vom Karteninhaber/von der Firma jederzeit und fristlos gekündigt werden. Die Bank kann den Kreditkartenvertrag jederzeit mit einer Frist von mindestens zwei Monaten und Vorliegen eines sachlichen Kündigungsgrundes kündigen. Die Bank kann den Kreditkartenvertrag fristlos kündigen, wenn ein wichtiger Grund vorliegt, durch den die Fortsetzung des Kreditkartenvertrags auch unter angemessener Berücksichtigung der berechtigten Belange des Karteninhabers/der Firma für die Bank unzumutbar ist. Ein solcher Grund liegt insbesondere vor, wenn der Karteninhaber/die Firma unrichtige Angaben über seine/ihre Vermögenslage gemacht hat oder eine wesentliche Verschlechterung seiner/ihrer Vermögenslage eintritt oder einzutreten droht und dadurch die Erfüllung der Verbindlichkeiten aus dem Kreditkartenvertrag gegenüber der Bank wesentlich gefährdet ist. Mit Wirksamwerden der Kündigung des Kreditkartenvertrags darf die Kreditkarte bzw. bei alleiniger Kündigung der Nutzung der digitalen Kreditkarte darf die digitale Kreditkarte nicht mehr benutzt werden.
21.2 Eingeräumte Kreditrahmen, für die weder eine Laufzeit noch eine abweichende Kündigungsregelung vereinbart ist, kann die Bank jederzeit – vorbehaltlich zwingender verbraucherschützender Rechtsvorschriften – ohne Einhaltung einer Kündigungsfrist kündigen; daneben steht der Bank das Recht zur fristlosen Kündigung aus wichtigem Grund zu. Die Bank wird bei Ausübung dieses Kündigungsrechts auf die berechtigten Belange des Karteninhabers/der Firma Rücksicht nehmen.

22. Einschaltung Dritter
Die Bank ist berechtigt, sich im Rahmen des Kreditkartenvertrags zur Bewirkung der von ihr zu erbringenden Leistungen und zur Einforderung der vom Karteninhaber zu erbringenden Leistungen Dritter zu bedienen.

23. Änderung persönlicher Daten
Änderungen von Anschrift, Name, Bankverbindung und sonstigen wesentlichen, auch wirtschaftlichen, Umständen sind der Bank unverzüglich in Textform mitzuteilen.

24. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit
Für die Beilegung von Streitigkeiten mit der Bank kann sich der Karteninhaber an die im Preis- und Leistungsverzeichnis näher bezeichnete/n Streitschlichtungsstelle/n wenden.

25. Rechtswahl, Erfüllungsort, Gerichtsstand
Auf den Kartenvertrag findet deutsches Recht Anwendung, sofern dem nicht zwingende gesetzliche Regelungen entgegenstehen. Erfüllungsort ist Stuttgart. Ist der Karteninhaber Kaufmann, ist Gerichtsstand Stuttgart. Im Übrigen wird Stuttgart als Gerichtsstand vereinbart für den Fall, dass der Karteninhaber nach Abschluss des Kartenvertrags seinen Wohnsitz oder gewöhnlichen Aufenthalt ins Ausland verlegt oder diese im Zeitpunkt der Klageerhebung nicht bekannt sind.

Bedingungen für die digitale Mastercard (Kreditkarte) mit individualisierten Authentifizierungsverfahren.

BW BANK
Ein Unternehmen der LBBW-Gruppe

Fassung: 14. September 2019

1. Anwendungsbereich
Die von der Baden-Württembergischen Bank (nachfolgend »Bank« genannt) ausgegebene digitale Mastercard ist eine Kreditkarte (nachfolgend digitale Kreditkarte genannt), die dem Kunden digital zur Speicherung auf einem mobilen Endgerät (Telekommunikations-, Digital- oder IT-Gerät) zur Nutzung von mobilen Bezahlverfahren bereitgestellt wird. Es gelten die »Bedingungen für die *Corporate*World Mastercard (Kreditkarte)«, sofern in den »Bedingungen für die digitale Mastercard mit individualisierten Authentifizierungsverfahren« nicht Abweichendes vereinbart ist. Diese Bedingungen regeln das Vertragsverhältnis zwischen der kartenausgebenden Bank und dem Karteninhaber. Vertragliche Vereinbarungen zwischen dem Karteninhaber und Dritten (z. B. Endgerätehersteller, Mobilfunkanbieter oder Anbieter von Bezahlplattformen, in denen digitale Kreditkarten hinterlegt werden können) bleiben unberührt. Die vertragliche Leistung der Bank betrifft nicht die Funktionsfähigkeit oder den Betrieb des mobilen Endgerätes oder von Bezahlplattformen wie Apps für digitale Geldbörsen (Wallets), in denen die digitale Kreditkarte hinterlegt werden kann.

2. Nutzung der digitalen Karte mit individualisierten Authentifizierungsverfahren
Der Karteninhaber kann die digitale Kreditkarte mit individualisierten Authentifizierungsverfahren nur nutzen, wenn er sich gegenüber der Bank authentifiziert hat. Die Authentifizierung ist das Verfahren, mit deren Hilfe die Bank die Identität des Karteninhabers oder die berechtigte Verwendung der digitalen Kreditkarte überprüfen kann.
Dafür werden als Authentifizierungselemente die digitale Kreditkarte auf dem mobilen Endgerät des Karteninhabers als erster Faktor (Besitzelement) und biometrische Elemente des Karteninhabers, z. B. Fingerabdruck, Gesichtserkennung bzw. sonstige Entsperrmechanismen des mobilen Endgerätes (z. B. der Entsperrcode), jeweils als zweiter Faktor vereinbart. Die Eingabe der für die digitale Kreditkarte geltenden persönlichen Geheimzahl (PIN) ist für die Nutzung der Kreditkarte mit individualisierten Authentifizierungsverfahren nicht vorgesehen.

3. Verwendungsmöglichkeiten
Der Karteninhaber kann die digitale Kreditkarte, soweit diese und die Terminals entsprechend ausgestattet sind, für folgende Zahlungsdienste nutzen:
a) Zum kontaktlosen Einsatz an automatisierten Kassen (Kontaktlos-Terminals) bei Handels- und Dienstleistungsunternehmen (Vertragsunternehmen).
b) Zum Einsatz bei elektronischen Fernzahlungsvorgängen über das Internet bei Vertragsunternehmen (Online-Handel). Sofern der Karteninhaber die digitale Kreditkarte einer digitalen Geldbörse (Wallet) hinzugefügt hat, kann die digitale Kreditkarte an allen Kontaktlos-Terminals und im Online-Handel eingesetzt werden, die an dem Akzeptanzzeichen der jeweiligen Bezahlanwendung zu erkennen sind.
Ergänzende Informationen erteilt die Bank in den jeweiligen Nutzungshinweisen für die digitale Kreditkarte.

4. Autorisierung von Kartenzahlungen durch den Karteninhaber
Mit dem Einsatz der digitalen Kreditkarte durch Heranführen des mobilen Endgerätes mit der digitalen Kreditkarte an das Kontaktlos-Terminal bzw. im Online-Handel durch Bestätigung der Bezahlanwendung erteilt der Karteninhaber die Zustimmung (Autorisierung) zur Ausführung der Kartenzahlung. Dazu ist zusätzlich die Verwendung der biometrischen Merkmale des Karteninhabers oder Eingabe des Entsperrcodes des Gerätes jeweils mit auf dem mobilen Endgerät vorhandenen Funktionen erforderlich. Die Zustimmung wird mit deren Einsatz erteilt. In der 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. Nach Erteilung der Zustimmung kann der Karteninhaber die Kartenzahlung nicht mehr widerrufen.

5. Verfügungsrahmen
Der Karteninhaber darf Verfügungen mit seiner digitalen Kreditkarte nur im Rahmen des für die Kreditkarte vereinbarten Verfügungsrahmens vornehmen. Bei jeder Nutzung wird geprüft, ob der Verfügungsrahmen durch vorangegangene Verfügungen (mit der digitalen oder der physischen Kreditkarte) bereits ausgeschöpft ist. Der Karteninhaber/die Firma kann mit der Bank eine Änderung des Verfügungsrahmens der Kreditkarte oder des täglichen Verfügungslimits vereinbaren.

