Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren und Online Services

PayLife

1. Präambel

Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren und Online Services (in der Folge kurz: BGB) ergänzen die Allgemeinen Geschäftsbedingungen (AGB) für von PayLife Kreditkarten (kurz: Karte), die dem zwischen easybank AG (kurz: Bank) und dem Karteninhaber (kurz: KI) 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 Kreditkartenvertrages erhalten hat, wird verwiesen.

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

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 www.paylife.at/3dsecure gestartet oder erfolgt während des Bezahlvorganges im Internet.

2. Online Services und Abrechnung:

2.1. Die Bank bietet die Online Services („myPayLife“) an. Diese ermöglichen dem Karteninhaber (kurz: KI) auf eigenen Wunsch, verschiedene Dienstleistungen von der Bank im Zusammenhang mit seiner Kreditkarte (kurz: Karte) in Anspruch zu nehmen und Informationen zu seiner Karte einzusehen. Um an den Online Services teilnehmen zu können, sind der vorherige Abschluss eines Kreditkartenvertrages zwischen dem KI und der Bank, die Legitimation durch persönliche Identifikationsmerkmale und die Registrierung für das 3D Secure Verfahren erforderlich. In den Online Services kann der KI verschiedene Abfragen vornehmen, Aufträge an die Bank erteilen und Änderungen der Stammdaten vornehmen. Die Leistungen im Rahmen der Online Services können via Internet Browser auf my.paylife.at oder über die myPayLife App (nur für Smartphones) genutzt werden. Aus Sicherheitsgründen behält sich die Bank das Recht vor, in regelmäßigen Abständen Updates der Online Services vorzunehmen.

2.2. Die derzeit verfügbaren Funktionen der Online Services sind auf der Website www.paylife.at einsehbar. Nimmt der KI an den Online Services teil, erhält er von der Bank automatisch ein virtuelles Postfach. Die Bank hat die Möglichkeit, in diesem Postfach Nachrichten für den KI zu hinterlegen. Wird eine solche Nachricht von der Bank hinterlegt, erhält der KI eine Verständigung per E-Mail oder Push-Nachricht (nur myPayLife App). Die Registrierung startet der KI auf der Website www.paylife.at/3dsecure oder während des Bezahlvorganges im Internet.

2.3. Sollte zwischen der Bank und dem KI nicht bereits bei Abschluss des Kreditkartenvertrages die Zurverfügungstellung einer OnlineAbrechnung vereinbart worden sein, kann der KI mit der Registrierung zu den Online Services auf der Website www.paylife.at/3dsecure, nach erfolgtem Login in myPayLife erklären, anstelle einer postalisch zugestellten Abrechnung in Papierform, eine Abrechnung in elektronischer Form erhalten zu wollen. Die Abrechnung wird dem KI in den Online Services mindestens einmal monatlich zur Verfügung gestellt. Darüber wird der KI verständigt. Diese Verständigung erfolgt per E-Mail an die vom KI selbst bekanntgegebene E-Mail-Adresse und kann vom Kunden geändert (z. B. SMS und Push-Nachricht) oder deaktiviert werden.

3. Definitionen:

3.1. Mastercard SecureCode bzw. Verified by Visa Passwort – „Passwort“
Das im Zuge des 3D Secure Registrierungsverfahrens vom KI selbst gewählte Passwort. Dieses wird bei Mastercard als „Mastercard Secure Code“ und bei Visa als „Verified by Visa Passwort“ bezeichnet. Dieses Passwort dient gleichzeitig für die Nutzung der von der Bank zur Verfügung gestellten Online Services, insbesondere für den Aufruf der Kreditkartenabrechnung, wenn der KI die Zugänglichmachung als Download auf der Website my.paylife.at samt entsprechender Benachrichtigung (per E-Mail an die zuletzt vom KI bekanntgegebene E-Mail-Adresse) gewählt hat.

