BESONDERE GESCHÄFTSBEDINGUNGEN FÜR DIE TEILNAHME AM 3D SECURE VERFAHREN

Gegenüberstellung der geänderten Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren in der zuletzt mit Ihnen vereinbarten Fassung mit den Besondere Bedingungen für die Teilnahme am 3D Secure Verfahren in der Fassung Mai 2020. Die folgenden Klauseln sind geändert; alle übrigen Klauseln sind in beiden Fassungen gleich.

Die Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren sind aus Gründen der leichteren Lesbarkeit nicht geschlechterspezifisch formuliert. Sämtliche geschlechtsspezifischen Ausführungen gelten in gleicher Weise für alle Geschlechter.

FASSUNG OKTOBER 2018 STAND FEBRUAR 2019

Präambel

Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren (in der Folge kurz: BGB) ergänzen die jeweils gültigen Kreditkarten- und Prepaid-Bedingungen, die dem zwischen dem Karteninhaber (im Folgenden KI) und der kartenausgebenden Bank (im Folgenden „Bank“) geschlossenen Kreditkartenvertrag zugrunde liegen. Auf die Informationen gemäß § 48 Zahlungsdienstegesetz 2018 (ZaDiG 2018) sowie gemäß §§ 5 und 8 Fern-Finanzdienstleistungs-Gesetz (Fern-FinG), die der KI vor Abschluss des Kreditkartenvertrages erhalten hat, wird verwiesen.

Das 3D Secure Code Verfahren (bei Zahlungen mit MasterCard® “MasterCard SecureCode™”) ist ein System, das ausnahmslos im Internet für eCommerceTransaktionen zur Anwendung gelangt und dem Zweck dient, die Daten des KI und seine personalisierten Sicherheitsmerkmale vor der Ausspähung und missbräuchlichen Verwendung durch Dritte zu schützen. Es ist am Verbindungsprotokoll https (Hyper Text Transfer Protocol Secure) erkennbar. Das 3D Secure Verfahren (z.B. MasterCard SecureCode) gilt derzeit als sicheres System iSd Punktes III.6.3 der Kreditkarten- bzw. des Punktes II.5.2 der Prepaidkarten-Bedingungen der kartenausgebenden Bank. Die Registrierung zum 3D Secure Verfahren ist derzeit z.B. kostenlos auf www.bawagpsk.com möglich. Sofern der Karteninhaber im 3D Secure Verfahren registriert ist, ist ihm die Verwendung dieses sicheren Verfahrens bei Vertragsunternehmen, die ebenfalls das 3D Secure Verfahren anbieten, möglich. Diese BGB 3D Secure regeln ausschließlich die Teilnahme des KI am 3D Secure Verfahren. Sie gehen den Kreditkarten- und Prepaid-Bedingungen, soweit sie den Zahlungsvorgang abweichend regeln, vor.

Diese BB BGB 3D Secure regeln ausschließlich die Teilnahme des KI am 3D Secure Verfahren. Sie gehen den Kreditkartenbedingungen, soweit sie den Zahlungsvorgang abweichend regeln, vor.

Die Geschäftsbedingungen für Kreditkarten- bzw. der Prepaidkarten-Bedingungen der BAWAG P.S.K. sind auf der Webseite https://www.bawagpsk.com unter „Geschäftsbedingungen“ zu finden.

FASSUNG FEBRUAR 2020

Präambel

Die ~~Besonderen~~ Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren (~~in der Folge~~ kurz: ~~BGB)~~ BG 3D Secure) regeln die Abwicklung von Zahlungen mit BAWAG P.S.K. Kreditkarten unter Verwendung des 3D Secure Verfahrens. Die BG 3D Secure gelten, wenn ihre Geltung vereinbart ist.

Sie ergänzen die ~~jeweils gültigen~~ Geschäftsbedingungen für Kreditkarten~~- und Prepaid-Bedingungen,~~ der BAWAG P.S.K. (~~im Folgenden~~ kurz: Kreditkartenbedingungen), die zu dem zwischen dem Karteninhaber (~~im Folgenden~~ kurz: KI) und der ~~kartenausgebenden~~ BAWAG P.S.K. (~~im Folgenden~~ kurz: Bank) geschlossenen Kreditkartenvertrag ~~zugrunde liegen. Auf die Informationen gemäß § 48 Zahlungsdienstegesetz 2018 (ZaDiG 2018) sowie gemäß §§ 5 und 8 Fern-Finanzdienstleistungs-Gesetz (FernFinG), die der KI vor Abschluss des Kreditkarten-vertrages erhalten hat, wird verwiesen.~~ vereinbart sind.

~~Das 3D Secure Code Verfahren (bei Zahlungen mit MasterCard® “MasterCard SecureCode™”) ist ein System, das ausnahmslos im Internet für eCommerce Transaktionen zur Anwendung gelangt und dem Zweck dient, die Daten des KI und seine personalisierten Sicherheitsmerkmale vor der Ausspä-hung und missbräuchlichen Verwendung durch Dritte zu schützen. Es ist am Verbindungsprotokoll https (Hyper Text Transfer Protocol Secure) erkennbar. Das 3D Secure Verfahren (z.B. MasterCard SecureCode) gilt derzeit als sicheres System iSd Punktes III.6.3 der Kreditkarten- bzw. des Punktes II.5.2 der Prepaidkarten-Bedingungen der kartenausgebenden Bank. Die Registrierung zum 3D Secure Verfahren ist derzeit z.B. kostenlos auf www.bawagpsk.com möglich. Sofern der Karteninhaber im 3D Secure Verfahren registriert ist, ist ihm die Verwendung dieses sicheren Verfahrens bei Vertragsunternehmen, die eben-falls das 3D Secure Verfahren anbieten, möglich. Diese BGB 3D Secure regeln ausschließlich die Teilnahme des KI am 3D Secure Verfahren. Sie gehen den Kreditkarten- und Prepaid-Bedingungen, soweit sie den Zahlungsvorgang abweichend regeln, vor.~~

~~Diese BB BGB 3D Secure regeln ausschließlich die Teilnahme des KI am 3D Secure Verfahren. Sie gehen den Kreditkartenbedingungen, soweit sie den Zahlungsvorgang abweichend regeln, vor.~~

~~Die Geschäftsbedingungen für Kreditkarten- bzw. der Prepaidkarten-Bedingungen der BAWAG P.S.K. sind auf der Webseite https://www.bawagpsk.com unter „Geschäftsbedingungen“ zu finden.~~

Die BGB regeln die Anmeldung und die Abwicklung des Zahlungsverkehrs in sicheren Systemen. Die Registrierung zu 3D Secure Verfahren wird entweder vorab online auf der Website https://www.bawagpsk.com unter „3D Secure“ durchgeführt oder erfolgt während des Bezahlvorganges im Internet.

1. Definitionen

1.1 Mastercard SecureCode bzw. Verified by Visa Passwort – „Passwort“
Das im Zuge des 3D Secure Registrierungsverfahrens vom KI selbst gewählte Passwort, wird bei Mastercard als „Mastercard SecureCode“ bzw. bei Visa als „Verified by Visa Passwort“ bezeichnet.

1.2 Mobile Transaktionsnummer (kurz: „1x CODE“) Der 1x CODE ist ein auf ein mobiles Datenendgerät (z. B. Mobiltelefon, Tablet) übermittelte einmalig gültige Transaktionsnummer und dient als zusätzliches Kennwort bei Kartenzahlungen mit dem „Mastercard SecureCode“ bzw. „Verified by Visa Passwort“. Auch bei der Registrierung zum 3D Secure Verfahren, ist die Eingabe des 1x CODE erforderlich. Die Bank stellt auf der Website www.bawagpsk.com unter dem Menüpunkt „3D Secure“ weitere Informationen zur Verfügung.

