Gegenüberstellung der BGB für 3D Secure und Online Services mit BGB myPayLife

Gegenüberstellung der geänderten Bestimmungen der Besonderen Geschäftsbedingungen für das Serviceportal „myPayLife“ in der Fassung Juli 2019 mit jenen der derzeit mit Ihnen vereinbarten Fassung, den Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren und Online Services in der Fassung Juli 2016, Stand Mai 2018.

Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren und Online Services Fassung Juli 2016, Stand Mai 2018	**Besondere Geschäftsbedingungen für das Serviceportal „myPayLife“ Fassung Juli 2019**
Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren und Online Services	**Besondere Geschäftsbedingungen für das Serviceportal „myPayLife“ ~~die Teilnahme am 3D Secure Verfahren und Online Services~~** Fassung Juli 2019 Diese Besonderen Geschäftsbedingungen 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 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.	~~**Präambel**~~ **Allgemeines** 1.1. Diese Besonderen Geschäftsbedingungen für das Serviceportal myPayLife ~~die Teilnahme am 3D Secure Verfahren und Online Services~~ (~~in der Folge~~ kurz: BGB myPayLife) regeln das Online Service der ~~ergänzen die Allgemeinen Geschäftsbedingungen (AGB) für von PayLife Kreditkarten (kurz: Karte), die dem zwischen~~ easybank AG (kurz: Bank) zu den von ihr ausgegebenen PayLife Kreditkarten und die Nutzung dieses Services durch den ~~und dem~~ Karteninhaber (kurz: KI); sie gelten, wenn sie mit dem KI vereinbart sind. Die BGB gelten ergänzend zu den zwischen der Bank und dem KI vereinbarten Allgemeinen Geschäftsbedingungen für PayLife Kreditkarten (kurz: AGB). ~~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.~~ 1.2. Die Möglichkeit zur Nutzung des Serviceportals myPayLife setzt das Bestehen eines Kreditkartenvertrages über eine PayLife Kreditkarte (kurz: Kreditkartenvertrag) zwischen der Bank und dem KI und den Abschluss einer Vereinbarung über die Nutzung des Serviceportals durch den KI voraus. 1.3 Um das Serviceportal nutzen zu können, muss sich der KI auf der Website my.paylife.at oder in der myPayLife App registrieren (siehe Punkt 4).
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	2. ~~Online Services und Abrechnung:~~ Serviceportal myPayLife - Kommunikation 2.1. Das „myPayLife“ genannte Serviceportal der Bank ermöglicht ~~Die Bank bietet die Online Services („myPayLife“) an. Diese ermöglichen~~ dem ~~Karteninhaber (kurz:~~ KI~~)~~ ~~auf eigenen Wunsch, verschiedene~~ bestimmte Dienstleistungen ~~von~~ und Angebote der Bank im Zusammenhang mit seiner PayLife Kreditkarte (kurz: Karte) in Anspruch zu nehmen, ~~und~~ Informationen zu seiner Karte einzusehen, Änderungen seiner Stammdaten vorzunehmen, Abfragen (insbesondere Umsatzabfragen) zu tätigen, Aufträge zu erteilen und rechtsverbindliche Willenserklärungen sowie sonstige Erklärungen gegenüber der Bank abzugeben. Im Rahmen des Serviceportals können keine Zahlungsaufträge erteilt werden; auch eine Verwendung der Karte ist nicht möglich. ~~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,~~

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.	~~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. Im Serviceportal 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 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 PushNachricht) oder deaktiviert werden.	~~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 PushNachricht) oder deaktiviert werden.~~ 2.3. 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 des Serviceportals; 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 bekannt gegebene E-Mail-Adresse informieren. Der KI und die Bank können im Serviceportal 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 Serviceportal dies jederzeit beauftragen. 2.4 Das Serviceportal steht via Internet Browser auf der Website my.paylife.at oder über die myPayLife App (nur für Smartphones) zur Verfügung.