6. Sperre der digitalen Kreditkarte mit individualisierten Authentifizierungsverfahren
a) Die Bank darf die digitale Kreditkarte mit individualisierten Authentifizierungsverfahren sperren (z. B. durch Löschung), wenn sie berechtigt ist, den Kartenvertrag aus wichtigem Grund zu kündigen, wenn sachliche Gründe im Zusammenhang mit der Sicherheit der individualisierten Authentifizierungselemente des Karteninhabers oder der digitalen Kreditkarte dies rechtfertigen oder wenn der Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines Authentifizierungselements oder der digitalen Kreditkarte besteht. Darüber wird die Bank den Karteninhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten. Die Angabe von Gründen darf unterbleiben, wenn die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde. Die Bank wird die digitale Kreditkarte entsperren oder eine neue digitale Kreditkarte bereitstellen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Auch hierüber unterrichtet sie den Karteninhaber unverzüglich.
b) Eine Sperre ausschließlich der digitalen Kreditkarte bewirkt keine Sperre der physischen Kreditkarte. Eine Sperre der physischen Kreditkarte hat stets auch eine Sperre aller zugehörigen digitalen Kreditkarten zur Folge.

7. Sorgfalts- und Mitwirkungspflichten des Karteninhabers
7.1 Schutz der individualisierten Authentifizierungselemente
Der Karteninhaber hat alle zumutbaren Vorkehrungen zu treffen, um seine für die Nutzung der digitalen Kreditkarte verwendeten biometrischen Merkmale (z. B. Fingerabdruck), das mobile Endgerät mit digitaler Kreditkarte und den Entsperrcode des mobilen Endgerätes vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass die digitale Kreditkarte missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird.
Dazu hat er Folgendes zu beachten:
a) Der Entsperrcode für das mobile Endgerät ist geheim zu halten. Er darf insbesondere
   – nicht mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
   – nicht ungesichert elektronisch gespeichert werden (z. B. Speicherung im Klartext im Computer oder im mobilen Endgerät) und
   – nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als mobiles Endgerät mit digitaler Kreditkarte dient.
b) Das mobile Endgerät mit digitaler Kreditkarte ist vor Missbrauch zu schützen, insbesondere
   – ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Karteninhabers (z. B. Mobiltelefon) nicht zugreifen können,
   – ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät gespeicherte digitale Kreditkarte nicht nutzen können,
   – ist die digitale Kreditkarte auf dem mobilen Endgerät zu löschen, bevor der Karteninhaber den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf, Entsorgung),
   – muss der Karteninhaber die ihm vom Hersteller des mobilen Endgerätes mit digitaler Kreditkarte jeweils angebotenen Software-Updates installieren,
   – muss der Karteninhaber, falls er einen Code zur Aktivierung der digitalen Kreditkarte von der Bank erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren.
c) Biometrische Merkmale, wie z. B. der Fingerabdruck des Karteninhabers, dürfen auf einem mobilen Endgerät des Karteninhabers mit digitaler Kreditkarte nur dann zur Autorisierung von Zahlungsaufträgen verwendet werden, wenn auf dem mobilen Endgerät keine biometrischen Merkmale anderer Personen gespeichert sind. Etwaige bereits auf dem mobilen Endgerät vorhandene biometrische Merkmale anderer Personen sind vor der Speicherung der digitalen Kreditkarte auf dem mobilen Endgerät zu entfernen.

7.2 Unterrichtungs- und Anzeigepflichten
a) Stellt der Karteninhaber den Verlust oder Diebstahl des mobilen Endgerätes mit digitaler Kreditkarte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung der digitalen Kreditkarte fest, so ist die Bank unverzüglich zu benachrichtigen (Sperranzeige). Die Sperranzeige kann der Karteninhaber auch jederzeit gegenüber dem Zentralen Sperrannahmedienst (Telefon: 116 116 aus dem Inland und +49 116 116 aus dem Ausland [ggf. abweichende Ländervorwahl]) abgeben. Der Karteninhaber hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei anzuzeigen.
b) Hat der Karteninhaber den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls unverzüglich eine Sperranzeige abgeben.
c) Durch die Sperre der digitalen Kreditkarte bei der Bank beziehungsweise gegenüber dem Zentralen Sperrannahmedienst wird nicht der Zugang zum mobilen Endgerät gesperrt. Eine Sperrung der sonstigen Funktionen auf dem mobilen Endgerät kann nur gegenüber dem jeweiligen Anbieter dieser Funktionen erfolgen. Der Karteninhaber hat die Bank unverzüglich nach Feststellung einer nicht autorisierten oder fehlerhaft ausgeführten Kartenverfügung zu unterrichten.
d) Auch wenn der Karteninhaber ein Sperr- oder Löschverfahren für das mobile Endgerät oder einer Bezahlplattform nutzt, bleibt die Verpflichtung zur Abgabe einer Sperranzeige nach Nummer 7.2 Absatz a) dieser Bedingungen bestehen; eine Sperre des mobilen Endgerätes hat keine Sperre der digitalen Kreditkarte zur Folge.

8. Ablehnung von Kartenzahlungen durch die Bank
Die Bank ist berechtigt, die Kartenzahlung abzulehnen, wenn
– der Karteninhaber die Autorisierung der Kartenzahlung nicht gemäß Nummer 4 erteilt hat,
– der vereinbarte Verfügungsrahmen oder die finanzielle Nutzungsgrenze nicht eingehalten ist oder
– die digitale Kreditkarte gesperrt ist.
Hierüber wird der Karteninhaber im Rahmen des Bezahlvorgangs unterrichtet.

9. Erstattungs-, Berichtigungs- und Schadensersatzansprüche des Karteninhabers
9.1 Erstattung bei nicht autorisierter Kartenverfügung
Im Falle einer nicht autorisierten Kartenverfügung, z. B. im Rahmen der Verwendung der digitalen Kreditkarte an Kontaktlos-Terminals bei Handels- und Dienstleistungsunternehmen oder im Online-Handel, hat die Bank gegen den Karteninhaber keinen Anspruch auf Erstattung ihrer Aufwendungen. Die Bank ist verpflichtet, dem Karteninhaber den Betrag ungekürzt zu erstatten. Wurde der Betrag dem Konto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne die nicht autorisierte Kartenverfügung befunden hätte. Diese Verpflichtung ist unverzüglich, spätestens jedoch bis zum Ende des Geschäftstags gemäß »Preis- und Leistungsverzeichnis« zu erfüllen, der auf den Tag folgt, an welchem der Bank angezeigt wurde, dass die Kartenverfügung nicht autorisiert ist oder die Bank auf andere Weise davon Kenntnis erhalten hat. Hat die Bank einer zuständigen Behörde berechtigte Gründe für den Verdacht, dass ein betrügerisches Verhalten des Kunden vorliegt, schriftlich mitgeteilt, hat die Bank ihre Verpflichtung aus Satz 2 unverzüglich zu prüfen und zu erfüllen, wenn sich der Betrugsverdacht nicht bestätigt.

9.2 Ansprüche bei nicht erfolgter oder fehlerhafter Ausführung einer autorisierten Kartenverfügung
a) Im Falle einer nicht erfolgten oder fehlerhaften Ausführung einer autorisierten Kartenverfügung, z. B. im Rahmen der Verwendung der digitalen Kreditkarte an Kontaktlos-Terminals bei Handels- und Dienstleistungsunternehmen oder im Online-Handel, kann der Karteninhaber von der Bank die unverzügliche und ungekürzte Erstattung des Verfügungsbetrages insoweit verlangen, als die Kartenverfügung nicht erfolgte oder fehlerhaft war. Wurde der Betrag dem Konto belastet, bringt die Bank dieses wieder auf den Stand, auf dem es sich ohne die nicht erfolgte oder fehlerhafte Kartenverfügung befunden hätte.
b) Der Karteninhaber kann über den Absatz 1 hinaus von der Bank die Erstattung der Entgelte und Zinsen insoweit verlangen, als ihm diese im Zusammenhang mit der nicht erfolgten oder fehlerhaften Ausführung der autorisierten Kartenverfügung in Rechnung gestellt oder seinem Konto belastet wurden.
c) Wurde eine autorisierte Kartenverfügung nicht oder fehlerhaft ausgeführt, wird die Bank die Kartenverfügung auf Verlangen des Karteninhabers nachvollziehen und ihn über das Ergebnis unterrichten.