3.2. 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 bzw. Verified by Visa Passwort. Auch bei der Registrierung zum 3D Secure Verfahren und bei bestimmten Datenänderungen in myPayLife, 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.

3.3. 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.

3.4. myPayLife App
Die myPayLife App vereinfacht den Zugang zu den Online Services am mobilen Datenendgerät (z. B. Mobiltelefon, Tablet). Für die Nutzung der App ist ein Download und Installierung aus dem entsprechenden App Store notwendig. Für die Authentifizierung ist die Registrierung für 3D Secure erforderlich und für den Login ein selbstgewählter 5-stelliger Zugangscode.

3.5. Sichere Systeme

3.5.1 3D Secure
Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das den KI zweifelsfrei als rechtmäßigen KI identifiziert.

3.5.2 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.

4. Registrierung zum 3D Secure Verfahren:

4.1. 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 sind alternativ entweder ein gültiges Einmalpasswort oder die Daten einer Kreditkartenabrechnung aus den letzten 6 Monaten 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.

4.2. 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 und den Online Services (kurz: Vereinbarung) zustande kommt.

4.3. Folgende persönliche Identifikationsmerkmale sind vom KI im Zuge der Registrierung selbst festzulegen:

- Benutzername
- 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.

4.4. Registrierung myPayLife App
Beim erstmaligen Aufrufen der Applikation gibt der KI seinen bei der 3D Secure Registrierung gewählten Benutzernamen oder seine Kartennummer ein. Nach der Anzeige der persönlichen Begrüßung (und Kontrolle des KI auf Korrektheit) gibt der KI das 3D Secure Passwort ein. Nach positiver Prüfung legt der KI seinen persönlichen Zugangscode für den Login auf diesem Endgerät fest.

4.5. Login Online Services (via Webbroser bzw. App)
Der KI gibt den bei der 3D Secure Registrierung gewählten Benutzernahmen oder seine Kartennummer ein. Nach der Anzeige der persönlichen Begrüßung (und Kontrolle des KI auf Korrektheit) gibt der KI das 3D Secure Passwort ein.

Wenn der KI myPayLife über die mobile App verwendet, so gibt er seinen Zugangscode in das dafür vorgesehene Login Feld ein.

5. Zahlen mit sicheren Systemen:

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

5.2. 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.

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

5.4. Die Zahlungstransaktion, insbesondere die Anweisung, erfolgt auch bei Verwendung des sicheren Systems gemäß Punkt 6. der dem Kartenauftrag 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.

6. 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.

7. Sperre des Zugangs:

7.1. 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. Da das Passwort auch den Zugang zu den Online Services ermöglicht, hat der KI im Fall einer Sperre auch keinen Zugang zu den Online Services. 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: E-Mail paylife24@paylife.at; Telefon +43 (0)5 99 06-6220.

7.2. 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.

8. Änderungen der BGB und der Adresse:

8.1. Änderungen der BGB werden dem KI an die von ihm selbst der Bank zuletzt bekannt gegebene E-Mail-Adresse. 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.

8.2. 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.

9. Sicherheitshinweise:

9.1. Solange der Zugang zu den sicheren Systemen gesperrt ist, kann die Karte weder für die Online Services noch im Internet bei Händlern zur Zahlung verwendet werden, wenn diese nur das 3D Secure Verfahren als sicheres System anbieten. Wird aus welchem Grund auch immer der Zugang zu den Online Services gesperrt, hat der KI keine Möglichkeit mehr, für den Zeitraum der Sperre in die OnlineAbrechnungen Einsicht zu nehmen. Die Bank empfiehlt daher, die jeweils zur Verfügung gestellte OnlineAbrechnung auf einem dauerhaften Datenträger zu speichern und die Sperre vom Contact Center unter der Telefonnummer +43 (0)5 99 06-6220 aufheben zu lassen.

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

9.4. 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.

9.5. 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. Die Online Services sollen jedes Mal mit der Logout-Funktion beendet werden.

9.6. 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:

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