Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten

Diese Bedingungen sind aus Gründen der leichteren Lesbarkeit nicht geschlechterspezifisch formuliert und gelten in gleicher Weise für alle Geschlechter.

Präambel

Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten (in der Folge kurz: BGB) regeln die Abwicklung von Zahlungen mit wiederaufladbaren PayLife Wertkarten unter Verwendung des 3D Secure Verfahrens. Die BGB gelten, wenn ihre Geltung vereinbart ist. Sie ergänzen die Allgemeinen Geschäftsbedingungen für wiederaufladbare PayLife Wertkarten (kurz: AGB), die zu dem zwischen easybank AG (kurz: Bank) und dem Karteninhaber (kurz: KI) geschlossenen Kartenvertrag über die Ausgabe einer wiederaufladbaren PayLife Wertkarte vereinbart sind.

1. Definitionen

1.1. Mastercard Identity Check
Das im Zuge des 3D Secure Registrierungsverfahrens vom KI selbst gewählte Passwort.

1.2. Mobile Transaktionsnummer (kurz: mobileTAN)
Die mobileTAN ist eine einmalig gültige Transaktionsnummer und dient als zusätzliches Kennwort bei Kartenzahlungen mit dem Mastercard Identity Check Passwort. Auch bei der Registrierung zum 3D Secure Verfahren und bei bestimmten Datenänderungen in der 3D Secure Kontoverwaltung, ist die Eingabe einer mobileTAN erforderlich. Die Bank sendet die mobileTAN an die vom KI für die Zwecke der Zustellung bekannt gegebene Mobiltelefonnummer per SMS.

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 Identity Check) ersetzt.

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.

1.6. 3D Secure
Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das die Voraussetzungen der starken Kundenauthentifizierung erfüllt.

2. Registrierung zum 3D Secure Verfahren

2.1. Registrierung
Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KIs für 3D Secure voraus. Die Registrierung kann auf der Website www.paylife.at/3dsecure gestartet werden.

Auf der Website www.paylife.at/3dsecure wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KIs im Zuge der Registrierung zum 3D Secure Verfahren sind ein gültiges Einmalpasswort sowie eine mobileTAN erforderlich.

Die mobileTAN für die Registrierung wird dem KI per SMS an die von ihm zuletzt bekannt gegebene Mobiltelefonnummer oder auf einem anderen, im Zuge des Registrierungsprozesses festgelegten Weg zur Kenntnis gebracht.

Das Einmalpasswort wird in jener Form, welche der KI selbst im Registrierungsprozess gewählt hat (z. B. per E-Mail oder SMS), zugestellt.

2.2. Der KI hat im Zuge der Registrierung folgendes selbst festzulegen:

- Benutzername
- Passwort (Mastercard Identity Check)
- persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt)

Der KI kann seinen Benutzernamen, sein Passwort und seine persönliche Begrüßung 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 Empfang von SMS oder aus dem Internetzugang entstehende Kosten hat der KI selbst zu tragen.

3. Zahlen mit 3D Secure

3.1. Im Rahmen des 3D Secure Verfahrens führt der KI Zahlungstransaktionen mit dem von ihm selbst festgelegten Passwort (Mastercard Identity Check) und einer mobileTAN durch. Zum Zweck der Kontrolle durch den KI werden die Details über den zu autorisierenden Auftrag in der Nachricht, mit welcher dem KI die mobileTAN übermittelt wird, angezeigt.

3.2. Anweisungen des KI erfolgen auch im Rahmen des 3D Secure Verfahrens gemäß Punkt 7 der AGB. Im Rahmen des 3D Secure Verfahrens erteilt der KI seine unwiderrufliche Anweisung durch die Eingabe seines Passworts und einer mobileTAN.

4. Sorgfaltspflichten des Karteninhabers

4.1 Der KI hat seine persönlichen Identifikationsmerkmale (Passwort, mobileTAN, Einmalpasswort, persönlicher Zugangscode) geheim zu halten; er darf sie Dritten nicht mitteilen und auch nicht in einer sonstigen Form offenlegen.

4.2. Der KI ist verpflichtet, größte Sorgfalt bei Aufbewahrung und Verwendung seiner persönlichen Identifikationsmerkmale walten zu lassen, um eine missbräuchliche oder sonst nicht autorisierte Verwendung seiner Karte für Onlinezahlungen zu vermeiden. Der KI hat insbesondere darauf zu achten, dass bei Verwendung der persönlichen Identifikationsmerkmale diese nicht ausgespäht werden können. Er darf sie weder auf dem Gerät, von dem aus er eine Onlinezahlung mit seiner Karte beauftragt, noch in seinem mobilen Endgerät, in welches Identifikationsmerkmale zugestellt werden, notieren bzw. speichern (etwa in einer App für Notizen).

4.3. Bei Verlust oder Diebstahl von persönlichen Identifikationsmerkmalen sowie dann, wenn der KI von einer missbräuchlichen oder einer sonstigen nicht autorisierten Nutzung seiner Karte für Onlinezahlungen Kenntnis erlangt hat, hat der KI unverzüglich die Sperre des Zugangs zum 3D Secure Verfahren zu veranlassen.