9.3 Schadensersatzansprüche des Karteninhabers

Im Falle einer nicht autorisierten Kartenverfügung oder im Falle einer nicht erfolgten oder fehlerhaften Ausführung einer autorisierten Kartenverfügung kann der Karteninhaber von der Bank einen Schaden, der nicht bereits von den Nummern 9.1 oder 9.2 erfasst ist, ersetzt verlangen. Dies gilt nicht, wenn die Bank die Pflichtverletzung nicht zu vertreten hat. Die Bank hat hierbei ein Verschulden, das einer zwischengeschalteten Stelle zur Last fällt, wie eigenes Verschulden zu vertreten, es sei denn, dass die wesentliche Ursache bei einer zwischengeschalteten Stelle liegt, die der Karteninhaber vorgegeben hat. Handelt es sich bei dem Karteninhaber nicht um einen Verbraucher oder erfolgt der Einsatz der digitalen Kreditkarte in einem Land außerhalb des Europäischen Wirtschaftsraumes, beschränkt sich die Haftung der Sparkasse/Landesbank 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 Sparkasse/Landesbank und Karteninhaber den Schaden zu tragen haben. Die Haftung nach diesem Absatz ist auf 12.500 EUR je Kartenverfügung begrenzt. Diese betragsmäßige Haftungsbeschränkung gilt nicht

- für nicht autorisierte Kartenverfügungen,
- bei Vorsatz oder grober Fahrlässigkeit der Bank
- für Gefahren, die die Bank besonders übernommen hat und
- für den dem Karteninhaber entstandenen Zinsschaden, soweit der Karteninhaber Verbraucher ist.

9.4 Haftungs- und Einwendungsausschluss

a) Ansprüche gegen die Bank nach Nummern 9.1 bis 9.3 sind ausgeschlossen, wenn der Karteninhaber die Bank nicht spätestens 13 Monate nach dem Tag der Belastung mit der Kartenverfügung darüber unterrichtet hat, dass es sich um eine nicht autorisierte, nicht erfolgte oder fehlerhafte Kartenverfügung handelt. Der Lauf der 13-monatigen Frist beginnt nur, wenn die Bank den Karteninhaber über die aus der Kartenverfügung resultierende Belastungsbuchung entsprechend dem für Kontoinformationen vereinbarten Weg spätestens innerhalb eines Monats nach der Belastungsbuchung unterrichtet hat; anderenfalls ist für den Fristbeginn der Tag der Unterrichtung maßgeblich. Haftungsansprüche nach Nummer 9.3 kann der Karteninhaber auch nach Ablauf der in Satz 1 genannten Frist geltend machen, wenn er ohne Verschulden an der Einhaltung dieser Frist verhindert war.

b) Ansprüche des Karteninhabers gegen die Bank sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände
   - auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das die Bank keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können oder
   - von der Bank aufgrund einer gesetzlichen Verpflichtung herbeigeführt wurden.

10. Haftung des Karteninhabers für nicht autorisierte Kartenverfügungen

10.1 Haftung des Karteninhabers bis zur Sperranzeige

a) Verliert der Karteninhaber seine digitale Kreditkarte (z. B. durch Verlust seines Mobiltelefons) oder eines seiner Authentifizierungselemente, werden ihm diese gestohlen oder kommen diese sonst abhanden oder werden diese missbräuchlich verwendet und kommt es dadurch zu nicht autorisierten Kartenverfügungen im Rahmen der Verwendung der digitalen Kreditkarte an Kontaktlos-Terminals bei Handels- und Dienstleistungsunternehmen oder im Online-Handel, dann haftet der Karteninhaber für Schäden, die bis zum Zeitpunkt der Sperranzeige verursacht werden, in Höhe von maximal 50 EUR. Seine Haftung nach Absatz f) für Vorsatz und grobe Fahrlässigkeit sowie für Handeln in betrügerischer Absicht bleibt unberührt.

b) Der Karteninhaber haftet nicht nach Absatz a), wenn
   - es dem Karteninhaber nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung der digitalen Kreditkarte oder eines seiner Authentifizierungselemente vor der nicht autorisierten Kartenverfügung zu bemerken oder
   - der Verlust der digitalen Kreditkarte oder eines seiner Authentifizierungselemente durch einen Angestellten, einen Agenten, eine Zweigstelle der Bank oder eine sonstige Stelle, an die Tätigkeiten der Bank ausgelagert wurden, verursacht worden ist.

   Die Haftung nach Absatz f) für Vorsatz und grobe Fahrlässigkeit sowie für Handeln in betrügerischer Absicht bleibt unberührt.

c) Handelt es sich bei dem Karteninhaber nicht um einen Verbraucher oder erfolgt der Einsatz der digitalen Kreditkarte außerhalb des Europäischen Wirtschaftsraumes, trägt der Karteninhaber den aufgrund nicht autorisierter Kartenverfügungen entstehenden Schaden nach Absatz a) auch über einen Betrag von maximal 50 EUR hinaus, wenn der Karteninhaber die ihm nach diesen Bedingungen obliegenden Pflichten fahrlässig verletzt hat. Hat die Bank durch eine Verletzung ihrer Pflichten zur Entstehung des Schadens beigetragen, haftet die Bank für den entstandenen Schaden im Umfang des von ihr zu vertretenden Mitverschuldens.

d) Die Bank verzichtet auf die Schadensbeteiligung durch den Karteninhaber in Höhe von maximal 50 EUR gemäß vorstehendem Absatz a) und übernimmt alle Schäden, die durch nicht autorisierte Zahlungsvorgänge bis zum Eingang der Sperranzeige nach Nummer 7.2 a) entstanden sind, wenn der Karteninhaber seine ihm gemäß Nummern 7.1 und 7.2 obliegenden Sorgfalts- und Mitwirkungspflichten nicht in betrügerischer Absicht, vorsätzlich oder grob fahrlässig verletzt hat. Eine Übernahme des vom Karteninhaber zu tragenden Schadens durch die Bank erfolgt nur, wenn der Karteninhaber die Voraussetzungen der Haftungsentlastung glaubhaft darlegt und Anzeige bei der Polizei erstattet.

e) Der Karteninhaber ist nicht zum Ersatz des Schadens nach den Absätzen a) und c) verpflichtet, wenn der Karteninhaber die Sperranzeige nach Nummer 7.2 a) nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

f) Kommt es vor der Sperranzeige nach Nummer 7.2 a) zu nicht autorisierten Kartenverfügungen und hat der Karteninhaber seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Karteninhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Karteninhabers kann insbesondere dann vorliegen, wenn
   - der Verlust, Diebstahl oder die missbräuchliche Verfügung der Bank oder dem Zentralen Sperrannahmedienst schuldhaft nicht unverzüglich mitgeteilt wurde, nachdem der Karteninhaber hiervon Kenntnis erlangt hat oder
   - der Entsperrcode ungesichert elektronisch gespeichert oder ungesichert auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt wurde, das als mobiles Endgerät mit digitaler Kreditkarte dient oder
   - die digitale Kreditkarte auf dem mobilen Endgerät nicht gelöscht wurde, bevor der Karteninhaber den Besitz an diesem mobilen Endgerät aufgibt (durch Verkauf, Entsorgung).

   Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den für die Kreditkarte geltenden Verfügungsrahmen.

g) Hat die Bank eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz (ZAG) nicht verlangt oder hat der Zahlungsempfänger oder sein Zahlungsdienstleister diese nicht akzeptiert, obwohl die Bank nach § 55 ZAG zur starken Kundenauthentifizierung verpflichtet war, bestimmt sich die Haftung des Karteninhabers und der Bank abweichend von den Absätzen a) bis f) nach den Bestimmungen in § 675v Absatz 4 des Bürgerlichen Gesetzbuches. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungsfaktoren (siehe Nummer 2 dieser Bedingungen).