1.3 Einmalpasswort
Das Einmalpasswort ist ein zufällig vergebenes Kennwort, welches zur Verifizierung des KIs während der Registrierung zum 3D Secure Verfahren dient. Im Zuge des 3D Secure Registrierungsprozesses wird das Einmalpasswort durch die Eingabe eines selbst gewählten, ausschließlich dem KI bekannten Passwortes (Mastercard SecureCode bzw. Verified by Visa Passwort) ersetzt.

1.4 Sichere Systeme
1.4.1 3D Secure Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das den KI zweifelsfrei als rechtmäßigen KI identifiziert.

1.4.2 Das Verbindungsprotokoll „https“ (Hypertext Transfer Protocol Secure) Dieses dient dem Zweck, die Daten des KIs und seine personalisierten Sicherheitsmerkmale für die Zwecke der Datenübertragung zu verschlüsseln und so vor der Ausspähung und missbräuchlichen Verwendung durch Dritte zu schützen.

~~Die BGB regeln die Anmeldung und die Abwicklung des Zahlungsverkehrs in sicheren Systemen. Die Registrierung zu 3D Secure Verfahren wird entweder vorab online auf der Website https://www.bawagpsk.com unter „3D Secure“ durchgeführt oder erfolgt während des Bezahlvorganges im Internet.~~

1. Definitionen

1.1 3D Secure
Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das die Voraussetzungen der starken Kundenauthentifizierung erfüllt.

1.~~1~~ 2 Mastercard ~~SecureCode~~ Identity Check bzw. ~~Verified by Visa~~ Visa Secure Passwort – „3D Secure Passwort“
Das ~~im Zuge des~~ 3D Secure ~~Registrierungsverfahrens~~ Passwort ist das im Zuge der Registrierung zum 3D Secure Verfahren vom KI selbst gewählte Passwort. Dieses wird bei Mastercard als „Mastercard ~~SecureCode~~“ Identity Check“ ~~bzw.~~ und bei Visa als ~~„Verified by Visa“~~ „Visa Secure Passwort“ bezeichnet und dient der Erteilung von Zahlungsaufträgen im Internet.

~~1.2~~ 1.3 „mobileTAN“
~~Mobile Transaktionsnummer (kurz: „1x CODE“) Der 1x CODE ist ein auf ein mobiles Datenendgerät (z. B. Mobiltelefon, Tablet) übermittelte einmalig gültige Transaktionsnummer und dient als zusätzliches Kennwort bei Kartenzahlungen mit dem „Mastercard SecureCode“ bzw. „Verified by Visa Passwort“. Auch bei der Registrierung zum 3D Secure Verfahren, ist die Eingabe des 1x CODE erforderlich. Die Bank stellt auf der Website www.bawagpsk.com unter dem Menüpunkt „3D Secure“ weitere Informationen zur Verfügung.~~

~~1.3 Einmalpasswort~~
~~Das Einmalpasswort ist ein zufällig vergebenes Kennwort, welches zur Verifizierung des KIs während der Registrierung zum 3D Secure Verfahren dient. Im Zuge des 3D Secure Registrierungsprozesses wird das Einmalpasswort durch die Eingabe eines selbst gewählten, ausschließlich dem KI bekannten Passwortes (Mastercard SecureCode bzw. Verified by Visa Passwort) ersetzt.~~

Die mobileTAN ist eine einmalig verwendbare Transaktionsnummer, die an die vom KI für die Zwecke der Zustellung der mobileTAN bekannt gegebene Mobiltelefonnummer per SMS gesendet wird. Die mobileTAN dient der Erteilung eines Zahlungsauftrages im Internet als zusätzliches Sicherheitsmerkmal zum 3D Secure Passwort. Auch bei der Registrierung zum 3D Secure Verfahren ist die Eingabe einer mobileTAN erforderlich.

~~1.4 Sichere Systeme~~
~~1.4.1 3D Secure Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das den KI zweifelsfrei als rechtmäßigen KI identifiziert.~~

~~1.4.2~~ ~~Das Verbindungsprotokoll „https“ (Hypertext Transfer Protocol Secure) Dieses dient dem Zweck, die Daten des KIs und seine personalisierten Sicherheitsmerkmale für die Zwecke der Datenübertragung zu verschlüsseln und so vor der Ausspähung und missbräuchlichen Verwendung durch Dritte zu schützen.~~

1.4 Authentifizierungscode
Der Authentifizierungscode ist ein Code, der bei starker Kundenauthentifizierung im Sinne der Delegierten Verordnung (EU) 2018/389 generiert wird und mit dem zu autorisierenden Schritt (z.B. mit dem zu autorisierenden Auftrag oder mit der abzugebenden Willenserklärung des KI) dynamisch verlinkt ist. Bei der mobileTAN handelt es sich um einen solchen Authentifizierungscode.

1.5 Starke Kundenauthentifizierung
Die starke Kundenauthentifizierung ist das in der Delegierten

2. Registrierung zum 3D Secure Verfahren

2.1 Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KIs für 3D Secure voraus. Diese kann entweder auf der Website www.bawagpsk.com gestartet werden oder die Registrierung wird während eines Online-Zahlungsvorganges bei einem Händler (Vertragsunternehmen), der am 3D Secure Verfahren teilnimmt, vorgenommen.

Auf der Website www.bawagpsk.com wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KIs im Zuge der Registrierung zum 3D Secure Verfahren sind alternativ entweder ein gültiges Einmalpasswort oder die Daten einer Kreditkartenabrechnung aus den letzten 6 Monaten sowie der 1x CODE erforderlich.

Der 1x CODE wird dem KI per SMS an die von ihm zuletzt bekannt gegebene Mobiltelefonnummer zur Kenntnis gebracht. Die Bank behält sich vor, zusätzliche Übermittlungswege für den 1x CODE anzubieten, welche auf der Website www.bawagpsk.com bekannt gegeben werden. Das Einmalpasswort wird im Umsatztext eines Umsatzes mit EUR 0,01 zugestellt.

2.2 Im Zuge der Registrierung zu 3D Secure werden dem KI diese BGB zur Verfügung gestellt. Für den weiteren Registrierungsvorgang ist es notwendig, dass der KI diese BGB an der vorgesehenen Stelle akzeptiert, womit eine Vereinbarung über die Teilnahme an sicheren Systemen (kurz: Vereinbarung) zustande kommt.

2.3 Folgende persönliche Identifikationsmerkmale sind vom KI im Zuge der Registrierung selbst festzulegen: Passwort (Mastercard SecureCode bzw. Verified by Visa Passwort) Persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt)

Der KI kann seine persönlichen Identifikationsmerkmale jederzeit selbst ändern. Hat der KI sein von ihm gewähltes Passwort vergessen, so hat er die Möglichkeit sich neuerlich gemäß Punkt 2.1 zu registrieren und kann im Rahmen dieser Passwort Erneuerung ein neues Passwort wählen.

Für die Nutzung des 3D Secure Services ist die Bekanntgabe der Mobiltelefonnummer und der E-Mail Adresse erforderlich. Allfällige aus dem SMS-Empfang entstehende Kosten hat der KI selbst zu tragen.

Verordnung (EU) 2018/389 geregelte Verfahren zur starken Kundenauthentifizierung. Die starke Kundenauthentifizierung basiert auf (mindestens) zwei Faktoren der Kategorien Wissen (z.B. Passwort), Besitz (z.B. Smartphone) und Inhärenz (z.B. Fingerabdruck, Gesichtserkennung) und zieht die Generierung eines Authentifizierungscodes nach sich.

