BESONDERE GESCHÄFTSBEDINGUNGEN FÜR DIE TEILNAHME AM 3D SECURE VERFAHREN (IM FOLGENDEN BG 3D SECURE)

FASSUNG Mai 2020, STAND JULI 2022

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

Präambel
Die Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren (kurz: BG 3D Secure) regeln die Abwicklung von Zahlungen mit BAWAG Kreditkarten unter Verwendung des 3D Secure Verfahrens. Die BG 3D Secure gelten, wenn ihre Geltung vereinbart ist.

Sie ergänzen die Geschäftsbedingungen für Kreditkarten der BAWAG (kurz: Kreditkartenbedingungen), die zu dem zwischen dem Karteninhaber (kurz: KI) und der BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (kurz: Bank) geschlossenen Kreditkartenvertrag vereinbart sind.

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.

1.2 Mastercard Identity Check bzw. Visa Secure Passwort – „3D Secure Passwort"
Das 3D Secure Passwort ist das im Zuge der Registrierung zum 3D Secure Verfahren vom KI selbst gewählte Passwort. Dieses wird bei Mastercard als „Mastercard Identity Check" und bei Visa als „Visa Secure Passwort" bezeichnet und dient der Erteilung von Zahlungsaufträgen im Internet.

1.3 „mobileTAN"
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 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 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. Zugang zum 3D Secure Verfahren
2.1 Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KI für das 3D Secure Verfahren voraus. Diese kann vom KI auf der Website www.bawag.at/3dsecure beauftragt werden.

2.2 Für die Identifizierung des KI im Zuge der Registrierung zum 3D Secure Verfahren ist ein zusätzliches Sicherheitsmerkmal, welches die Bank bekannt gibt, sowie der mobileTAN erforderlich

2.3 Folgende persönliche Identifikationsmerkmale sind vom KI im Zuge der Registrierung zum 3D Secure Verfahren selbst festzulegen:
* Passwort (Mastercard Identity Check bzw. Visa Secure Passwort)
* persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt)
Der KI kann seine persönlichen Identifikationsmerkmale jederzeit selbst ändern. Für die Nutzung des 3D Secure Services ist 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.

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

5. Sperre des Zugangs zum 3D Secure Verfahren
5.1 Automatische Sperre
Aus Sicherheitsgründen wird nach 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 Zahlungsanweisungen mit dem 3D Secure Verfahren durchführen.

5.2 Sperre durch den KI
Der KI kann die Sperre des 3D Secure Verfahrens durch die fünf Mal aufeinanderfolgende falsche Eingabe des 3D

Secure Passworts selbst vornehmen oder telefonisch unter +43 (0)5 99 05-83330 veranlassen.

5.3 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, empfohlene Sicherheitsmaßnahmen und Haftung
6.1 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 Schadener-satzansprüche gegenüber der Bank führen.

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. Änderungen der Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren
7.1 Änderungen der BG 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 ePostfach im eBanking) erklärter Widerspruch des KI bei der Bank einlangt.
Die Bank wird den KI im Änderungsangebot darauf aufmerk-

sam 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 ePostfach im eBanking, wobei der KI über das Vorhandensein des Änderungsangebots in seinem ePostfach 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 Judi katur 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 BG 3D Secure ist ausgeschlossen.

8. Änderung der Mobiltelefonnummer des KI

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 bleibt hiervon unberührt.

9. Sicherheitshinweise

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.bawag.at/3dsecure weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.