10.2 Haftung des Karteninhabers ab Sperranzeige

Sobald der Bank oder dem Zentralen Sperrannahmedienst der Verlust oder Diebstahl der digitalen Kreditkarte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung der digitalen Kreditkarte oder der Authentifizierungselemente angezeigt wurde, übernimmt die Bank alle danach durch Kartenverfügungen entstehenden Schäden.

Handelt der Karteninhaber in betrügerischer Absicht, trägt der Karteninhaber auch die nach der Sperranzeige nach Nummer 7.2 a) entstehenden Schäden.

11. Kündigung

Die Bank ist berechtigt, die Nutzung der digitalen Kreditkarte mit individualisierten Authentifizierungsverfahren mit einer Frist von mindestens zwei Monaten zu kündigen. Der Karteninhaber/die Firma ist hierzu jederzeit ohne Einhaltung einer Kündigungsfrist berechtigt. Die Bank kann den Kreditkartenvertrag zur digitalen Kreditkarte mit individualisierten Authentifizierungsverfahren fristlos kündigen, wenn ein wichtiger Grund vorliegt, durch den die Fortsetzung des Vertrages auch unter angemessener Berücksichtigung der Belange des Karteninhabers/der Firma für die Bank nicht zumutbar ist. Ein solcher Grund liegt insbesondere vor, wenn der Karteninhaber/die Firma unrichtige Angaben über seine/ihre Vermögensverhältnisse gemacht hat oder eine wesentliche Verschlechterung seiner/ihrer Vermögensverhältnisse eintritt oder einzutreten droht und dadurch die Erfüllung der Verbindlichkeiten aus dem Kreditkartenvertrag gegenüber der Bank wesentlich gefährdet ist. Mit Wirksamwerden der Kündigung darf der Karteninhaber die digitale Kreditkarte mit individualisierten Authentifizierungsverfahren nicht mehr nutzen.

12. Zahlungsverpflichtung der Bank; Reklamationen

Die Bank ist gegenüber den Handels- und Dienstleistungsunternehmen vertraglich verpflichtet, die Beträge, über die unter Verwendung der an den Karteninhaber ausgegebenen digitalen Kreditkarte verfügt wurden, zu vergüten. Einwendungen und sonstige Beanstandungen des Karteninhabers aus dem Vertragsverhältnis zu dem Vertragsunternehmen, bei dem bargeldlos bezahlt worden ist, sind unmittelbar gegenüber diesem Unternehmen geltend zu machen. Gleiches gilt für Funktionsstörungen einer Bezahlplattform oder einer elektronischen Geldbörse (Wallet), in der die digitale Kreditkarte hinterlegt worden ist.

13. Außergerichtliche Streitschlichtung und Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Karteninhaber an die im »Preis- und Leistungsverzeichnis« näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

Bedingungen für BW Kartenservice Online.

Fassung: 14. September 2019

BW BANK
Ein Unternehmen der LBBW-Gruppe

1. Leistungsangebot
(1) Der Karteninhaber – nachfolgend als »Teilnehmer« bezeichnet – ist berechtigt, den BW Kartenservice Online (KSO) in dem von der Baden-Württembergischen Bank – nachfolgend als »Bank« bezeichnet – angebotenen Umfang für die von ihm dort verwaltete Kredit- oder Debitkarte (nachstehend Karte genannt) zu nutzen. Zudem kann er Informationen der Bank mittels KSO abrufen.

2. Voraussetzungen zur Nutzung des KSO
(1) Der Teilnehmer kann den KSO nutzen, wenn die Bank ihn authentifiziert hat.
(2) Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3) sowie Aufträge erteilen (siehe Nummer 4).
(3) Authentifizierungselemente sind
– Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer [PIN])
– Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN], die den Besitz des Teilnehmers nachweisen, wie das mobile Endgerät) oder
– Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers.
Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

3. Zugang zum KSO
(1) Der Teilnehmer erhält Zugang zum KSO der Bank, wenn
– er seine individuelle Teilnehmerkennung (z. B. Kartennummer) angibt und
– er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
– keine Sperre des Zugangs (siehe Nummern 8.1 und 9) vorliegt.
Nach Gewährung des Zugangs zum KSO kann auf Informationen zugegriffen oder können nach Nummer 4 Aufträge erteilt werden.
(2) Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z. B. zum Zweck der Änderung der Anschrift Teilnehmers) fordert die Bank den Teilnehmer auf, sich unter Verwendung eines weiteren Authentifizierungselements auszuweisen, wenn beim Zugang zum KSO nur ein Authentifizierungselement angefordert wurde.

4. Aufträge
4.1 Auftragserteilung
Der Teilnehmer muss einem Auftrag (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers, Änderung der Anschrift des Teilnehmers) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente (z. B. Eingabe einer TAN als Nachweis des Besitzelements) zu verwenden. Die Bank bestätigt mittels KSO den Eingang des Auftrags.

4.2 Widerruf von Aufträgen
Die Widerrufbarkeit eines Auftrags (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers) richtet sich nach den für die jeweilige Auftragsart geltenden Bedingungen. Der Widerruf von Aufträgen kann nur außerhalb des KSO erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit im KSO ausdrücklich vor.

5. Bearbeitung von Aufträgen durch die Bank
(1) Die Bearbeitung der Aufträge (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers) erfolgt an den für die Abwicklung der jeweiligen Auftragsart im »Preis- und Leistungsverzeichnis« bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitsablaufs. Geht der Auftrag nach dem im »Preis- und Leistungsverzeichnis« angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß »Preis- und Leistungsverzeichnis« der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Geschäftstag.
(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:
– Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1).
– Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers, Änderung der Anschrift des Teilnehmers) liegt vor.
– Das KSO-Datenformat ist eingehalten.
– Die weiteren Ausführungsbedingungen nach den für die jeweilige Auftragsart maßgeblichen Bedingungen liegen vor.
Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Bedingungen aus.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem Teilnehmer 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, mittels KSO zur Verfügung stellen.

6. Information des Teilnehmers über KSO-Verfügungen
Die Bank unterrichtet den Teilnehmer mindestens einmal monatlich über die mittels KSO getätigten Verfügungen (z. B. Kontoüberträge auf eigenes Girokonto des Teilnehmers) auf dem hierfür vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers
7.1 Schutz der Authentifizierungselemente
(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass der KSO missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummer 3 und 4)
(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:
(a) Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere
– nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
– nicht außerhalb des KSO 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 Anwendung für KSO und Fingerabdrucksensor) dient.
(b) Besitzelemente, wie z. B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
– ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
– ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für den KSO (z. B. BW-Secure-App) nicht nutzen können,
– ist die Anwendung für den KSO (z. B. BW-Secure-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)
– dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des KSO mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
– muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für den KSO) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für den KSO des Teilnehmers aktivieren.
(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Teilnehmers für den KSO nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für den KSO genutzt wird, Seinselemente anderer Personen gespeichert, ist für den KSO das von der Bank ausgegebene Wissenselement (z. B. PIN in der Anwendung BW-Secure) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

7.2 Sicherheitshinweise der Bank
Der Teilnehmer muss die Sicherheitshinweise auf der KSO-Seite der Bank, insbesondere die Maßnahmen zum Schutz der von ihm eingesetzten Hard- und Software, beachten.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten
Die Bank zeigt dem Teilnehmer die von ihr empfangenen Auftragsdaten (z. B. Betrag des Kontoübertrags auf eigenes Konto des Teilnehmers) Kontonummer des Empfängerkontos bei Kontoübertrag auf eigenes Konto des Teilnehmers, über das gesondert vereinbarte Gerät des Teilnehmers an (z. B. mittels mobilen Endgeräts). Der Teilnehmer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten
8.1 Sperranzeige
(1) Stellt der Teilnehmer
– den Verlust oder den Diebstahl eines Besitzelements zur Authentifizierung (z. B. mobiles Endgerät) oder
– die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung eines Authentifizierungselements fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.
(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.
(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge
Der Teilnehmer hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre
9.1 Sperre auf Veranlassung des Teilnehmers
Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1, den KSO-Zugang für ihn oder seine Authentifizierungselemente zur Nutzung des KSO.