2. Registrierung Zugang zum 3D Secure Verfahren

2.1 Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KIs für das 3D Secure Verfahren voraus. Diese kann ~~entweder~~ vom KI auf der Website ~~www.bawagpsk.com gestartet~~ www.bawagpsk.com/3dsecure beauftragt werden. ~~oder die Registrierung wird während eines Online-Zahlungsvorganges bei einem Händler (Vertragsunternehmen), der am 3D Secure Verfahren teilnimmt, vorgenommen.~~

2.2 ~~Auf der Website www.bawagpsk.com wird dem KI der Ablauf der Registrierung erklärt.~~ Für die Identifizierung des KIs im Zuge der Registrierung zum 3D Secure Verfahren ~~sind alternativ entweder~~ ist ein ~~gültiges Einmalpasswort oder~~ zusätzliches Sicherheitsmerkmal, welches die ~~Daten einer Kreditkartenabrechnung aus den letzten 6 Monaten~~ Bank bekannt gibt, sowie der ~~1x CODE~~ mobileTAN erforderlich.

~~Der 1x CODE wird dem KI per SMS an die von ihm zuletzt bekannt gegebene Mobiltelefonnummer zur Kenntnis gebracht. Die Bank behält sich vor, zusätzliche Übermittlungswege für den 1x CODE anzubieten, welche auf der Website www.bawagpsk.com bekannt gegeben werden. Das Einmalpasswort wird im Umsatztext eines Umsatzes mit EUR 0,01 zugestellt.~~

~~**2.2** Im Zuge der Registrierung zu 3D Secure werden dem KI diese BGB zur Verfügung gestellt. Für den weiteren Registrierungsvorgang ist es notwendig, dass der KI diese BGB an der vorgesehenen Stelle akzeptiert, womit eine Vereinbarung über die Teilnahme an sicheren Systemen (kurz: Vereinbarung) zustande kommt.~~

2.3 Folgende persönliche Identifikationsmerkmale sind vom KI im Zuge der Registrierung zum 3D Secure Verfahren selbst festzulegen:
* Passwort (Mastercard ~~SecureCode~~ Identity Check bzw. ~~Verified by~~ Visa Secure Passwort)
* persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt)

Der KI kann seine persönlichen Identifikationsmerkmale jederzeit selbst ändern. ~~Hat der KI sein von ihm gewähltes Passwort vergessen, so hat er die Möglichkeit sich neuerlich gemäß Punkt 2.1 zu registrieren und kann im Rahmen dieser Passwort Erneuerung ein neues Passwort wählen~~.

Für die Nutzung des 3D Secure Services ist ~~die Bekanntgabe der Mobiltelefonnummer und der E-Mail Adresse erforderlich. Allfällige aus dem SMS-Empfang entstehende Kosten hat der KI selbst zu tragen~~ es erforderlich, dass der KI seine Mobiltelefonnummer bekannt gibt.

3. Vertragsdauer, Kündigung und Beendigung

3.1 Diese Vereinbarung über das 3D Secure Verfahren wird auf unbestimmte Zeit geschlossen. Sie endet spätestens mit dem Ende des zugrunde liegenden Kartenvertrages.

3.2 Der KI ist berechtigt, die Vereinbarung jederzeit ohne Angabe von Gründen zu kündigen. Nach Einlangen der Kündigung wird die Bank den Zugriff auf das 3D Secure Verfahren sperren.

3.3 Die Bank ist berechtigt, die Vereinbarung jederzeit unter Einhaltung einer Frist von zwei Monaten ohne Angabe von Gründen zu kündigen.

3.4 Sowohl der KI als auch die Bank sind berechtigt, die Vereinbarung jederzeit bei Vorliegen eines wichtigen Grundes mit sofortiger Wirkung aufzulösen.

3.5 Die Beendigung der Vereinbarung lässt den Kreditkartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.

3.6 Die Vereinbarung endet automatisch mit dem Ende des Kreditkartenvertrages.

3. Zahlen mit sicheren Systemen

~~3.~~ 4. Zahlen mit ~~sicheren Systemen~~ 3D Secure

Zahlungstransaktionen im Internet führt der KI mit seinem selbst festgelegten 3D Secure Passwort und einer mobileTAN durch.

3.1 Im 3D Secure Verfahren erfolgt die Abgabe von Willenserklärungen sowie Anweisung einer Zahlung gemäß Punkt III.7.1 der Kreditkarten- bzw. Punkt II.7.1 der Prepaidkarten-Bedingungen der Bank durch die Eingabe der 16stelligen Kreditkartennummer, des Ablaufdatums der Kreditkarte, des rückseitigen dreistelligen CVC bzw. CVV Codes, die Eingabe eines nur dem KI bekannten selbstgewählten Passwortes sowie einer dem KI auf sein mobiles Endgerät zugesendeten 1x CODE.

~~**3.1** Im 3D Secure Verfahren erfolgt die Abgabe von Willenserklärungen sowie Anweisung einer Zahlung gemäß Punkt III.7.1 der Kreditkarten- bzw. Punkt II.7.1 der Prepaidkarten-Bedingungen der Bank durch die Eingabe der 16stelligen Kredit-kartennummer, des Ablaufdatums der Kreditkarte, des rückseitigen dreistelligen CVC bzw. CVV Codes, die Eingabe eines nur dem KI bekannten selbstgewählten Passwortes sowie einer dem KI auf sein mobiles Endgerät zugesendeten 1x CODE.~~

3.2 Der KI sollte bei der Verwendung der Karte im Internet (ECommerce), Zahlungsanweisungen in sicheren Systemen durchführen. Es handelt sich dabei um das 3D Secure Verfahren (Mastecard SecureCode oder Verified by Visa) und das Verbindungsprotokoll „https“ (Hypertext Transfer Protocol Secure). Voraussetzung ist, dass der Händler (Vertragsunternehmen) diese (technisch) ermöglicht.

~~**3.2** Der KI sollte bei der Verwendung der Karte im Internet (ECommerce), Zahlungsanweisungen in sicheren Systemen durchführen. Es handelt sich dabei um das 3D Secure Verfahren (Mastecard SecureCode oder Verified by Visa) und das Verbindungsprotokoll „https“ (Hypertext Transfer Protocol Secure). Voraussetzung ist, dass der Händler (Vertragsunternehmen) diese (technisch) ermöglicht.~~

3.3 Mit dem vom KI selbst festgelegten Passwort und dem 1x CODE kann der KI Zahlungstransaktionen in sicheren Systemen durchführen. Die per SMS übermittelten Daten sind vom KI vor Verwendung des 1x CODE auf ihre Richtigkeit zu prüfen. Nur bei Übereinstimmung der per SMS übermittelten Daten mit dem gewünschten Auftrag, darf der 1x CODE zur Auftragsbestätigung verwendet werden. Weichen die Daten in der SMS vom beabsichtigten Auftrag ab, hat der KI dies der Bank unverzüglich unter der Telefonnummer +43 599 05 – 83330 bekannt zu geben und den Zahlungsvorgang abzubrechen. Beendet der KI dennoch den Zahlungsvorgang, kann dies ein Mitverschulden für allfällige Schäden begründen.

