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

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

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

Fassung Juli 2016, Stand Mai 2018	Fassung September 2019
1. Präambel Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren und Online Services (in der Folge kurz: BGB) ergänzen die Allgemeinen Geschäfts-bedingungen (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.	**1. Präambel** Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren und Online Services für PayLife Kreditkarten (in der Folge kurz: BGB) regeln die Nutzung der Online Services und die Abwicklung von Zahlungen mit PayLife Kreditkarten unter Verwendung des 3D Secure Verfahrens. Die BGB gelten, wenn ihre Geltung vereinbart ist. Sie ergänzen die Allgemeinen Geschäftsbedingungen ~~(AGB)~~ für ~~von~~ PayLife Kreditkarten (kurz: ~~Karte~~ AGB), die zu dem zwischen der 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.~~ über die Ausgabe seiner PayLife Kreditkarte (kurz: Karte) vereinbart sind. ~~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.~~ 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, die Registrierung für das 3D Secure Verfahren und der Abschluss einer Vereinbarung über die Teilnahme am 3D Secure Verfahren und den Online Services (kurz: Vereinbarung) erforderlich.
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.Online Services, Kommunikation und Abrechnung:** **2.1.** Die Bank bietet die ~~Online Services (~~„myPayLife“~~)~~ genannten Online Services 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 OnlineServices kann der KI ~~verschiedene Abfragen vornehmen, Aufträge an die Bank erteilen~~ bestimmte Dienstleistungen und Angebote der Bank im Zusammenhang mit seiner Karte in Anspruch nehmen, Informationen zu seiner Karte einsehen, Änderungen der Stammdaten vornehmen, Abfragen (insbesondere Umsatzabfragen) tätigen, Aufträge erteilen, rechtsverbindliche Erklärungen sowie sonstige Erklärungen gegenüber der Bank abgeben. Im Rahmen der Online Services können keine Zahlungsaufträge erteilt werden. ~~Die Leistungen im Rahmen der~~ Online Services können via Internet Browser über die Website 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.	**2.2.** ~~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.~~ In den Online Services ist ein virtuelles Postfach eingerichtet, über welches die Bank mit dem KI kommuniziert, ihn informiert und ihm gegenüber Erklärungen abgibt; dieses virtuelle Postfach ist jenes, welches für die Kommunikation gemäß Punkt 17.1. AGB vereinbart ist.
2.3. Sollte zwischen der Bank und dem KI nicht bereits bei Abschluss des Kreditkartenvertrages die Zurverfügungstellung einer Online Abrechnung 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.	**2.3**. ~~Sollte zwischen der Bank und dem KI nicht bereits bei Abschluss des Kreditkartenvertrages die Zurverfügungstellung einer Online Abrechnung 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.~~ Ist zwischen der Bank und dem KI vereinbart, dass die Bank die Abrechnungen zu seiner Karte dem KI online zum Download zur Verfügung stellt, erfolgt dies im Rahmen der Online Services; eine solche Vereinbarung beinhaltet Punkt 11.1 AGB. Die Bank wird den KI über die Verfügbarkeit der Abrechnung per E-Mail an die von ihm bekanntgegebene E-Mail-Adresse informieren. Der KI und die Bank können in den Online Services eine andere Art der Verständigung (z.B. per SMS oder Push-Nachricht) vereinbaren. Der KI kann die Verständigung auch deaktivieren, wobei die Bank in diesem Fall nicht mehr verpflichtet ist, den KI über die

	Verfügbarkeit der Abrechnung zu verständigen. Haben die Bank und der KI nicht bereits bei Abschluss des Kreditkartenvertrages die Zurverfügungstellung einer Online Abrechnung vereinbart, kann der KI im Rahmen der Online Services dies jederzeit beauftragen.
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. Definitionen:** **3.1.** Mastercard ~~SecureCode~~ Identity Check bzw. ~~Verified by~~ Visa Secure Passwort Das im Zuge des 3D Secure Registrierungsverfahrens vom KI selbst gewählte Passwort. Dieses wird bei Mastercard als „Mastercard ~~SecureCode~~ Identity Check" und bei Visa als „~~Verified by~~ Visa Secure 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.	**3.2.** 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 bzw. ~~Verified by~~ Visa Secure Passwort sowie bei der Abgabe von Willenserklärungen und der Erteilung von Aufträgen im Rahmen der Online Services. Auch bei der Registrierung zum 3D Secure Verfahren und bei bestimmten Datenänderungen in myPayLife, ist die Eingabe einer mobileTAN erforderlich. Die Bank ~~stellt~~ sendet die mobileTAN an die vom KI für die Zwecke der Zustellung bekannt gegebene Mobiltelefonnummer per SMS oder per Push-Nachricht über die myPayLife App.