9.2 Sperre auf Veranlassung der Bank
(1) Die Bank darf den Zugang zum KSO für einen Teilnehmer sperren, wenn
– sie berechtigt ist, den Vertrag zum KSO aus wichtigem Grund zu kündigen,
– sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
– der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.
(2) Die Bank wird den Teilnehmer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre
Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Teilnehmer unverzüglich.

9.4 Automatische Sperre des Zugangs für KSO
Wird dreimal in Folge ein falsches Authentifizierungselement (z. B. die PIN) eingegeben, so sperrt die Bank automatisch den Zugang zum KSO für diesen Teilnehmer. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des KSO wiederherzustellen.

10. Haftung
10.1 Haftung der Bank bei Ausführung eines nicht autorisierten Auftrags und eines nicht, fehlerhaft oder verspätet ausgeführten Auftrags
Die Haftung der Bank bei einem nicht autorisierten Auftrag (z. B. Kontoübertrag auf eigenes Girokonto des Teilnehmers) und einem nicht, fehlerhaft oder verspätet ausgeführten Auftrag richtet sich nach den für die jeweilige Auftragsart vereinbarten Bedingungen.

10.2 Haftung des Teilnehmers bei missbräuchlicher Nutzung der Authentifizierungselemente

10.2.1 Haftung des Teilnehmers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungselements oder auf der sonstigen missbräuchlichen Verwendung eines Authentifizierungselements, haftet der Teilnehmer für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 EUR, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Teilnehmer ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

– es dem Teilnehmer nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Authentifizierungselements vor dem nicht autorisierten Zahlungsvorgang zu bemerken oder
– der Verlust des Authentifizierungselements durch einen Angestellten, einen Agenten, eine Zweigniederlassung/Zweigstelle eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Anzeigepflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Teilnehmer abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er eine seiner Sorgfaltspflichten nach

– Nummer 7.1 Absatz 2,
– Nummer 7.3 oder
– Nummer 8.1 Absatz 1

verletzt hat.

(4) Abweichend von den Absätzen 1 und 3 ist der Teilnehmer nicht zum Schadensersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 ZAG nicht verlangt hat. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Authentifizierungselementen aus den Kategorien Wissen, Besitz oder Sein (siehe Nummer 2 Absatz 3).

(5) Der Teilnehmer ist nicht zum Ersatz des Schadens nach Absatz 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(6) Die Absätze 2 und 4 sowie 5 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(7) Ist der Teilnehmer kein Verbraucher, gilt ergänzend Folgendes:

– Der Teilnehmer haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 EUR nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
– Die Haftungsbeschränkung in Absatz 2 Satz 1 findet keine Anwendung.

10.2.2 Haftung ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte KSO-Aufträge entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.3 Haftungsausschluss

Haftungsansprüche 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 von ihr nicht hätten vermieden werden können.

11. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit

Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die im »Preis- und Leistungsverzeichnis« näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

Bedingungen für die Nutzung des Elektronischen Postfachs im BW Kartenservice Online.

BW BANK
Ein Unternehmen der LBBW-Gruppe

Fassung: 14. September 2019

1. Gegenstand der Bedingungen
1.1 Nutzung des Elektronischen Postfachs im BW Kartenservice Online
Diese Bedingungen regeln die Nutzung der Anwendung »Elektronisches Postfach« auf der Plattform BW Kartenservice Online (KSO). Damit kann ein Karteninhaber (nachfolgend »Teilnehmer« genannt) im Rahmen seines KSO-Zugangs »elektronische Post« zu der von ihm über den KSO verwalteten Kredit- oder Debitkarte (nachfolgend »Karte« genannt) empfangen und elektronische Nachrichten an die Baden-Württembergische Bank (nachfolgend »Bank« genannt) senden. Elektronische Post sind sämtliche Mitteilungen der Bank, die in das Elektronische Postfach im KSO eingestellt werden, insbesondere rechtsverbindliche Mitteilungen zur laufenden Geschäftsbeziehung (z. B. Änderung der Kartenbedingungen einschließlich der Entgelte), Kartenbezogene Informationen oder nicht rechtsverbindliche werbliche Inhalte (»Werbeinhalte«). kartenbezogene Informationen sind insbesondere Kartenabrechnungen einschließlich der darin enthaltenen Rechnungsabschlüsse, Anzeigen über die Nichtausführung von Aufträgen, die Sperrung von Authentifizierungsinstrumenten und deren Entsperrung, Informationen zu Kartenprodukten sowie weitere gesetzlich geschuldete Informationen. Kann der Text über das Elektronische Postfach im KSO nicht mitgeteilt werden, wird die Bank per Post oder in einer anderen vereinbarten Form informieren.

1.2 Bestimmung als Empfangsvorrichtung des Teilnehmers (Widmung)
Zu dem dargestellten Zweck bestimmt der Teilnehmer das Elektronische Postfach im KSO als Vorrichtung des Teilnehmers zum Empfang elektronischer Post im Sinne von Ziffer 1.1 und insbesondere rechtsverbindlicher Dokumente. Der Teilnehmer kann einzelne oder alle Dokumente jederzeit löschen. Eine Löschung von Dokumenten durch die Bank ist ausgeschlossen. Die Bank hat keinen Lesezugriff auf den Inhalt des Elektronischen Postfachs im KSO. Sofern der Teilnehmer das Elektronische Postfach im KSO nicht mehr als seine Empfangsvorrichtung nutzen möchte, kann er das Postfach gemäß Nr. 4 kündigen.

1.3 Externe Dokumente
Neben dem Inhalt des Postfachs werden dem Teilnehmer auch Verknüpfungen (»Links«) zu Dokumenten angezeigt, die außerhalb des Elektronischen Postfachs im KSO abgelegt sind. Diese Verknüpfungen weisen ein Ablaufdatum auf, ab dem sie nicht mehr zur Verfügung stehen. Ruft der Teilnehmer ein verknüpftes Dokument nicht bis zum Eintreten dieses Ablaufdatums auf, darf die Bank dem Teilnehmer dieses Dokument postalisch gegen Portoersatz zusenden.

1.4 Erweiterung der Postfachnutzung
Das Elektronische Postfach im KSO wird ständig weiterentwickelt. Sofern neue Dokumenttypen für die Postfachnutzung zur Verfügung stehen, wird die Bank dem Teilnehmer eine entsprechende Erweiterung der Postfachnutzung zwei Monate vor Inkrafttreten der Änderung anbieten. Die Zustimmung des Teilnehmers zum Angebot der Bank gilt als erteilt, wenn der Teilnehmer seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt angezeigt hat. Auf diese Genehmigungswirkung wird die Bank in ihrem Angebot besonders hinweisen.

2. Leistungsangebot
2.1 Nutzung des Elektronischen Postfachs im KSO
Der Teilnehmer ist berechtigt, das Elektronische Postfach im KSO in dem jeweils von der Bank angebotenen Umfang zu nutzen.

2.2 Freischaltung
Das Elektronische Postfach im KSO steht dem Teilnehmer erst nach Freischaltung zur Verfügung.

2.3 Umstellung auf elektronischen Versand
Soweit nicht ausdrücklich etwas anderes vereinbart wurde, übermittelt die Bank nach Freischaltung elektronische Post, insbesondere Kartenabrechnungen ausschließlich in elektronischer Form. Kartenabrechnungen werden erst ab dem der Freischaltung folgenden Abrechnungsstichtag in das Elektronische Postfach im KSO übermittelt. Vor dem Abrechnungsstichtag erfolgt die Abrechnung nach den bestehenden Verfahren (Postversand oder in sonstiger vereinbarter Weise).

2.4 Format der Dokumente
Die Übermittlung der elektronischen Post erfolgt in geeigneten elektronischen Dateiformaten (z. B. im Format »Portable Document Format« (PDF)). Die Bank weist darauf hin, dass der Ausdruck elektronischer Dokumente eine Kopie darstellt und ggf. beweis- und steuerrechtlich einem Original nicht gleichgestellt ist.

2.5 Regelmäßige Kontrolle des Elektronischen Postfachs im KSO
Der Teilnehmer hat regelmäßig, mindestens alle 14 Tage sowie unverzüglich nach Erhalt einer E-Mail-Benachrichtigung den Inhalt des Elektronischen Postfachs im KSO zu überprüfen.