~~**3.3** Mit dem vom KI selbst festgelegten Passwort und dem 1x CODE kann der KI Zahlungstransaktionen in sicheren Systemen durchführen. Die per SMS übermittelten Daten sind vom KI vor Verwendung des 1x CODE auf ihre Richtigkeit zu prüfen. Nur bei Übereinstimmung der per SMS übermittelten Daten mit dem gewünschten Auftrag, darf der 1x CODE zur Auftragsbestätigung verwendet werden. Weichen die Daten in der SMS vom beabsichtigten Auftrag ab, hat der KI dies der Bank unverzüglich unter der Telefonnummer +43 599 05 – 83330 bekannt zu geben und den Zahlungsvorgang abzubrechen. Beendet der KI dennoch den Zahlungsvorgang, kann dies ein Mitverschulden für allfällige Schäden begründen.~~

3.4 Sollte der Händler das Bezahlen mittels 3D Secure Verfahrens ermöglichen, ist der KI verpflichtet die Transaktionen im Rahmen des 3D Secure Verfahrens durchzuführen.

~~**3.4** Sollte der Händler das Bezahlen mittels 3D Secure Verfahrens ermöglichen, ist der KI verpflichtet die Transaktionen im Rahmen des 3D Secure Verfahrens durchzuführen.~~

3.5 Die Zahlungstransaktion, insbesondere die Anweisung, erfolgt auch bei Verwendung des sicheren Systems gemäß Punkt III.6.3 der Kreditkarten- bzw. Punkt II.5.2 der Prepaidkarten-Bedingungen der Bank. Wird jedoch das 3D Secure Verfahen verwendet, hat der KI sein von ihm selbst gewähltes Passwort und den 1x CODE einzugeben. Mit der Eingabe des Passwortes und dem für diesen Zahlungsvorgang generierten 1x CODE wird die Zahlungsanweisung unwiderruflich erteilt.

~~**3.5** Die Zahlungstransaktion, insbesondere die Anweisung, erfolgt auch bei Verwendung des sicheren Systems gemäß Punkt III.6.3 der Kreditkarten- bzw. Punkt II.5.2 der Prepaidkarten-Bedingungen der Bank. Wird jedoch das 3D Secure Verfahen verwendet, hat der KI sein von ihm selbst gewähltes Passwort und den 1x CODE einzugeben. Mit der Eingabe des Passwortes und dem für diesen Zahlungsvorgang generierten 1x CODE wird die Zahlungsanweisung unwiderruflich erteilt.~~

4. Geheimhaltung

Der KI ist verpflichtet die unter Punkt 2.3 angeführten persönlichen Identifikationsmerkmale und den 1x CODE so geheim zu halten, dass sie unbefugten Dritten nicht zugänglich sind. Im Fall einer schuldhaften Verletzung dieser Pflichten haftet der KI für allfällige Schäden, wobei die Haftung bei leichter Fahrlässigkeit auf den Betrag von EUR 50,00 beschränkt ist.

~~**4. Geheimhaltung**~~

~~Der KI ist verpflichtet die unter Punkt 2.3 angeführten persönlichen Identifikationsmerkmale und den 1x CODE so geheim zu halten, dass sie unbefugten Dritten nicht zugänglich sind. Im Fall einer schuldhaften Verletzung dieser Pflichten haftet der KI für allfällige Schäden, wobei die Haftung bei leichter Fahrlässigkeit auf den Betrag von EUR 50,00 beschränkt ist.~~

5. Sperre des Zugangs zum 3D Secure Verfahren

5.1 Die Bank ist berechtigt, den Zugang des KI zum 3D Secure Verfahren zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit der Kreditkarte oder des 3D Secure Verfahrens dies rechtfertigen; oder der Verdacht

5. Sperre des Zugangs zum 3D Secure Verfahren

5.1 Automatische Sperre

~~Die Bank ist berechtigt, den Zugang des KI zum 3D Secure Verfahren zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit der Kreditkarte oder des~~

einer nicht autorisierten oder betrügerischen Verwendung des 3D Secure Verfahrens besteht; oder wenn der KI seinen Zahlungspflichten gegenüber der Bank im Zusammenhang mit der Verwendung der Kreditkarte im 3D Secure Verfahren nicht nachgekommen ist und entweder die Erfüllung dieser Zahlungspflichten aufgrund einer Verschlechterung oder Gefährdung der Vermögensverhältnisse des KI oder eines Mitverpflichteten gefährdet ist oder beim KI die Zahlungsunfähigkeit eingetreten ist oder diese unmittelbar droht.

5.2 Aus Sicherheitsgründen wird nach sechsmaliger Falscheingabe des Passwortes der Zugang zum 3D Secure Verfahren von der Bank gesperrt. Solange die Sperre aufrecht ist, kann der KI keine Zahlungstransaktionen mit dem 3D Secure Verfahren durchführen. Der KI kann in diesem Fall die Aufhebung der Sperre schriftlich (per E-Mail) oder telefonisch bei der Bank beauftragen. Die Bank stellt dafür folgende Kontaktadressen zur Verfügung:
Telefon: +43 599 05 – 83330;
E-Mail: kundenservice@bawagpsk.com

5.3 Der KI kann die Bank jederzeit auffordern, seinen Zugang zum 3D Secure Verfahren zu sperren. Die Bank wird den Zugang zum 3D Secure Verfahren unverzüglich nach Eingang einer solchen Aufforderung sperren.

5.4 Sollte der KI wissen, oder den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen (insbesondere dem Passwort) erlangt haben, so empfiehlt die Bank die Identifikationsmerkmale zu ändern. Sollte dem KI dies, aus welchem Grund auch immer, nicht möglich sein, ist er berechtigt, von der Bank jederzeit die Sperre seines Zugangs zu verlangen. In diesem Fall ist die Bank verpflichtet, die Sperre unverzüglich nach Eingang der Aufforderung des KIs vorzunehmen.

5.5 Ist eine Sperre erfolgt, ist der KI nicht berechtigt, die Karte im Internet für Zahlungen bei VU, die das 3D Secure Verfahren anbieten, zu verwenden.

5.6 Will der KI nach einer erfolgten Sperre wieder am 3D Secure Verfahren teilnehmen, muss er sich erneut registrieren.

~~3D Secure Verfahrens dies rechtfertigen; oder der Verdacht einer nicht autorisierten oder betrügerischen Verwendung des 3D Secure Verfahrens besteht; oder wenn der KI seinen Zahlungspflichten gegenüber der Bank im Zusammenhang mit der Verwendung der Kreditkarte im 3D Secure Verfahren nicht nachgekommen ist und entweder die Erfüllung dieser Zahlungspflichten aufgrund einer Verschlechterung oder Gefährdung der Vermögensverhältnisse des KI oder eines Mitverpflichteten gefährdet ist oder beim KI die Zahlungsunfähigkeit eingetreten ist oder diese unmittelbar droht.~~

~~**5.2**~~ Aus Sicherheitsgründen wird nach ~~sechsmaliger Falscheingabe des Passwortes der Zugang zum~~ fünf Mal aufeinanderfolgender falscher Eingabe des 3D Secure Passworts das 3D Secure Verfahren von der Bank gesperrt. Solange die Sperre aufrecht ist, kann der KI keine Zahlungstransaktionen Zahlungsanweisungen mit dem 3D Secure Verfahren durchführen. ~~Der KI kann in diesem Fall die Aufhebung der Sperre schriftlich (per E-Mail) oder telefonisch bei der Bank beauftragen. Die Bank stellt dafür folgende Kontaktadressen zur Verfügung:~~
~~Telefon: +43 599 05 – 83330;~~
~~E-Mail: kundenservice@bawagpsk.com~~

~~5.3~~ 5.2 Sperre durch den KI
Der KI kann die ~~Bank jederzeit auffordern, seinen Zugang zum~~ Sperre des 3D Secure ~~Verfahren zu sperren. Die Bank wird den Zugang zum 3D Secure Verfahren unverzüglich nach Eingang einer solchen Aufforderung sperren.~~
Verfahrens durch die fünf Mal aufeinanderfolgende falsche Eingabe des 3D Secure Passworts selbst vornehmen oder telefonisch unter +43 (0)5 99 05-83330 veranlassen.