3.3. [...] 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.	**3.3.** [...] Im Zuge des 3D Secure Registrierungsprozesses wird das Einmalpasswort durch die Eingabe eines selbst gewählten, ausschließlich dem KI bekannten Passwortes (Mastercard ~~SecureCode~~ Identity Check bzw. ~~Verified by~~ Visa Secure Passwort), ersetzt.
	3.4. 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.
	3.5. Starke Kunden- authentifizierung 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.
3.4. myPayLife App [...] Für die Authentifizierung ist die Registrierung für 3D Secure erforderlich und für den Login ein selbstgewählter 5-stelliger Zugangscode.	~~**3.4.**~~ **3.6.** myPayLife App [...] Für die Authentifizierung ist die Registrierung für 3D Secure erforderlich und für den Login ein selbstgewählter 5-stelliger Zugangscode (kurz: persönlicher Zugangscode). Der KI kann in der myPayLife App ein biometrisches Merkmal (z.B. Fingerabdruck) hinterlegen und bei der Anmeldung als Alternative zum persönlichen Zugangscode verwenden.
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.** Sichere Systeme~~ ~~**3.5.1**~~ **3.7.** 3D Secure Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das ~~den KI zweifelsfrei als rechtmäßigen KI identifiziert.~~ die Voraussetzungen der starken Kundenauthentifizierung erfüllt.
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.	~~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. [...]	**4. Registrierung zum 3D Secure Verfahren:** **4.1.** Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KIs für 3D Secure voraus. ~~Diese~~ Die Registrierung kann ~~entweder~~ online im Serviceportal myPayLife ~~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~~ erfolgen. 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 für die Registrierung wird dem KI per SMS an die von ihm zuletzt bekannt gegebene Mobiltelefon-nummer 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.~~ [...]
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.	~~**4.2.** 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	~~**4.3.**~~ **4.2.** ~~Folgende persönliche Identifikationsmerkmale sind vom KI~~ Der KI hat im Zuge der Registrierung Folgendes selbst festzulegen: • Benutzername • Passwort (Mastercard ~~SecureCode~~ Identity Check bzw. ~~Verified by~~ Visa Secure Passwort) • Persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt). Der KI kann ~~seine persönlichen Identifikationsmerkmale~~ seinen Benutzernamen, sein Passwort und seine

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.	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.~~ 4.1. 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~~ Empfang von SMS bzw. Push-Nachrichten oder aus dem Internetzugang entstehende Kosten hat der KI selbst zu tragen.
4.4. Registrierung myPayLife App [...]	~~**4.4.**~~ **4.3.** Registrierung myPayLife App [...] Bei der Registrierung in der myPayLife App kann der KI ein biometrisches Sicherheitsmerkmal (z.B. Fingerabdruck) hinterlegen, welches er danach beim Login als Alternative zum persönlichen Zugangscode nutzen kann.
4.5. Login Online Services (via Webbroser bzw. App) [...] Wenn der KI myPayLife über die mobile App verwendet, so gibt er seinen Zugangscode in das dafür vorgesehene Login Feld ein.	~~**4.5.**~~ **4.4.** Login Online Services (via Webbroser bzw.App) [...] Wenn der KI myPayLife über die mobile App verwendet, so gibt er seinen persönlichen Zugangscode in das dafür vorgesehene Login Feld ein. Alternativ kann er sein in der App hinterlegtes biometrisches Sicherheitsmerkmal (z.B. Fingerabdruck) verwenden.Wechselt der KI das mobile Endgerät, ist für die Nutzung der myPayLife App auf diesem neuen Gerät eine neuerliche Registrierung erforderlich.