3. Änderung des Leistungsangebots
Die Bank ist berechtigt, das Elektronische Postfach im KSO inhaltlich und funktional weiterzuentwickeln, insbesondere weitere Leistungen in ihr Leistungsangebot aufzunehmen. Die Bank hat das Recht, ihr Leistungsangebot zum Elektronischen Postfach im KSO insgesamt, in Teilen oder auf bestimmte Zugänge und Legitimationsmedien zu beschränken, wenn ihr die Fortführung aus Gründen der IT-Sicherheit oder geänderter technischer oder rechtlicher Rahmenbedingungen, auf die sie keinen Einfluss hat, unzumutbar ist. Die Bank ist unter den gleichen Voraussetzungen berechtigt, das Elektronische Postfach im KSO den geänderten rechtlichen oder technischen Rahmenbedingungen anzupassen (z. B. die Formate der elektronischen Dokumente für die Zukunft zu modifizieren oder neue Sicherheitsverfahren, Signaturen etc. einzuführen). Über wesentliche Änderungen wird die Bank mindestens zwei Monate vor dem Inkrafttreten unter Hinweis auf das Kündigungsrecht des Teilnehmers nach Nr. 4 informieren. Die Bank ist berechtigt, das Elektronische Postfach im KSO in der Größe angemessen zu beschränken und bei Überschreiten der Größenbeschränkung den Funktionsumfang des Elektronischen Postfachs im KSO so lange einzuschränken, bis der Teilnehmer die Überschreitung einstellt (z. B. durch Löschen bisheriger Mitteilungen).

4. Kündigung
Der Teilnehmer ist berechtigt, das Elektronische Postfach im KSO insgesamt oder einzelne Leistungsangebote mit einer Kündigungsfrist von zwei Wochen zum Monatsende in Textform zu kündigen. Da der Zugriff auf das Elektronische Postfach im KSO nur mittels KSO möglich ist, stellt eine Kündigung der Rahmenvereinbarung über die Teilnahme am KSO durch den Teilnehmer auch eine Kündigung dieser Bedingungen über die Nutzung des Elektronischen Postfachs im KSO dar. Die Bank ist berechtigt, das Elektronische Postfach im KSO insgesamt oder einzelne Leistungsangebote mit einer Frist von zwei Monaten zu kündigen. Das Recht auf Kündigung aus wichtigem Grund bleibt davon unberührt. Nach Wirksamwerden der Kündigung stellt die Bank auf Postversand um. Der vom Teilnehmer jeweils abgeschlossene Kartenvertrag bleibt im Übrigen von einer Kündigung des Elektronischen Postfachs im KSO unberührt.

5. Änderungen
Diese Bedingungen für die Nutzung des Elektronischen Postfachs im KSO können zwischen dem Teilnehmer und der Bank durch entsprechende Vereinbarung wie nachfolgend beschrieben geändert werden: Die Bank übermittelt die geänderten Bedingungen vor dem geplanten Inkrafttreten in Text- oder Schriftform an den Teilnehmer und weist auf die Neuregelungen sowie das Datum des geplanten Inkrafttretens gesondert hin. Zugleich wird die Bank dem Teilnehmer eine angemessene, mindestens zwei Monate lange Frist für die Erklärung einräumen, ob er die geänderten Nutzungsbedingungen für die weitere Inanspruchnahme der Leistungen akzeptiert. Erfolgt innerhalb dieser Frist, welche ab Erhalt der Nachricht zu laufen beginnt, keine Erklärung, so gelten die geänderten Bedingungen als vereinbart. Die Bank wird den Teilnehmer bei Fristbeginn gesondert auf diese Rechtsfolge, d. h. das Widerspruchsrecht, die Widerspruchsfrist und die Bedeutung des Schweigens, hinweisen.

6. Steuerrechtliche Anerkennung
Für nicht buchführungspflichtige Kunden (i. d. R. Verbraucher) ist nach heutiger Rechtslage die steuerrechtliche Anerkennung von im Elektronischen Postfach des KSO bereitgestellten Kartenabrechnungen durch die Finanzverwaltung gewährleistet. Für buchführungspflichtige Kunden (i. d. R. Unternehmer) ist die steuerliche Anerkennung durch die Finanzverwaltung ebenfalls gewährleistet. Voraussetzung der Anerkennung ist jedoch, dass die elektronischen Kartenabrechnungen vom Steuerpflichtigen geprüft und dieses Vorgehen dokumentiert/protokolliert wird. Für die revisionssichere Archivierung ist der Steuerpflichtige verantwortlich.

Preise und Leistungen für die *Corporate*World Mastercard (Kreditkarte).

Fassung: 1. Januar 2023

BW BANK
Ein Unternehmen der LBBW-Gruppe

Jahrespreise: Ausgabe einer Kreditkarte

*Corporate*World Mastercard (Kreditkarte) mit Abrechnung über das Firmenkonto	
Classic (Kreditkarte) (jährlich)	28,00 EUR
Premium (Kreditkarte) (jährlich)	59,00 EUR
*Corporate*World Mastercard (Kreditkarte) mit Abrechnung über das Privatkonto	
Classic (Kreditkarte) (jährlich)	68,00 EUR
Premium (Kreditkarte) (jährlich)	99,00 EUR

Von diesem Jahrespreis abweichende Konditionen können sich aufgrund eines Rahmenvertrages zwischen der BW-Bank und dem Arbeitgeber ergeben. Der Arbeitgeber teilt diese Sonderkonditionen im Namen der BW-Bank dem Karteninhaber vor oder bei Vertragsabschluss mit.

Sonstige Preise:

Ersatz für eine	
– verlorene, gestohlene, missbräuchlich verwendete oder sonst nicht autorisiert genutzte Kreditkarte auf Verlangen des Kunden[1]	5,45 EUR
Zurverfügungstellung einer »emergency card« auf Verlangen des Kunden	kostenlos
Bereitstellung von »emergency cash« auf Verlangen des Kunden	kostenlos
Schadensersatz aufgrund der vergeblichen Ausführung von Lastschrifteinzügen von Fremdbankkonten, soweit vom Kunden zu vertreten. Dem Kunden steht es frei nachzuweisen, dass der Bank kein oder ein geringerer Schaden entstanden ist.	9,50 EUR zzgl. Fremdbankenentgelt
Postversand nicht abgerufener Kreditkartenabrechnungen bei Kartenservice Online	kostenlos
Erstellung einer zusätzlichen Rechnungskopie auf Verlangen des Kunden (soweit durch vom Kunden zu vertretende Umstände verursacht)	5,00 EUR
Bargeldauszahlung im Inland und Ausland[2),3)]:	
am Geldautomaten	2 % mind. 3,00 EUR
am Schalter	3 % mind. 5,00 EUR

Bitte beachten Sie, dass Betreiber von Geldautomaten oder fremde Kreditinstitute darüber hinaus eigene Gebühren erheben können. Diese Gebühren werden von der BW-Bank nicht erstattet.

Bestellung einer Wunsch-PIN:	
– Erstbestellung	kostenlos
– jede weitere Bestellung	je 4,90 EUR
Vereinbarungsgemäße Zurverfügungstellung einer Aktivierungs-PIN für eine nicht gesperrte Karte auf Verlangen des Kunden, soweit durch vom Kunden zu vertretende Umstände verursacht (z. B. Vergessen der PIN)	4,90 EUR
Einsatz der Kreditkarte im Ausland (Auslandseinsatzentgelt):	
Umsätze in EUR	0 % vom Umsatz
Umsätze in fremder Währung[4]	1,5 % vom Umsatz
Tägliches Verfügungslimit[5] für die Bargeldauszahlung an eigenen/fremden Geldautomaten (Bargeldservice):	500 EUR pro Tag

Ausführungsfrist:

Der Kartenzahlungsbetrag wird beim Zahlungsdienstleister des Zahlungsempfängers spätestens wie folgt eingehen:

Kartenzahlungen in Euro innerhalb des Europäischen Wirtschaftsraumes (EWR)	max. 1 Geschäftstag
Kartenzahlungen im EWR in einer anderen EWR-Währung als Euro	max. 4 Geschäftstage
Kartenzahlungen außerhalb des EWR unabhängig von der Währung	Die Kartenzahlung wird baldmöglichst bewirkt.