3. Definitionen: 3.1. Mastercard SecureCode bzw. Verified by Visa Passwort – „Passwort“ Das im Zuge des 3D Secure Registrierungs-verfahrens 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~~:~~ und Begriffsbestimmungen 3.1. ~~Mastercard SecureCode bzw. Verified by Visa Passwort – „Passwort“~~ ~~Das im Zuge des 3D Secure Registrierungs-verfahrens 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.~~ PayLife Kundennummer (kurz: Kundennummer) Der KI erhält als Identifikationsmerkmal eine mehrstellige Kundennummer, welche von ihm nicht geändert werden kann. Die Kundennummer dient sowohl bei der Registrierung als auch bei der Anmeldung des KI zum Serviceportal als Identifikationsmerkmal.
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 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.~~ Einmalpasswort Das Einmalpasswort ist ein von der Bank vorgegebenes Identifikationsmerkmal, das vom KI nicht geändert werden kann; es dient der Legitimierung des KI bei der Registrierung im Serviceportal.

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.	3.3. ~~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.~~ Passwort Das Passwort ist das vom KI bei der Registrierung zum Serviceportal festgelegte Geheimwort (Kombination aus Zeichen). Das Passwort ist ein persönliches Identifikationsmerkmal des KI, welches bei zusätzlicher Angabe der Kundennummer der Identifizierung des KI für den Zugang zum Serviceportal dient. Das Passwort kann vom KI im Serviceportal geändert werden.
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.	3.4. ~~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.~~ Mobile Transaktionsnummer (kurz: mobileTAN) Die mobileTAN dient der Registrierung für das Serviceportal, der Erteilung von Aufträgen und der Abgabe von rechtsverbindlichen Willenserklärungen sowie von sonstigen Erklärungen durch den KI. Die Bank sendet die nur einmalig verwendbare mobileTAN an die vom KI für die Zwecke der Zustellung bekannt gegebene Mobiltelefonnummer per SMS.
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.	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.~~ 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. Die Zustellung des Authentifizierungscodes erfolgt an die vom KI bekannt gegebene Mobiltelefonnummer per SMS. Bei der mobileTAN handelt es sich um einen solchen Authentifizierungscode. 3.6 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. 3.7. myPayLife App Die myPayLife App ist eine von der Bank zur Verfügung gestellte App; sie ermöglicht den Zugang zum Serviceportal am mobilen Datenendgerät des KI (z.B. Mobiltelefon, Tablet). Um die App nutzen zu können, muss sie der KI auf seinem Datenendgerät installieren. Der KI kann in der myPayLife App ein biometrisches Merkmal (z.B. Fingerabdruck) hinterlegen und bei der Anmeldung als Alternative zum Passwort verwenden.
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	4. Registrierung ~~zum 3D Secure Verfahren:~~ und Login 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.	~~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.~~ Registrierung via Webbrowser bzw. App (1) Die Registrierung des KI für das Serviceportal erfolgt durch die vorgegebenen Schritte. Beim erstmaligen Einstieg in das Serviceportal muss der KI seine Kundennummer und das Einmalpasswort eingeben. Im Anschluss wird eine mobileTAN an die vom KI bekannt gegebene Mobiltelefonnummer gesandt, welche der KI während der Registrierung eingeben muss. Nach positiver Prüfung durch die Bank ist durch den KI ein selbstgewähltes Passwort zu definieren. (2) Bei der Registrierung in der myPayLife App kann der KI ein biometrisches Sicherheitsmerkmal (z.B. Fingerprint) hinterlegen, welches er danach beim Login als Alternative zum Passwort nutzen kann.
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.~~ Login via Webbrowser bzw. App (1) Beim Login in das Serviceportal via Webbrowser gibt der KI die Kundennummer und sein selbst gewähltes Passwort ein. Nach positiver Prüfung kann der KI das Serviceportal nutzen. (2) Beim Login über die myPayLife App kann der KI als Alternative zum Passwort sein in der App hinterlegtes biometrisches Sicherheitsmerkmal (z.B. Fingerprint) verwenden.
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.	4.3. ~~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.~~ Wechsel des Endgeräts Wechselt der KI das mobile Endgerät, ist für die Nutzung der myPayLife App auf diesem neuen Endgerät eine neuerliche Registrierung erforderlich.