~~**5.4** Sollte der KI wissen, oder den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen (insbesondere dem Passwort) erlangt haben, so empfiehlt die Bank die Identifi-kationsmerkmale zu ändern. Sollte dem KI dies, aus welchem Grund auch immer, nicht möglich sein, ist er berechtigt, von der Bank jederzeit die Sperre seines Zugangs zu verlangen. In diesem Fall ist die Bank verpflichtet, die Sperre unverzüglich nach Eingang der Aufforderung des KIs vorzunehmen.~~

~~**5.5** Ist eine Sperre erfolgt, ist der KI nicht berechtigt, die Karte im Internet für Zahlungen bei VU, die das 3D Secure Verfahren anbieten, zu verwenden.~~

~~**5.6** Will der KI nach einer erfolgten Sperre wieder am 3D Secure Verfahren teilnehmen, muss er sich erneut registrieren.~~

5.3 Sperre durch die Bank
5.3.1 Die Bank ist berechtigt, das 3D Secure Verfahren für den KI zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit dies rechtfertigen oder der Verdacht einer nicht autorisierten oder betrügerischen Verwendung besteht.

5.3.2 Die Bank wird den KI über eine Sperre des 3D Secure Verfahrens und deren Gründe möglichst vor, spätestens aber unverzüglich nach der Sperre informieren, soweit die Bekanntgabe der Sperre oder die Gründe für die Sperre nicht eine gerichtliche oder verwaltungsbehördliche Anordnung verletzen bzw. österreichischen oder gemeinschaftsrechtlichen Rechtsnormen oder objektiven Sicherheitserwägungen zuwiderlaufen würde.

5.4. Bekanntgabe und Aufhebung der Sperre
5.4.1 Bevor eine Sperre dauerhaft wird, erhält der KI eine Warnung.
5.4.2 Die Bank wird eine Sperre gemäß Punkt 5.3. aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen. Die Bank wird den KI über die Aufhebung der Sperre unverzüglich informieren.
5.4.3 Der KI kann die Aufhebung einer Sperre telefonisch unter +43 (0)5 99 05-83330 beauftragen.

6. Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen

6.1 Sorgfaltspflichten
Der KI verpflichtet sich, sein 3D Secure Passwort geheim zu halten. Kommt dem KI das 3D Secure Passwort aus welchem Grund auch immer abhanden oder treten Umstände ein, die Kenntnis eines Dritten vom 3D Secure Passwort vermuten lassen, ist der KI verpflichtet, unverzüglich die Sperre seiner Registrierung oder seiner Kreditkarte zu veranlassen oder sein 3D Secure Passwort selbständig zu ändern und zu kontrollieren, ob es bereits zu missbräuchlicher Verwendung seiner Daten gekommen ist.

6.2 Solange der Zugang zu den sicheren Systemen gesperrt ist, kann die Karte nicht im Internet bei Händlern zur Zahlung verwendet werden, wenn diese nur das 3D Secure Verfahren als sicheres System anbieten. Die Bank empfiehlt daher die Sperre unter der Telefonnummer +43 599 05 – 83330 aufheben zu lassen.

6.3 Zur Vermeidung von Risiken, die mit der Kenntnis des Passwortes verbunden sind, empfiehlt die Bank, dieses regelmäßig (z.B. jeden Monat) zu ändern.

6.4 Es wird empfohlen, den Zugang zum Gebrauch der mobilen Datenendgeräte zu sichern. Bei Verlust oder Diebstahl des mobilen Datenendgerätes empfiehlt die Bank die Kontaktaufnahme mit dem Mobilfunkanbieter zur Sperre der SIM Karte.

6.5 Die Bank empfiehlt dem KI, die von ihm im Zuge des Zahlvorganges verwendeten Internetseiten so zu schließen, dass es einem unberechtigten Dritten nicht möglich ist, auf diese zugreifen zu können.

6.6 Die Bank empfiehlt dem KI, sein 3D Secure Passwort in elektronischen Medien nur dann zu speichern, wenn es durch geeignete Vorkehrungen (z.B. durch ein Passwort) vor einem unberechtigten Zugriff Dritter geschützt ist.

6.7 Zu beachten ist, dass die Verwendung von Passwörtern an gemeinsam benutzten Computern und mobilen Datenendgeräten (z. B. in einem Internetcafé, in einem Hotel, am Arbeitsplatz) unbefugten Dritten die Ausspähung von Passwörtern möglich macht.

6.8 Der Computer und mobile Datenendgeräte sollten über einen aktuellen Malware und Virenschutz, aktualisierte Betriebssoftware sowie eine Firewall verfügen. Dadurch kann das Risiko der Ausspähung und missbräuchlichen Verwendung durch Dritte minimiert werden. Die Online Services sollen jedes Mal mit der Logout-Funktion beendet werden.

6.9 Die Bank stellt auf der Website www.bawagpsk.com unter dem Menüpunkt „Sicherheitsportal der BAWAG P.S.K.“ weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.

6. Sorgfaltspflichten ~~und~~, empfohlene Sicherheitsmaßnahmen und Haftung

6.1 ~~Sorgfaltspflichten~~ Einhaltung und Rechtsfolgen
Jeder KI ist zur Einhaltung der in den Punkten 6.2. bis 6.4. enthaltenen Sorgfaltspflichten verpflichtet. KI, die Unternehmer sind, sind zusätzlich zur Einhaltung der in Punkt 6.5 empfohlenen Sicherheitsmaßnahmen verpflichtet. KI, die Verbraucher sind, empfiehlt die Bank die Einhaltung der empfohlenen Sicherheitsmaßnahmen, ohne dass Verbraucher zur Einhaltung verpflichtet sind. Eine Verletzung dieser Verpflichtungen kann gemäß Punkt 6.6 zu Schadenersatzpflichten des KI oder zum Entfall bzw. zur Minderung seiner Schadenersatzansprüche gegenüber der Bank führen.

~~**6.1 Sorgfaltspflichten**~~
~~Der KI verpflichtet sich, sein 3D Secure Passwort geheim zu halten. Kommt dem KI das 3D Secure Passwort aus welchem Grund auch immer abhanden oder treten Umstände ein, die Kenntnis eines Dritten vom 3D Secure Passwort vermuten lassen, ist der KI verpflichtet, unverzüglich die Sperre seiner Registrierung oder seiner Kreditkarte zu veranlassen oder sein 3D Secure Passwort selbständig zu ändern und zu kontrollieren, ob es bereits zu missbräuchlicher Verwendung seiner Daten gekommen ist.~~

~~**6.2** Solange der Zugang zu den sicheren Systemen gesperrt ist, kann die Karte nicht im Internet bei Händlern zur Zahlung verwendet werden, wenn diese nur das 3D Secure Verfahren als sicheres System anbieten. Die Bank empfiehlt daher die Sperre unter der Telefonnummer +43 599 05 – 83330 aufheben zu lassen.~~

~~**6.3** Zur Vermeidung von Risiken, die mit der Kenntnis des Passwortes verbunden sind, empfiehlt die Bank, dieses regelmäßig (z.B. jeden Monat) zu ändern.~~

~~**6.4** Es wird empfohlen, den Zugang zum Gebrauch der mobilen Datenendgeräte zu sichern. Bei Verlust oder Diebstahl des mobilen Datenendgerätes empfiehlt die Bank die Kontaktauf-nahme mit dem Mobilfunkanbieter zur Sperre der SIM Karte.~~