Annahmefrist:

Auftrag zur Rücküberweisung von Kreditkartenguthaben auf Abrechnungskonto	16:00 Uhr an Geschäftstagen

Geschäftstag ist jeder Tag, an dem die an der Ausführung eines Zahlungsvorgangs beteiligten Zahlungsdienstleister den für die Ausführung von Zahlungsvorgängen erforderlichen Geschäftsbetrieb unterhalten. Die Bank unterhält den für die Ausführung von Zahlungen erforderlichen Geschäftsbetrieb an allen Werktagen, mit Ausnahme von Samstagen, dem 24. und 31. Dezember, regionalen Feiertagen: Maßgeblich für die Bestimmung von regionalen Feiertagen ist der Feiertagskalender von Baden-Württemberg.

Währungsumrechnungskurs beim Auslandseinsatz:

Umsätze mit der Visa Card/Mastercard (Kreditkarte) innerhalb des EWR[6] in EWR-Fremdwährung[7] werden zum zuletzt verfügbaren Euro-Referenzwechselkurs der Europäischen Zentralbank (EZB) umgerechnet. Der jeweilige Euro-Referenzwechselkurs der EZB ist unter www.bw-bank.de/ezbkursreferenz abrufbar. Umsätze mit der Visa Card/Mastercard (Kreditkarte) in Drittstaatenwährung[8] werden zum jeweiligen Referenzwechselkurs von Visa umgerechnet. Dieser ist unter www.bw-bank.de/visakursreferenz abrufbar. Sofern Zahlungen in Landeswährung an die Empfängerländer wegen entgegenstehender Vorschriften oder wegen Abwicklungsschwierigkeiten nicht möglich sind, erfolgt die Umrechnung über eine zahlbare Drittwährung zum aktuell gültigen Referenzwechselkurs.

Hinweis auf die Möglichkeit der außergerichtlichen Streitbeilegung, der sonstigen Beschwerdemöglichkeiten und zivilrechtlichen Klage

Für die Beilegung von Streitigkeiten mit der Bank besteht für Verbraucher die Möglichkeit, sich an die beim Bundesverband Öffentlicher Banken Deutschlands (VÖB) eingerichtete Verbraucherschlichtungsstelle zu wenden. Bei Streitigkeiten über Zahlungsdienste und E-Geld können auch Nichtverbraucher (Geschäftskunden) die Schlichtungsstelle beim Bundesverband Öffentlicher Banken Deutschlands (VÖB) anrufen.

Die Beschwerde ist in Textform zu richten an:
Bundesverband Öffentlicher Banken Deutschlands (VÖB)
Verbraucherschlichtungsstelle
Postfach 11 02 72
10832 Berlin
Email: ombudsmann@voeb-kbs.de
Internet: www.voeb.de
Näheres regelt die Verfahrensordnung der vorgenannten Schlichtungsstelle, die auf Wunsch zur Verfügung gestellt wird. Die Bank nimmt am Streitbeilegungsverfahren vor dieser anerkannten Verbraucherschlichtungsstelle teil.

Streitbeilegung bei online abgeschlossenen Verträgen
Zur Beilegung von Streitigkeiten aus online abgeschlossenen Verträgen können sich Verbraucher alternativ an die Online-Plattform unter http://ec.europa.eu/odr wenden.

Bei behaupteten Verstößen gegen
– das Zahlungsdiensteaufsichtsgesetz,
– die §§ 675c bis 676c des Bürgerlichen Gesetzbuchs oder
– Artikel 248 des Einführungsgesetzes zum Bürgerlichen Gesetzbuch
kann auch Beschwerde bei der Bundesanstalt für Finanzdienstleistungsaufsicht eingelegt werden. Die Adressen lauten:
Bundesanstalt für Finanzdienstleistungsaufsicht
Graurheindorfer Straße 108, 53117 Bonn
und
Marie-Curie-Straße 24 – 28, 60439 Frankfurt am Main.

In den vorgenannten Fällen kann selbstverständlich auch Beschwerde bei der Bank selbst eingelegt werden. Die Bank beantwortet diese Beschwerden schriftlich oder auf einem anderen dauerhaften Datenträger.

Ferner besteht die Möglichkeit, den Rechtsweg zu beschreiten.

Zuständige Aufsichtsbehörde:

Für die Zulassung der Bank zuständige Aufsichtsbehörde:
Europäische Zentralbank, Sonnemannstraße 20
60314 Frankfurt am Main (Internet: www.ecb.europa.eu)

Für den Verbraucherschutz zuständige Aufsichtsbehörde:
Bundesanstalt für Finanzdienstleistungsaufsicht
Graurheindorfer Straße 108, 53117 Bonn und
Marie-Curie-Straße 24 – 28, 60439 Frankfurt am Main (Internet: www.bafin.de)

1) Wird nur berechnet, wenn der Kunde die Umstände, die zum Ersatz der Karte geführt haben, zu vertreten hat und die Bank nicht zur Ausstellung einer Ersatzkarte verpflichtet ist.
2) Zzgl. Auslandseinsatzentgelt bei Währungsumrechnung.
3) Lotto-, Wett- und Casinoumsätze werden wie Bargeldumsätze behandelt.
4) Dies gilt jedoch nicht für Verfügungen in Schweizer Franken, Norwegischen Kronen, Schwedischen Kronen und Rumänischen Lei.
5) Verfügungslimit kann bei fremden Geldautomaten, insbesondere im Ausland, geringer sein.
6) EWR-Staaten 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.
7) Zu den EWR-Fremdwährungen gehören derzeit: Bulgarischer Lew, Dänische Krone, Isländische Krone, Norwegische Krone, Polnischer Zloty, Rumänischer Leu, Schwedische Krone, Schweizer Franken (nur für Liechtenstein), Tschechische Krone, Ungarischer Forint.
8) Drittstaaten sind alle Staaten außerhalb des Europäischen Wirtschaftsraums (EWR).

*Corporate*World Mastercard Premium/Classic (Kreditkarte)

BW BANK
Ein Unternehmen der LBBW-Gruppe

Wer ist versichert: Inhaber einer gültigen *Corporate*World MasterCard Premium/Classic (Kreditkarte) unabhängig vom Karteneinsatz, auf Dienstreisen

Geltungsbereich: weltweit; Autoschutzbrief: geographisches Europa (Grenzen: im Westen die Azoren, im Norden das Nordkap, im Osten der Ural, im Südosten der Kaukasus und Bosporus)

Reisedauer: *Corporate*World MasterCard Classic (Kreditkarte): 45 Tage pro Reise
*Corporate*World MasterCard Premium (Kreditkarte): 90 Tage pro Reise (die Anzahl der Reisen pro Jahr ist für beide Karten unbegrenzt)