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.	~~4.4. 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.	~~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. ~~Zahlen mit sicheren Systemen:~~ Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen
	Der KI ist zur Einhaltung der in Punkt 5.1. und in Punkt 5.2. vereinbarten Sorgfaltspflichten verpflichtet. Ist der KI Unternehmer, ist er zusätzlich zur Einhaltung der empfohlenen Sicherheitsmaßnahmen gemäß Punkt 5.3. verpflichtet. Ist der KI Verbraucher, so empfiehlt die Bank die Einhaltung der empfohlenen Sicherheitsmaßnahmen gemäß Punkt 5.3., ohne dass Verbraucher zur Einhaltung verpflichtet sind.
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.	5.1. ~~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.~~
	Geheimhaltungs- und Sperrverpflichtung
	(1) Der KI hat seine persönlichen Identifikationsmerkmale (Passwort, mobileTAN, Kundennummer und Einmalpasswort) geheim zu halten; er darf sie Dritten nicht mitteilen oder in einer sonstigen Form offenlegen.
	(2) Der KI ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung seiner persönlichen Identifikationsmerkmale walten zu lassen, um einen missbräuchlichen Zugriff auf das Serviceportal zu vermeiden. Der KI hat insbesondere darauf zu achten, dass bei Verwendung seiner persönlichen Identifikationsmerkmale diese nicht ausgespäht werden können. Er darf sie weder auf dem Gerät, von dem aus er in das Serviceportal einsteigt, noch in seinem mobilen Endgerät, in welches Identifikationsmerkmale zugestellt werden, notieren bzw. speichern (etwa in einer App für Notizen).
	(3) Bei Verlust oder Diebstahl von persönlichen Identifikationsmerkmalen sowie dann, wenn der KI von einer missbräuchlichen oder einer sonstigen nicht autorisierten Nutzung des Serviceportals Kenntnis erlangt hat, hat der KI unverzüglich die Sperre des Zugangs zum Serviceportal 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.	5.2. ~~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.~~
	Sorgfaltspflichten im Zusammenhang mit der Nutzung des Serviceportals mit mobileTAN
	(1) 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 SMS 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.
	(2) Eine Änderung der zum Empfang von mobileTANs bekannt gegebenen Mobiltelefonnummer ist vom KI entweder selbst im Serviceportal vorzunehmen oder durch Bekanntgabe an die Bank mittels Änderungsformulars zu veranlassen. Die technische Einrichtung zum korrekten Empfang der SMS und die daraus entstehenden Kosten fallen in den Verantwortungsbereich des KI, sodass er auch die diesbezüglichen Kosten zu tragen hat.
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.	5.3. ~~Sollte der Händler das Bezahlen mittels 3D Secure Verfahrens ermöglichen, ist der KI verpflichtet, die Transaktionen im Rahmen des 3D Secure Verfahrens durchzuführen.~~
	Empfohlene Sicherheitsmaßnahmen bei der Nutzung des Serviceportals

	(1) Dem KI wird empfohlen, das gewählte Passwort regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern. (2) Dem KI wird empfohlen, bei Verlust oder Diebstahl des mobilen Endgeräts, auf welches er Identifikationsmerkmale erhält oder auf welchem die myPayLife App installiert ist, unverzüglich das Passwort zu ändern oder die Sperre des Zugangs zum Serviceportal zu veranlassen. (3) Dem KI wird empfohlen, unverzüglich das Passwort zu ändern oder die Sperre des Zugangs zum Serviceportal zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis von den persönlichen Identifikationsmerkmalen haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten den Missbrauch ermöglichen könnten. (4) Dem KI wird empfohlen, seinen Computer bzw. sein mobiles Endgerät, auf welchem die myPayLife App installiert ist, hinsichtlich Risiken aus dem Internet abzusichern, insbesondere eine Firewall und/oder einen aktuellen Virenschutz zu verwenden und diese am aktuellen Stand zu halten, sowie Sicherheitsupdates seines Betriebssystems durchzuführen. (5) Dem KI wird empfohlen, nur Apps aus den geschützten Stores der jeweiligen Anbieter (z.B. Apple App Store, Google Play Store) zu installieren. (6) Um sicher zu sein, dass der KI im Webbrowser mit der Bank verbunden ist, wird dem KI empfohlen, nach Möglichkeit die Zertifikatsinformationen der Transport Layer Security (TLS)-Verschlüsselung auf folgenden Inhalt hin zu überprüfen: Eigentümer: easybank AG Aussteller: www.digicert.com. Ausgestellt für: my.paylife.at
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.	~~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.	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.~~ Sperre: Achtung: Der Zugang zum Serviceportal wird automatisch gesperrt, wenn während eines Zugriffs sechs Mal aufeinanderfolgend das Passwort falsch eingegeben wird. 6.1. Der KI kann die Sperre des Zuganges zum Serviceportal jederzeit telefonisch unter +43 (0)5 99 06-6220 veranlassen. 6.2. Die Aufhebung einer solchen Sperre ist nur durch den KI selbst schriftlich oder telefonisch +43 (0)5 99 06-6220 möglich. 6.3. Die Bank ist berechtigt, das Serviceportal zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit dies rechtfertigen, oder der Verdacht einer nicht autorisierten oder betrügerischen Verwendung besteht. Die Bank wird eine Sperre aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen oder der KI die Aufhebung der Sperre beauftragt.