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 (Mastecard SecureCode oder Verified by Visa) und das Verbindungsprotokoll „https“ (Hypertext Transfer Protocol Secure). Voraussetzung ist, dass der Händler (Vertragsunternehmen) diese (technisch) ermöglicht.	**5. Zahlen mit ~~sicheren Systemen:~~3D Secure:** ~~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 (Mastecard SecureCode oder Verified by Visa) und das Verbindungsprotokoll „https“ (Hypertext Transfer Protocol Secure). Voraussetzung ist, dass der Händler (Vertragsunternehmen) diese (technisch) ermöglicht.~~ **5.1.** Im Rahmen des 3D Secure Verfahrens führt der KI Zahlungstransaktionen mit dem von ihm selbst festgelegten Passwort (Mastercard Identity Check bzw. Visa Secure Passwort) 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.
	5.2. Anweisungen des KI erfolgen auch im Rahmen des 3D Secure Verfahrens gemäß Punkt 6 der AGB. Im Rahmen des 3D Secure Verfahrens erteilt der KI seine unwiderrufliche Anweisung durch die Eingabe seines Passworts und einer mobileTAN.
	6. Sorgfaltspflichten des KI: **6.1.** 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.
	6.2. 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 bzw. missbräuchliche oder sonst nicht autorisierte Nutzung der Online Services 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 bzw. von dem aus er in die Online Services einsteigt, noch in seinem mobilen Endgerät, in welches Identifikationsmerkmale zugestellt werden, notieren bzw. speichern (etwa in einer App für Notizen).
	6.3. 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 bzw. von einer missbräuchlichen oder einer sonstigen nicht autorisierten Nutzung der Online Services Kenntnis erlangt hat, hat der KI unverzüglich die Sperre des Zugangs zum 3D Secure Verfahren zu veranlassen.
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.	~~**5.2.**~~ **6.4.** ~~Mit dem vom KI selbst festgelegten Passwort und einer mobileTAN kann der KI Zahlungstransaktionen in sicheren Systemen durchführen. Die per SMS übermittelten Daten~~ Die mit der mobileTAN übermittelten Angaben sind vom KI vor Verwendung der mobileTAN auf ihre Richtigkeit zu ~~prüfen~~ überprüfen. 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.	~~**5.4.**~~ **7. Haftung des KI** ~~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.~~ **7.1.** 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 6. zugefügt hat. ~~Ist die Verletzung der Sorgfaltspflichten gemäß Punkt 6. auf leichte Fahrlässigkeit des KIs zurückzuführen, ist seine Haftung auf höchstens EUR 50,-- beschränkt.~~ Hat der KI die Sorgfaltspflichten gemäß Punkt 6. 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.
	7.2. War für den KI vor der Zahlung der Verlust oder Diebstahl seiner persönlichen Identifikationsmerkmale oder die missbräuchliche Verwendung seiner Karte nicht bemerkbar, haftet er abweichend von Punkt 7.1. bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 6. nicht. Der KI haftet bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 6. auch dann nicht, wenn die Bank den Verlust der persönlichen Identifikationsmerkmale verursacht hat.
	7.3. Abweichend von Punkt 7.1. 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.
	7.4. Der KI haftet nicht, wenn der Schaden aus einer nicht autorisierten Nutzung der Karte bei einer Onlinezahlung nach Beauftragung der Sperre gemäß Punkt 8. entstanden ist, es sei denn, der KI hat in betrügerischer Absicht gehandelt.
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.~~ 8. Sperre des Zugangs:** **~~7.1.~~ 8.1.** 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 9906-6220.~~
	8.2. Der KI kann die Sperre des Zugangs zum 3D Secure Verfahren jederzeit telefonisch unter +43 (0)5 99 06-6220 veranlassen.
	8.3. 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.
	8.4. 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.
	8.5. 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.
	8.6. 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.
	8.7. Die Bank wird eine Sperre aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen oder der KI die Aufhebung der Sperre beauftragt.
