Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren

PayLife

Präambel

Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren (in der Folge kurz: BGB) ergänzen die Allgemeinen Geschäftsbedingungen (AGB) für wiederaufladbare PayLife Wertkarten (kurz: Karte), die dem zwischen easybank AG (kurz: Bank) und dem Karteninhaber (kurz: KI) geschlossenen Kartenvertrag zugrunde liegen. Auf die Informationen gemäß Zahlungsdienstegesetz (ZaDiG) sowie gemäß Fern-Finanzdienstleistungs-Gesetz (FernFinG), die der KI vor Abschluss des Kartenvertrages erhalten hat, wird verwiesen.

Die vorvertraglichen Informationen sind auf der Website www.paylife.at/agb zu finden. Darüber hinaus ergänzen sie die „Besonderen Geschäftsbedingungen, für den von der Bank angebotenen Dienst Info SMS“ in der jeweils geltenden Fassung.

Die BGB regeln die Anmeldung und die Abwicklung des Zahlungsverkehrs in sicheren Systemen. Die Registrierung zu den sicheren Systemen wird entweder vorab online auf der Website www.paylife.at/3dsecure gestartet oder erfolgt während des Bezahlvorganges im Internet.

1. Definitionen

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

1.2. Mobile Transaktionsnummer (kurz: mobileTAN)
Die mobileTAN ist eine auf ein mobiles Datenendgerät (z. B. Mobiltelefon, Tablet) übermittelte einmalig gültige Transaktionsnummer und dient als zusätzliches Kennwort bei Kartenzahlungen mit dem Mastercard SecureCode. 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 stellt auf der Website www.paylife.at unter dem Menüpunkt „Service“ weitere Informationen zu den Online Services 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) 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.

2. Registrierung zum 3D Secure Verfahren

2.1. Registrierung
Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KIs für 3D Secure voraus. Diese kann entweder auf der Website www.paylife.at/3dsecure 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.paylife.at/3dsecure wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KIs im Zuge der Registrierung zum 3D Secure Verfahren ist ein gültiges Einmalpasswort sowie eine mobileTAN erforderlich.

Die mobileTAN wird dem KI per SMS an die von ihm zuletzt bekannt gegebene Mobiltelefonnummer zur Kenntnis gebracht. Die Bank behält sich vor, zusätzliche Übermittlungswege für die mobileTAN anzubieten, welche auf der Website www.paylife.at/3dsecure bekannt gegeben werden.

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

- Benutzername
- Passwort (Mastercard SecureCode)
- 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.

3. Zahlen mit sicheren Systemen

3.1. Der KI sollte bei der Verwendung der Karte im Internet (E-Commerce), Zahlungsanweisungen in sicheren Systemen durchzuführen. Es handelt sich dabei um das 3D Secure Verfahren (Mastercard SecureCode) und das Verbindungsprotokoll „https“ (Hypertext Transfer Protocol Secure). Voraussetzung ist, dass der Händler (Vertragsunternehmen) diese (technisch) ermöglicht.

3.2. Mit dem vom KI selbst festgelegten Passwort und einer mobileTAN kann der KI Zahlungstransaktionen in sicheren Systemen durchführen. Die per SMS übermittelten Daten sind vom KI vor Verwendung der mobileTAN auf ihre Richtigkeit zu prüfen. Nur bei Übereinstimmung der per SMS übermittelten Daten mit dem gewünschten Auftrag, darf die mobileTAN 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 (0)5 99 06-6220 bekannt zu geben und den Zahlungsvorgang abzubrechen. Beendet der KI dennoch den Zahlungsvorgang, kann dies ein Mitverschulden für allfällige Schäden begründen.

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

3.4. Die Zahlungstransaktion, insbesondere die Anweisung, erfolgt auch bei Verwendung des sicheren Systems gemäß § 7 der dem Kartenantrag zugrundeliegenden Allgemeinen Geschäftsbedingungen. Wird jedoch das 3D Secure Verfahren verwendet, hat der KI sein von ihm selbst gewähltes Passwort und eine mobileTAN einzugeben. Mit der Eingabe der Bestätigung des Passwortes und der für diesen Zahlungsvorgang generierten mobileTAN wird die Zahlungsanweisung unwiderruflich erteilt.

4. Geheimhaltung

Der KI ist verpflichtet, die unter Punkt 2.3. angeführten persönlichen Identifikationsmerkmale und die mobileTAN 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

5.1. 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 beantragen. Die Bank stellt dafür folgende Kontaktadressen zur Verfügung: E-Mail paylife24@paylife.at; Telefon +43 (0)5 99 06-6220.

5.2. 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.

6. Allgemeine Bestimmungen und Sicherheitshinweise

6.1. Änderungen der BGB

6.1.1. Änderungen der BGB werden dem KI an die von ihm selbst der Bank zuletzt bekannt gegebene E-Mail-Adresse bzw. postalische Adresse zur Kenntnis gebracht. Diese Verständigung hat in Papierform oder, sofern dies vorher mit dem KI vereinbart wurde, auf einem anderen dauerhaften Datenträger (z. B. E-Mail) zu erfolgen. Im Übrigen gelten die Bestimmungen des Punktes 15. der AGB sinngemäß.

6.2. Änderung der Adresse, der E-Mail-Adresse und der Mobiltelefonnummer des KIs
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.

6.3. Sicherheitshinweise

6.3.1. Solange der Zugang zu den sicheren Systemen gesperrt ist, kann die Karte im Internet bei Händlern nicht zur Zahlung verwendet werden, wenn diese nur das 3D Secure Verfahren als sicheres System anbieten.

6.3.2. Zur Vermeidung von Risiken, die mit der Kenntnis des Mastercard SecureCode verbunden sind, empfiehlt die Bank, diesen regelmäßig (z. B. jeden Monat) zu ändern.

6.3.3. 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.

6.3.4. 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.

6.3.5. 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.

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

7. Vertragsdauer und Beendigung

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.

Fassung Juli 2016, Stand Mai 2018