4.4. Die mit der mobileTAN übermittelten Angaben sind vom KI vor Verwendung der mobileTAN auf ihre Richtigkeit zu überprüfen. Nur bei Übereinstimmung der per SMS übermittelten Daten mit dem gewünschten Auftrag, darf die mobileTAN zur Auftragsbestätigung verwendet werden.

5. Haftung des Karteninhabers

5.1. 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 Punkt 4 zugefügt hat. Hat der KI die Sorgfaltspflichten gemäß Punkt 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.

5.2. War für den KI vor der Zahlung der Verlust oder Diebstahl seiner persönlichen Identifikationsmerkmale oder die missbräuchliche Verwendung seiner Karte nicht bemerkbar, haftet er bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 4 nicht. Der KI haftet bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 4 auch dann nicht, wenn die Bank den Verlust der persönlichen Identifikationsmerkmale verursacht hat.

5.3. Abweichend von Punkt 5.1. 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.

5.4. Der KI haftet nicht, wenn der Schaden aus einer nicht autorisierten Nutzung der Karte bei einer Onlinezahlung nach Beauftragung der Sperre gemäß Punkt 6 entstanden ist, es sei denn, der KI hat in betrügerischer Absicht gehandelt.

6. Sperre des Zugangs

6.1. Aus Sicherheitsgründen wird nach sechsmaliger Falscheingabe des Passwortes der Zugang zum 3D Secure Verfahren von der Bank gesperrt.

6.2. Der KI kann die Sperre des Zugangs zum 3D Secure Verfahren jederzeit telefonisch unter +43 (0)5 99 06-6220 veranlassen.

6.3. Die Bank ist berechtigt, den Zugang zum 3D Secure Verfahren zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit dies rechtfertigten, oder der Verdacht einer nicht autorisierten oder betrügerischen Verwendung besteht.

6.4. Die Bank informiert den KI möglichst vor, spätestens jedoch unverzüglich nach der Sperre des Zugangs zum 3D Secure Verfahren über die Sperre und deren Gründe. Dies gilt nicht, wenn dem gesetzliche Regelungen oder gerichtliche bzw. behördliche Anordnungen entgegenstehen oder die Information über die Sperre das Sicherheitsrisiko erhöhen könnte oder wenn die Sperre auf Wunsch des KI erfolgte.

6.5. Solange die Sperre aufrecht ist, kann der KI keine Zahlungstransaktionen mit dem 3D Secure Verfahren durchführen.

6.6. Der KI kann die Aufhebung einer Sperre schriftlich (per E-Mail) oder telefonisch bei der Bank beauftragen. Die Bank stellt dafür folgende Kontaktadressen zur Verfügung: E-Mail paylife24@paylife.at; Telefon +43 (0)5 99 06-6220.

6.7. Die Bank wird eine Sperre aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen oder der KI die Aufhebung der Sperre beauftragt.

7. Änderungen der BGB

7.1. Änderungen der BGB 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 Bedingungen 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) 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, die Vereinbarung über die Teilnahme am 3D Secure Verfahren als auch den Kartenvertrag vor Inkrafttreten der Änderungen kostenlos fristlos zu kündigen. Außerdem wird die Bank die Gegenüberstellung sowie die vollständige Fassung der neuen Bedingungen auf ihrer Internetseite veröffentlichen und dem KI über sein Ersuchen die vollständige Fassung der neuen Bedingungen 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.

7.3. Die Änderung dieser Bedingungen 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 das 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 über das 3D Secure Verfahren erforderlich ist. Die Einführung von Entgelten oder die Änderung vereinbarter Entgelte durch eine Änderung dieser BGB ist ausgeschlossen.

8. Änderung der Adresse, der E-Mail Adresse und der Mobiltelefonnummer des Karteninhabers

Der KI verpflichtet sich, jede Änderung seiner Adresse, E-Mail-Adresse und Mobiltelefonnummer der Bank schriftlich oder per E-Mail bekannt zu geben. Die Bestimmung des Punktes 16. der AGB bleibt hiervon unberührt.

9. Sicherheitshinweise

9.1. Solange der Zugang zum 3D Secure Verfahren gesperrt ist, kann die Karte im Internet bei Händlern nicht zur Zahlung verwendet werden, wenn diese das 3D Secure Verfahren anbieten.

9.2. Zur Vermeidung von Risiken, die mit der Kenntnis des Passwortes 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 seinen Identifikationsmerkmalen (insbesondere dem Passwort) erlangt haben, so empfiehlt die Bank die Identifikationsmerkmale zu ändern.

9.4. 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.

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. 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.

9.7. Die Bank stellt auf der Website www.paylife.at unter dem Menüpunkt „Service“ weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.

10. Vertragsdauer und Beendigung

10.1. Die Vereinbarung über die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten wird auf unbestimmte Zeit geschlossen.

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

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

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

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

10.6. Die Vereinbarung endet automatisch mit dem Ende des Kartenvertrages.

Fassung September 2019