~~**6.5** Die Bank empfiehlt dem KI, die von ihm im Zuge des Zahlvorganges verwendeten Internetseiten so zu schließen, dass es einem unberechtigten Dritten nicht möglich ist, auf diese zugreifen zu können.~~

~~**6.6** Die Bank empfiehlt dem KI, sein 3D Secure Passwort in elektronischen Medien nur dann zu speichern, wenn es durch geeignete Vorkehrungen (z.B. durch ein Passwort) vor einem unberechtigten Zugriff Dritter geschützt ist.~~

~~**6.7** Zu beachten ist, dass die Verwendung von Passwörtern an gemeinsam benutzten Computern und mobilen Datenendgeräten (z. B. in einem Internetcafé, in einem Hotel, am Arbeitsplatz) unbefugten Dritten die Ausspähung von Passwörtern möglich macht.~~

~~**6.8** Der Computer und mobile Datenendgeräte sollten über einen aktuellen Malware und Virenschutz, aktualisierte Betriebssoft-ware sowie eine Firewall verfügen. Dadurch kann das Risiko der Ausspähung und missbräuchlichen Verwendung durch Dritte minimiert werden. Die Online Services sollen jedes Mal mit der Logout-Funktion beendet werden.~~

~~**6.9** Die Bank stellt auf der Website www.bawagpsk.com unter dem Menüpunkt „Sicherheitsportal der BAWAG P.S.K.“ weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.~~

6.2 Geheimhaltungs- und Sperrverpflichtung
6.2.1 Der KI hat sein 3D Secure Passwort geheim zu halten und darf dieses nicht an unbefugte Dritte weitergeben. Die Weitergabe des 3D Secure Passworts an Zahlungsauslösedienstleister und Kontoinformationsdienstleister ist jedoch

zulässig, soweit sie erforderlich ist, damit diese ihre Dienstleistungen für den KI erbringen können.

6.2.2 Der KI ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung seines 3D Secure Passworts walten zu lassen, um einen Missbrauch zu vermeiden. Der KI hat insbesondere darauf zu achten, dass sein 3D Secure Passwort bei deren Verwendung nicht ausgespäht wird.

6.2.3 Bei Verlust des 3D Secure Passworts sowie dann, wenn der KI von einer missbräuchlichen Verwendung oder einer sonstigen nicht autorisierten Nutzung des 3D Secure Verfahren Kenntnis erlangt hat, hat der KI die Sperre des 3D Secure Verfahrens unverzüglich zu veranlassen.

6.3 Sorgfaltspflichten zur Sperre des Endgeräts

Der KI ist verpflichtet, den Zugang zum Gebrauch des mobilen Endgerätes bzw. den Zugriff auf dort gespeicherte Daten für Nichtberechtigte zu sperren, wenn er das Endgerät nicht benutzt.

6.4 Sorgfaltspflichten bei Aufträgen

6.4.1 Zahlungsfreigabe mit mobileTAN

Die in der mobileTAN angezeigten Daten sind vom KI vor der Verwendung auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit dem gewünschten Zahlungsauftrag darf die mobileTAN zur Erteilung von Aufträgen verwendet werden.

6.5 Empfohlene Sicherheitsmaßnahmen bei der Verwendung des 3D Secure Zahlungsverfahrens

6.5.1 Dem KI wird empfohlen, das 3D Secure Passwort regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.

6.5.2 Dem KI wird empfohlen, unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis vom Passwort erlangt haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen könnten.

6.5.3 Dem KI wird empfohlen, sein mobiles Endgerät, auf welchem er die mobileTAN bekommt, hinsichtlich Risiken aus dem Internet abzusichern, insbesondere einen aktuellen Virenschutz zu verwenden und diesen am aktuellen Stand zu halten, sowie Sicherheitsupdates des Betriebssystems des mobilen Endgeräts durchzuführen.

6.6 Haftung des KI

6.6.1 Der KI haftet für den gesamten Schaden einer nicht autorisierten Onlinezahlung, welche er der Bank durch die vorsätzliche oder grob fahrlässige Verletzung der Sorgfaltspflichten gemäß den Punkten 6.2. bis 6.4. zugefügt hat. Hat der KI die Sorgfaltspflichten gemäß den Punkten 6.2. bis 6.4. weder in betrügerischer Absicht noch vorsätzlich verletzt, sind bei einer allfälligen Schadensteilung zwischen dem KI und der Bank insbesondere die Art der personalisierten Sicherheitsmerkmale sowie die besonderen Umstände, unter denen die missbräuchliche Verwendung der Karte stattgefunden hat, zu berücksichtigen.

6.6.2 War für den KI vor der Zahlung der Verlust oder Diebstahl seines 3D Secure Passworts oder die missbräuchliche Verwendung seiner Karte nicht bemerkbar, haftet er abweichend von Punkt 6.6.1. bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß den Punkten 6.2. bis 6.4. nicht. Der KI haftet bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß den Punkten 6.2. bis 6.4. auch dann nicht, wenn die Bank den Verlust des 3D Secure Passworts verursacht hat.

6.6.3 Abweichend von Punkt 6.6.1. haftet der KI nicht, wenn die Bank bei einer missbräuchlichen oder sonst nicht autorisierten Verwendung der Karte bei einer Onlinezahlung keine starke Kundenauthentifizierung verlangt hat (das

heißt, dass die Onlinezahlung ohne Verwendung des 3D Secure Verfahrens durchgeführt wurde). Wurde eine nicht autorisierte Onlinezahlung in betrügerischer Absicht durch den KI ermöglicht, so haftet der KI unabhängig davon, ob die Bank eine starke Kundenauthentifizierung verlangt hat oder nicht.

6.6.4 Der KI haftet nicht, wenn der Schaden aus einer nicht autorisierten Nutzung der Karte bei einer Onlinezahlung nach Beauftragung der Sperre gemäß Punkt 5. entstanden ist, es sei denn, der KI hat in betrügerischer Absicht gehandelt.

7. Vertragsdauer und Beendigung:

7.1 Die Vereinbarung wird auf unbestimmte Zeit geschlossen. Sie endet jedenfalls mit der Beendigung des zugrundeliegenden Kartenvertrages oder Beendigung oder Einstellung des 3D Secure Verfahrens, worüber die Bank den KI unverzüglich informiert.

7.2 Kündigung durch den KI
Der KI ist berechtigt, das Vertragsverhältnis jederzeit ohne Angabe von Gründen zum letzten Tag des laufenden Monats kostenlos zu kündigen, wobei aber Kündigungen, die am letzten Geschäftstag eines Monats ausgesprochen werden, erst zum ersten Geschäftstag des folgenden Monats wirken. Bestehende Verpflichtungen werden durch die Kündigung nicht berührt und sind zu erfüllen. Die Möglichkeit einer sofortigen Beendigung des 3D Secure Verfahrens durch den KI aus wichtigem Grund und das Recht zur Kündigung anlässlich einer von der Bank vorgeschlagenen Änderung der Leistung oder der BGB 3D Secure (Punkt 6. Und 7.) bleiben unberührt.

7.3 Kündigung durch die BAWAG P.S.K.
Die Bank ist berechtigt, das 3D Secure Verfahren unter Einhaltung einer Frist von zwei Monaten zu kündigen. Bei Vorliegen eines wichtigen Grundes ist die Bank berechtigt, das 3D Secure Verfahren jederzeit mit sofortiger Wirkung zu kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn der KI seinen Zahlungsverpflichtungen nicht nachgekommen ist.