Teil	Leistungsbeschreibung	Höchstentschädigung je Schadensfall und versicherter Person	Classic	Premium
A Dienstreise - Krankenversicherung	Heilbehandlungen bei Krankheit und Unfall **inkl. Chiropraktiker/Heilpraktiker; Unterkunft, Verpflegung, Fahrtkosten** bis zur Transportfähigkeit; Krankenrücktransport, sinnvoll und vertretbar; **Psychologische Betreuung;** **Tod** im Ausland: wahlweise Kostenübernahme bei Bestattung vor Ort oder Überführung zum Bestattungsort	€ 1.000.000,- bis € 1.500,- bis € 1.500,- Selbstbehalt: € 50,- je Versicherungsfall	–	✓
B Dienstreise-Soforthilfe-Versicherung	**Notrufzentrale;** **Informationen zur ärztlichen Versorgung** im Reiseland; **Kostenvorschuss** gegenüber dem **Krankenhaus*;** **Such-, Rettungs- und Bergungskosten;** **Organisation der Überführung bzw. Bestattung im Ausland*;** **Arzneimittelversand*;** **Hilfe bei Auffindung oder Ersatzbeschaffung** von Reisedokumenten; **Vorstrecken von Gerichts- / Anwalts- / Dolmetscherkosten** und **Strafkautionskosten**	 bis € 15.000,- bis € 10.000,- bis € 2.500,- bis € 12.500,-	✓ *nicht enthalten	✓
C Dienstreise-Unfallversicherung	**Unfallversicherung** für **berufliche** und **außerberufliche Unfälle** auf Dienstreisen Leistung bei Invalidität und Tod Einschluss von **Koma**	Invalidität: € 100,000,-1 € 250,000,-² Tod: € 50,000,-1 € 150,000,-²	✓	✓
D Versicherung für Verspätungen auf Dienstreisen	**Kosten für Unterkunft und Verpflegung bei:** - mehr als 6h Verspätung eines öffentl. Verkehrsmittels **Notwendige Ersatzkäufe bei Gepäckverspätung:** - von mehr als 6h - von mehr als 48h (nur Hinreise)	 bis € 200.- bis € 200.- bis weitere € 300.-	–	✓
E Autoschutzbrief auf Dienstreisen	**Hilfe bei Pannen, Unfällen und Diebstahl** - Pannenhilfe am Schadenort - Ersatzteilbeschaffung und -versand - Erstattung zusätzlicher Mietwagen-, Übernachtungs- und Reisekosten	 bis € 250,- pro KFZ bis € 2.500,- pro KFZ	–	✓
F Mietwagen- & Opfer-Rechtsschutz auf Dienstreisen	Kostenübernahme für die Wahrnehmung rechtlicher Interessen im Zusammenhang mit dem Führen eines Mietwagens - Schadenersatz-Rechtsschutz - Rechtsschutz im Vertrags- und Sachenrecht - Verwaltungs-Rechtsschutz in Verkehrssachen - Straf-Rechtsschutz - Ordnungswidrigkeiten-Rechtsschutz Opferrechtschutz als Opfer einer Gewaltstraftat, insb. im Rahmen der Nebenklage*	Max. € 55.000,- Strafkaution max. € 30.000,- Selbstbehalt: € 150,- je Rechtsschutzfall	✓ *nicht enthalten	✓

Zusatzleistungen für Premium-Karteninhaber: Informationsübermittlung an Arbeitgeber und Angehörige in Notfällen. Auf Wunsch Besorgung von Blumen oder Geschenken (Feinkostartikel) und Organisation des Versands. Bei der Bestellung werden Details inkl. Preisrahmen besprochen. Der Versand innerhalb Deutschlands ist uneingeschränkt möglich, für den Versand ins Ausland sind insbesondere für Lebensmittel internationale Regelungen zu beachten. Ihre Bestellung ist verbindlich. Die Bezahlung erfolgt i. d. R. über Ihre Kreditkarte. Bestellen Sie unter dem Punkt "Versicherungen" über die Service Hotline 0711-124 46688.

Es gelten die Versicherungsbedingungen VB-ERV/CTI-CorporateWorld 2008 und die Bedingungen für den Mietwagen-Rechtsschutz - Auszug aus den D.A.S. ARB 2007.
Stand 08.2008

—Ausfertigung für den Kunden—

Baden-Württembergische Bank
Kleiner Schlossplatz 11
70173 Stuttgart
Steuer-Nr. 2899/014/09009
UST-IDNr. DE 147 800 343

BW BANK
Ein Unternehmen der LBBW-Gruppe

Meine persönlichen Angaben

Vorname, Name ☐ Frau ☐ Herr	Personen-Nr.
	Geburtsdatum, ggf. Geburtsname

Informationsbogen für den Einleger

Einlagen bei der Landesbank Baden-Württemberg (LBBW) sind geschützt durch:	Sicherungssystem der Sparkassen-Finanzgruppe(1)
Sicherungsobergrenze:	100.000 EUR pro Einleger pro Kreditinstitut(2) Die folgende Marke ist Teil Ihres Kreditinstituts: Baden-Württembergische Bank (BW-Bank)
Falls Sie mehrere Einlagen bei demselben Kreditinstitut haben:	Alle Ihre Einlagen bei demselben Kreditinstitut werden „aufaddiert“, und die Gesamtsumme unterliegt der Obergrenze von 100.000 EUR(2)
Falls Sie ein Gemeinschaftskonto mit einer oder mehreren anderen Personen haben:	Die Obergrenze von 100.000 EUR gilt für jeden einzelnen Einleger(3)
Erstattungsfrist bei Ausfall eines Kreditinstituts:	7 Arbeitstage
Währung der Erstattung:	Euro (EUR)
Kontaktdaten:	Sicherungssystem der Sparkassen-Finanzgruppe Adresse: Deutscher Sparkassen- und Giroverband e.V. Charlottenstraße 47 10117 Berlin Telefon: +49 30 20225-0 E-Mail: sicherungssystem@dsgv.de
Weitere Informationen:	http://www.dsgv.de
Empfangsbestätigung durch den Einleger:	✗

Zusätzliche Informationen:
(1) Ihr Kreditinstitut ist Teil eines institutsbezogenen Sicherungssystems, das als Einlagensicherungssystem amtlich anerkannt ist. Das heißt, alle Institute, die Mitglied dieses Einlagensicherungssystems sind, unterstützen sich gegenseitig, um eine Insolvenz zu vermeiden. Im Falle einer Insolvenz werden Ihre Einlagen bis zu 100.000 EUR erstattet.

(2) Sollte eine Einlage nicht verfügbar sein, weil ein Kreditinstitut seinen finanziellen Verpflichtungen nicht nachkommen kann, so werden die Einleger von dem Einlagensicherungssystem entschädigt. Die betreffende Deckungssumme beträgt maximal 100.000 Euro pro Kreditinstitut. Das heißt, dass bei der Ermittlung dieser Summe alle bei demselben Kreditinstitut gehaltenen Einlagen addiert werden. Hält ein Einleger beispielsweise 90.000 EUR auf einem Sparkonto und 20.000 EUR auf einem Girokonto, so werden ihm lediglich 100.000 EUR erstattet.

Diese Methode wird auch angewandt, wenn ein Kreditinstitut unter unterschiedlichen Marken auftritt. Die LBBW ist auch unter dem Namen BW-Bank tätig. Das heißt, dass die Gesamtsumme aller Einlagen bei einem oder mehreren dieser Marken in Höhe von bis zu 100.000 EUR gedeckt ist.

(3) Bei Gemeinschaftskonten gilt die Obergrenze von 100.000 EUR für jeden Einleger.
Einlagen auf einem Konto, über das zwei oder mehrere Personen als Mitglieder einer Personengesellschaft oder Sozietät, einer Vereinigung oder eines ähnlichen Zusammenschlusses ohne Rechtspersönlichkeit verfügen können, werden bei der Berechnung der Obergrenze von 100.000 EUR allerdings zusammengefasst und als Einlage eines einzigen Einlegers behandelt. In den Fällen des § 8 Absätze 2 bis 4 des Einlagensicherungsgesetzes sind Einlagen über 100.000 EUR hinaus gesichert. Weitere Informationen sind erhältlich über: http://www.dsgv.de.

(4) Erstattung:
Das zuständige Einlagensicherungssystem ist das Sicherungssystem der Sparkassen-Finanzgruppe
Adresse: Deutscher Sparkassen- und Giroverband e.V.
Charlottenstraße 47
10117 Berlin
Telefon: +49 30 20225-0
E-Mail: sicherungssystem@dsgv.de
Website: http://www.dsgv.de

Es werden Ihnen Ihre Einlagen (bis zu 100.000 EUR) innerhalb von 7 Arbeitstagen erstattet.

Haben Sie die Erstattung innerhalb dieser Fristen nicht erhalten, sollten Sie mit dem Einlagensicherungssystem Kontakt aufnehmen, da der Gültigkeitszeitraum für Erstattungsforderungen nach einer bestimmten Frist abgelaufen sein kann. Weitere Informationen sind erhältlich über: http://www.dsgv.de

Weitere wichtige Informationen:
Einlagen von Privatkunden und Unternehmen sind im Allgemeinen durch Einlagensicherungssysteme gedeckt. Für bestimmte Einlagen geltende Ausnahmen werden auf der Website des zuständigen Einlagensicherungssystems mitgeteilt. Ihr Kreditinstitut wird Sie auf Anfrage auch darüber informieren, ob bestimmte Produkte gedeckt sind oder nicht. Wenn Einlagen entschädigungsfähig sind, wird das Kreditinstitut dies auch auf dem Kontoauszug bestätigen.