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

Gegenüberstellung Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren in der zuletzt mit Ihnen vereinbarten Fassung mit der Fassung September 2019. Die folgenden Klauseln sind geändert; alle übrigen Klauseln sind in beiden Fassungen gleich.

Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren	**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 (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.	**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 ~~(AGB)~~ für wiederaufladbare PayLife Wertkarten (kurz: AGB ~~Karte~~), die zu dem zwischen easybank AG (kurz: Bank) und dem Karteninhaber (kurz: KI) geschlossenen Kartenvertrag über die Ausgabe einer wiederaufladbaren PayLife Wertkarte vereinbart sind. ~~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.~~
1.1. Mastercard SecureCode	**Mastercard ~~SecureCode~~ Identity Check**
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. […].Die Bank stellt auf der Website www.paylife.at unter dem Menüpunkt „Service“ weitere Informationen zu den Online Services zur Verfügung.	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~~ Identity Check Passwort. […] Die Bank sendet die mobileTAN an die vom KI für die Zwecke der Zustellung bekannt gegebene Mobiltelefonnummer per SMS.
1.3. […] Im Zuge des 3D Secure Registrierungsprozesses wird das Einmalpasswort durch die Eingabe eines selbst gewählten, ausschließlich dem KI bekannten Passwortes (Mastercard SecureCode) ersetzt.	1.3. […] Im Zuge des 3D Secure Registrierungsprozesses wird das Einmalpasswort durch die Eingabe eines selbst gewählten, ausschließlich dem KI bekannten Passwortes (Mastercard ~~SecureCode~~ 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.
1.4. Sichere Systeme	~~1.4. Sichere Systeme~~ 1.6. 3D Secure
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.	~~1.4.1. 3D Secure~~ Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das die Voraussetzungen der starken Kundenauthentifizierung erfüllt. ~~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.~~
2.1. 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.	2.1. Registrierung Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KIs für 3D Secure voraus. ~~Diese~~ Die Registrierung kann auf der Website www.paylife.at/3dsecure gestartet werden. ~~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~~ 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. ~~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.	~~2.2. 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.	~~2.3. Folgende persönliche Identifikationsmerkmale sind vom KI im Zuge der Registrierung selbst festzulegen:~~ 2.2. Der KI hat im Zuge der Registrierung folgendes selbst festzulegen: • Benutzername • Passwort (Mastercard ~~SecureCode~~) • persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt). Der KI kann ~~seine persönlichen Identifikationsmerkmale~~ 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. ~~SMS-Empfang entstehende Kosten hat der KI selbst zu tragen.~~
3. Zahlen mit sicheren Systemen	**3. Zahlen mit ~~sicheren Systemen~~ 3D Secure**
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.	~~3.1. 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.~~ 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. 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.	3.2. ~~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.~~ 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.
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.	~~3.3. 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.	~~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	**4. ~~Geheimhaltung~~ Sorgfaltspflichten des Karteninhabers**
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.	~~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.~~ 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.
5. Sperre des Zugangs	~~5.~~ **6. 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.	~~5.1.~~ 6.1. 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.	~~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.~~ 6.2. 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.
6. Allgemeine Bestimmungen und Sicherheitshinweise	~~**6. Allgemeine Bestimmungen und Sicherheitshinweise**~~ **7. Änderungen der BGB**
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.	~~6.1. 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.~~ 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.
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	~~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.	~~Mobiltelefonnummer der Bank schriftlich oder per E-Mail bekannt zu geben. Die Bestimmung des Punktes 16. der AGB bleibt hiervon unberührt.~~ 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.
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.	~~6.3.~~ **9. Sicherheitshinweise** ~~6.3.1.~~ 9.1. Solange der Zugang ~~zu den sicheren Systemen~~ zum 3D Secure Verfahren 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.~~ 9.2. Zur Vermeidung von Risiken, die mit der Kenntnis des ~~Mastercard SecureCode~~ Passwortes verbunden sind, empfiehlt die Bank, ~~diesen~~ dieses regelmäßig (z. B. jeden Monat) zu ändern. ~~6.3.3.~~ 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. ~~6.3.3.~~ 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. ~~6.3.4.~~ 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. ~~6.3.5.~~ 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. ~~6.3.6.~~ 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.
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.	~~7.~~ **10. Vertragsdauer und Beendigung** 10.1. Die Vereinbarung über die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten 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.~~
	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 Juli 2016, Stand Mai 2018	Fassung September 2019