7. ~~Vertragsdauer und Beendigung~~ Änderungen der Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren
~~**7.1** Die Vereinbarung wird auf unbestimmte Zeit geschlossen. Sie endet jedenfalls mit der Beendigung des zugrundeliegenden Kartenvertrages oder Beendigung oder Einstellung des 3D Secure Verfahrens, worüber die Bank den KI unverzüglich informiert.~~

~~**7.2** Kündigung durch den KI~~
~~Der KI ist berechtigt, das Vertragsverhältnis jederzeit ohne Angabe von Gründen zum letzten Tag des laufenden Monats kostenlos zu kündigen, wobei aber Kündigungen, die am letzten Geschäftstag eines Monats ausgesprochen werden, erst zum ersten Geschäftstag des folgenden Monats wirken. Bestehende Verpflichtungen werden durch die Kündigung nicht berührt und sind zu erfüllen. Die Möglichkeit einer sofortigen Beendigung des 3D Secure Verfahrens durch den KI aus wichtigem Grund und das Recht zur Kündigung anlässlich einer von der Bank vorgeschlagenen Änderung der Leistung oder der BGB 3D Secure (Punkt 6. Und 7.) bleiben unberührt.~~

~~**7.3 Kündigung durch die BAWAG P.S.K.**~~
~~Die Bank ist berechtigt, das 3D Secure Verfahren unter Einhaltung einer Frist von zwei Monaten zu kündigen. Bei Vorliegen eines wichtigen Grundes ist die Bank berechtigt, das 3D Secure Verfahren jederzeit mit sofortiger Wirkung zu kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn der KI seinen Zahlungsverpflichtungen nicht nachgekommen ist.~~

7.1 Änderungen der GB 3D Secure werden dem KI von der Bank mindestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens angeboten; dabei werden die vom Änderungsangebot betroffenen Bestimmungen und die vorgeschlagenen Änderungen dieser Geschäftsbedingungen in einer dem Änderungsangebot angeschlossenen Gegenüberstellung (im Folgenden „Gegenüberstellung“) dargestellt. Das Änderungsangebot wird dem KI mitgeteilt. Die Zustimmung des KI gilt als erteilt, wenn vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens kein schriftlicher oder in einer mit dem KI vereinbarten Weise elektronisch (z.B. per E-Mail oder über das e-Postfach im eBanking) erklärter Widerspruch des KI bei der Bank einlangt.
Die Bank wird den KI im Änderungsangebot darauf aufmerksam machen, dass sein Stillschweigen durch das Unterlassen eines schriftlichen oder in einer mit dem KI vereinbarten Weise elektronisch erklärten Widerspruchs als Zustimmung zu den Änderungen gilt, sowie dass der KI, der Verbraucher ist, das Recht hat, sowohl die Vereinbarung zur Teilnahme am 3D Secure Verfahren als auch den Kreditkartenvertrag vor Inkrafttreten der Änderungen kostenlos fristlos zu kündigen. Außerdem wird die Bank die Gegenüberstellung sowie die vollständige Fassung der neuen Geschäftsbedingungen auf ihrer Internetseite veröffentlichen und dem KI über sein Ersuchen die vollständige Fassung der neuen Geschäftsbedingungen übersenden; auch darauf wird die Bank im Änderungsangebot hinweisen.

7.2 Die Mitteilung an den KI über die angebotenen Änderungen kann in jeder Form erfolgen, die mit ihm vereinbart

ist. Eine solche Form ist auch die Übermittlung des Änderungsangebots samt Gegenüberstellung an die der Bank vom KI bekannt gegebene E-Mail-Adresse oder in das e-Postfach im eBanking, wobei der KI über das Vorhandensein des Änderungsangebots in seinem e-Postfach auf die mit ihm vereinbarte Weise (Push-Nachricht, SMS, E-Mail, Post oder sonst vereinbarte Form) informiert werden wird.

7.3 Die Änderung dieser Geschäftsbedingungen ist auf sachlich gerechtfertigte Fälle beschränkt; eine sachliche Rechtfertigung liegt dann vor,
(i) wenn die Änderung durch eine Änderung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen gesetzlichen Bestimmungen oder durch Vorgaben der Finanzmarktaufsicht, der Europäischen Bankenaufsichtsbehörde, der Europäischen Zentralbank oder der Österreichischen Nationalbank erforderlich ist,
(ii) wenn die Änderung durch die Entwicklung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen Judikatur erforderlich ist,
(iii) wenn die Änderung die Sicherheit des Bankbetriebs oder die Sicherheit der Abwicklung der Geschäftsverbindung mit dem KI über die Teilnahme am 3D Secure Verfahren fördert,
(iv) wenn die Änderung zur Umsetzung technischer Entwicklungen oder zur Anpassung an neue Programme zur Nutzung von Endgeräten erforderlich ist,
(v) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für die Erteilung von Aufträgen und für die Abgabe von Erklärungen über die Teilnahme am 3D Secure erforderlich ist,
(vi) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für jene Bankgeschäfte, welche der KI über das 3D Secure Verfahren abwickeln kann, erforderlich ist.
Die Einführung von Entgelten oder die Änderung vereinbarter Entgelte durch eine Änderung dieser BB 3D Secure ist ausgeschlossen.

8. Änderungen der BGB und der Adresse

8.1 Änderungen dieser BGB 3DSecure gelten nach Ablauf von zwei Monaten ab Zugang der Mitteilung der angebotenen Änderungen an den KI als vereinbart, sofern bis dahin kein Widerspruch des KI bei der Bank einlangt. Die Bank wird den KI in der Mitteilung auf die Änderungen hinweisen und darauf aufmerksam machen, dass sein Stillschweigen nach Ablauf der zwei Monate ab Zugang der Mitteilung als Zustimmung zur Änderung gilt. Außerdem wird die Bank eine Gegenüberstellung über die von der Änderung der BGB 3D Secure betroffenen Bestimmungen sowie die vollständige Fassung der neuen BGB 3D Secure auf seiner Internetseite veröffentlichen und die Gegenüberstellung dem KI auf sein Verlangen zur Verfügung stellen. Darauf wird die Bank in der Mitteilung hinweisen.

8.2 Im Falle einer solchen beabsichtigten Änderung der BGB 3D Secure hat der KI das Recht, seinen Vertrag über die Teilnahme am 3D Secure Verfahren vor dem Inkrafttreten der Änderung kostenlos fristlos zu kündigen.

8.3 Die Mitteilung an den Kontoinhaber über die angebotenen Änderungen kann in jeder Form erfolgen, die mit ihm vereinbart ist. Eine solche Form ist auch die Übermittlung des Änderungsangebots samt Gegenüberstellung an das im BAWAG P.S.K. eBanking des Kontoinhabers eingerichtete ePostfach, wobei der Kontoinhaber über das Vorhandensein des Änderungsangebots in seinem ePostfach in der mit ihm vereinbarten Weise (SMS, Email, Post oder sonstige vereinbarte Form) informiert werden wird. Im Übrigen gelten die Bestimmungen des Punktes III.16. der Kreditkarten- bzw. des Punktes II.18. der Prepaidkarten-Bedingungen der Bank sinngemäß.

8.4 Änderung der Mobiltelefonnummer des KIs. Der KIs verpflichtet sich, jede Änderung seiner Mobiltelefonnummer der Bank schriftlich oder per E-Mail bekannt zu geben.