	9. Aufträge und Erklärungen in den Online Services **9.1.** Aufträge und rechtsverbindliche Willenserklärungen sowie sonstige Erklärungen des KI in den Online Services gelten als vom KI erteilt bzw. abgegeben, wenn der KI diese mittels mobileTAN freigegeben hat. Zum Zweck der Kontrolle durch den KI werden die Details über den zu autorisierenden Auftrag oder über die rechtsverbindliche Willenserklärung bzw. sonstige Erklärung in der Nachricht (SMS oder Push-Nachricht) mit dem mobileTAN angezeigt. Die mit der mobileTAN übermittelten Angaben sind vom KI vor Verwendung der mobileTAN auf ihre Richtigkeit zu überprüfen. Nur bei Übereinstimmung der übermittelten Daten mit dem gewünschten Auftrag bzw. der gewünschten rechtsverbindlichen Willenserklärung darf die mobileTAN zur Auftragsbestätigung verwendet werden
	9.2. Die Abgabe rechtsverbindlicher Willenserklärungen durch den KI kann auch dadurch erfolgen, dass der KI in den Online Services ein ihm von der Bank ausdrücklich unterbreitetes Anbot dadurch annimmt, dass er die Annahme erklärt (etwa durch das Anklicken einer Box mit seiner Einverständniserklärung) und er seine Annahme danach bestätigt (etwa durch das Betätigen eines Buttons); auf diese Weise kann der KI auch sonstige Erklärungen abgeben.
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.~~ 10. 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.~~ **10.1.** 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 oder über das virtuelle Postfach in den Online Services) 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, sowohl die Vereinbarung über die Teilnahme am 3D Secure Verfahren und den Online Services als auch den Kreditkartenvertrag 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.
	10.2. 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 an das gemäß Punkt 2.2 für den KI eingerichtete virtuelle Postfach, wobei der KI über das Vorhandensein des Änderungsangebots in seinem virtuellen Postfach auf die mit ihm vereinbarte Weise (Push-Nachricht, E-Mail, SMS, Post oder sonst vereinbarte Form) informiert werden wird.
	10.3. 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 Bankenaufsichts-behörde, 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 Geschäfts-verbindung mit dem KI über das 3D Secure Verfahren oder die Online Services 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 das 3D Secure Verfahren oder die Online Services erforderlich ist, (vi) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für jene Bankgeschäfte, welche der KI über die Online Services abwickeln kann, erforderlich ist. Die Einführung von Entgelten oder die Änderung vereinbarter Entgelte durch eine Änderung dieser BGB ist ausgeschlossen.
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.	~~**8.2. Änderung der Adresse**~~ **11. Änderung der E-Mail-Adresse und der Mobiltelefonnummer des KIs** **11.1.** Der KI verpflichtet sich, jede Änderung seiner ~~Adresse,~~ E-Mail-Adresse und seiner 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. [...]	~~**9.**~~ **12. Sicherheitshinweise:** ~~**9.1.**~~ **12.1.** Solange der Zugang zu ~~den sicheren Systemen~~ 3D Secure Verfahren 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. [...]
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.	~~**9.2.**~~ **12.2.** Zur Vermeidung von Risiken, die mit der Kenntnis des Passwortes verbunden sind, empfiehlt die Bank, dieses regelmäßig (z. B. jeden Monat) zu ändern.
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.	~~**7.2.**~~ **12.3.** 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.~~
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.	~~**9.3.**~~ **12.4.** Es wird empfohlen, den Zugang zum Gebrauch der mobilen Datenendgeräte zu sichern. Bei Verlust oder Diebstahl des mobilen Datenendgerätes empfiehlt ~~easybank~~ die Bank die Kontaktaufnahme mit dem Mobilfunkanbieter zur Sperre der SIM Karte.
9.4. [...]	~~**9.4.**~~ **12.5** [...]
9.5. [...]	~~**9.5.**~~ **12.6.** [...]
9.6. [...]	~~**9.6.**~~ **12.7.** [...]
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.	~~**10.**~~ **13. Vertragsdauer, Kündigung und Beendigung:** 13.1. Die Vereinbarung über die Teilnahme am 3D Secure Verfahren und den Online Services 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.~~
	13.2. 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 und die Online Services sperren.
	13.3. Die Bank ist berechtigt, die Vereinbarung jederzeit unter Einhaltung einer Frist von zwei Monaten ohne Angabe von Gründen zu kündigen.
	13.4. Sowohl der KI als auch die Bank sind berechtigt, die Vereinbarung jederzeit bei Vorliegen eines wichtigen Grundes mit sofortiger Wirkung aufzulösen.
	13.5. Die Beendigung der Vereinbarung lässt den Kreditkartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.
	13.6. Die Vereinbarung endet automatisch mit dem Ende des Kreditkartenvertrages.