8. ~~Änderungen der BGB und der Adresse~~ Änderung der Mobiltelefonnummer des KI

~~**8.1** Änderungen dieser BGB 3DSecure gelten nach Ablauf von zwei Monaten ab Zugang der Mitteilung der angebotenen Änderungen an den KI als vereinbart, sofern bis dahin kein Widerspruch des KI bei der Bank einlangt. Die Bank wird den KI in der Mitteilung auf die Änderungen hinweisen und darauf aufmerksam machen, dass sein Stillschweigen nach Ablauf der zwei Monate ab Zugang der Mitteilung als Zustimmung zur Änderung gilt. Außerdem wird die Bank eine Gegenüberstellung über die von der Änderung der BGB 3D Secure betroffenen Bestimmungen sowie die vollständige Fassung der neuen BGB 3D Secure auf seiner Internetseite veröffentlichen und die Gegenüberstellung dem KI auf sein Verlangen zur Verfügung stellen. Darauf wird die Bank in der Mitteilung hinweisen.~~

~~**8.2** Im Falle einer solchen beabsichtigten Änderung der BGB 3D Secure hat der KI das Recht, seinen Vertrag über die Teilnahme am 3D Secure Verfahren vor dem Inkrafttreten der Änderung kostenlos fristlos zu kündigen.~~

~~**8.3** Die Mitteilung an den Kontoinhaber über die angebotenen Änderungen kann in jeder Form erfolgen, die mit ihm vereinbart ist. Eine solche Form ist auch die Übermittlung des Änderungs-angebots samt Gegenüberstellung an das im BAWAG P.S.K. eBanking des Kontoinhabers eingerichtete ePostfach, wobei der Kontoinhaber über das Vorhandensein des Änderungsangebots in seinem ePostfach in der mit ihm vereinbarten Weise (SMS, Email, Post oder sonstige vereinbarte Form) informiert werden wird. Im Übrigen gelten die Bestimmungen des Punktes III.16. der Kreditkarten- bzw. des Punktes II.18. der Prepaidkarten-Bedingungen der Bank sinngemäß.~~

~~**8.4** Änderung der Mobiltelefonnummer des KIs. Der KIs verpflichtet sich, jede Änderung seiner Mobiltelefonnummer der Bank schriftlich oder per E-Mail bekannt zu geben.~~

9. Änderungen der vereinbarten Leistungen

9.1 Änderungen der von der Bank dem KI zu erbringenden Dauerleistungen werden dem KI von der Bank spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens angeboten. Die Zustimmung des KI zu diesen Änderungen gilt als erteilt, wenn bei der Bank vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens kein schriftlicher Widerspruch des KI einlangt. Darauf wird die Bank den KI im Änderungsangebot hinweisen. Der Kunde hat das Recht, diese Vereinbarung über die Teilnahme am 3D Secure Verfahren bis zum Inkrafttreten der Änderung kostenlos fristlos zu kündigen. Auch darauf wird die Bank im Änderungsangebot hinweisen. Das Änderungsangebot ist dem KI von der Bank mitzuteilen. Die Mitteilung an den KI kann schriftlich (insbesondere durch Benachrichtigung auf einer Kreditkartenabrechnung), durch Einstellen einer elektronischen Nachricht in das elektronische Postfach oder über die elektronische Kreditkartenabrechnung erfolgen.

9.2 Die Mitteilung an den Kontoinhaber über die angebotenen Änderungen kann in jeder Form erfolgen, die mit ihm vereinbart ist. Eine solche Form ist auch die Übermittlung des Änderungsangebots samt Gegenüberstellung an das im BAWAG P.S.K. eBanking des Kontoinhabers eingerichtete ePostfach, wobei der Kontoinhaber über das Vorhandensein des Änderungsangebots in seinem ePostfach in der mit ihm vereinbarten Weise (SMS, Email, Post oder sonstige vereinbarte Form) informiert werden wird.

9.3 Auf dem in Punkt 9.1 vereinbarte Wege, dürfen nur Leistungsänderungen vorgenommen werden, die unter Berücksichtigung aller Umstände sachlich gerechtfertigt sind. Als sachlich gerechtfertigt gelten Leistungsänderungen aufgrund der Änderung der vorherrschenden Kundenbedürfnisse, gesetzlicher und aufsichtsbehördlicher Anforderungen, der Sicherheit des Bankbetriebs oder der technischen Entwicklung.

Der KI verpflichtet sich, jede Änderung seiner Mobiltelefonnummer der Bank schriftlich oder per E-Mail bekannt zu geben. Die Bestimmung des Punktes 16. der Geschäftsbedingungen für Kreditkarten der BAWAG P.S.K. bleibt hiervon unberührt.

9. ~~Änderungen der vereinbarten Leistungen~~ Sicherheitshinweise

~~**9.1** Änderungen der von der Bank dem KI zu erbringenden Dauerleistungen werden dem KI von der Bank spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens angeboten. Die Zustimmung des KI zu diesen Änderungen gilt als erteilt, wenn bei der Bank vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens kein schriftlicher Widerspruch des KI einlangt. Darauf wird die Bank den KI im Änderungsangebot hinweisen. Der Kunde hat das Recht, diese Vereinbarung über die Teilnahme am 3D Secure Verfahren bis zum Inkrafttreten der Änderung kostenlos fristlos zu kündigen. Auch darauf wird die Bank im Änderungsangebot hinweisen. Das Änderungsangebot ist dem KI von der Bank mitzuteilen. Die Mitteilung an den KI kann schriftlich (insbesondere durch Benachrichtigung auf einer Kreditkartenabrechnung), durch Einstellen einer elektronischen Nachricht in das elektronische Postfach oder über die elektronische Kreditkartenabrechnung erfolgen.~~

~~**9.2** Die Mitteilung an den Kontoinhaber über die angebotenen Änderungen kann in jeder Form erfolgen, die mit ihm vereinbart ist. Eine solche Form ist auch die Übermittlung des Änderungs-angebots samt Gegenüberstellung an das im BAWAG P.S.K. eBanking des Kontoinhabers eingerichtete ePostfach, wobei der Kontoinhaber über das Vorhandensein des Änderungsangebots in seinem ePostfach in der mit ihm vereinbarten Weise (SMS, Email, Post oder sonstige vereinbarte Form) informiert werden wird.~~

~~**9.3** Auf dem in Punkt 9.1 vereinbarte Wege, dürfen nur Leis-tungsänderungen vorgenommen werden, die unter Berücksichtigung aller Umstände sachlich gerechtfertigt sind. Als sachlich gerechtfertigt gelten Leistungsänderungen aufgrund der Änderung der vorherrschenden Kundenbedürfnisse, gesetzlicher und aufsichtsbehördlicher Anforderungen, der Sicherheit des Bank-betriebs oder der technischen Entwicklung.~~

9.1 Solange der Zugang zum 3D Secure Verfahren gesperrt ist, kann die Karte nicht im Internet bei Händlern zur Zahlung verwendet werden, wenn diese das 3D Secure Verfahren anbieten.
9.2 Zur Vermeidung von Risiken, die mit der Kenntnis des 3D Secure Passworts verbunden sind, empfiehlt die Bank, dieses regelmäßig (z. B. jeden Monat) zu ändern.
9.3 Sollte der KI den Verdacht haben, dass Dritte Kenntnis von seinem 3D Secure Passwort erlangt haben, so empfiehlt die Bank dieses zu ändern.
9.4 Es wird empfohlen, den Zugang zum Gebrauch der mobilen Datenendgeräte zu sichern. Bei Verlust oder Diebstahl des mobilen Datenendgeräts empfiehlt die Bank die Kontaktaufnahme mit dem Mobilfunkanbieter zur Sperre der SIM Karte.
9.5 Zu beachten ist, dass die Verwendung von Passwörtern an gemeinsam benutzten Computern und mobilen Datenendgeräten (z. B. in einem Internetcafé, in einem Hotel, am Arbeitsplatz) unbefugten Dritten die Ausspähung von Passwörtern möglich macht.
9.6 Die Bank stellt auf der Website www.bawagpsk.com/3dsecure weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.