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	7. ~~Sperre des Zugangs:~~ Aufträge und Erklärungen: 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~~

folgende Kontaktadressen zur Verfügung: E-Mail paylife24@paylife.at; Telefon +43 (0)5 99 06-6220.	~~beauftragen. Die Bank stellt dafür folgende Kontaktadressen zur Verfügung: E-Mail paylife24@paylife.at; Telefon +43 (0)5 99 06-6220.~~ Aufträge und rechtsverbindliche Willenserklärungen sowie sonstige Erklärungen des KI im Serviceportal gelten als vom KI erteilt bzw. abgegeben, wenn der KI diese mittels mobileTAN freigegeben hat.
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. ~~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.~~ Die Abgabe rechtsverbindlicher Willenserklärungen durch den KI kann auch dadurch erfolgen, dass der KI im Serviceportal 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. ~~Änderungen der BGB und der Adresse:~~ Vertragsdauer, Kündigung und Beendigung
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.	8.1. ~~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.~~ Die Vereinbarung über die Teilnahme am Serviceportal wird auf unbestimmte Zeit geschlossen.
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, 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.~~ Der KI ist berechtigt, die Vereinbarung über die Teilnahme am Serviceportal jederzeit ohne Angabe von Gründen und ohne Kündigungsfrist zu kündigen. Nach Einlangen der Kündigung wird die Bank den Zugriff auf das Serviceportal sperren. 8.3. Die Bank ist berechtigt, die Vereinbarung über die Teilnahme am Serviceportal jederzeit unter Einhaltung einer Frist von zwei Monaten ohne Angabe von Gründen zu kündigen. 8.4. Sowohl der KI als auch die Bank sind berechtigt, die Vereinbarung über die Teilnahme am Serviceportal jederzeit bei Vorliegen eines wichtigen Grundes mit sofortiger Wirkung aufzulösen. 8.5. Die Beendigung der Vereinbarung über die Teilnahme am Serviceportal lässt den Kreditkartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären. 8.6. Die Vereinbarung über die Teilnahme am Serviceportal endet automatisch mit dem Ende des Kreditkartenvertrages.
9. Sicherheitshinweise:	9. ~~Sicherheitshinweise:~~ Änderungen der BGB myPayLife
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.	9.1. ~~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.~~ Änderungen der BGB myPayLife 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 im Serviceportal) 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, der Verbraucher ist, das Recht hat, sowohl die Vereinbarung zur Teilnahme am Serviceportal 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.
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. ~~Zur Vermeidung von Risiken, die mit der Kenntnis des Passwortes verbunden sind, empfiehlt die Bank, dieses regelmäßig (z. B. jeden Monat) zu ändern.~~ 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 10. für den KI eingerichtete virtuelle Postfach, wobei der KI über das Vorhandensein des Änderungsangebots in seinem virtuellen Postfach auf die in Punkt 9. geregelte Weise (Push-Nachricht, SMS, E-Mail, Post oder sonst vereinbarte Form) informiert werden wird.
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. ~~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.~~ 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 Serviceportal 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 Serviceportal erforderlich ist, (vi) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für jene Bankgeschäfte, welche der KI über das Serviceportal abwickeln kann, erforderlich ist.
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.	9.4. ~~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.~~ Die Einführung von Entgelten oder die Änderung vereinbarter Entgelte durch eine Änderung dieser Bedingungen für die Teilnahme ams Serviceportal ist ausgeschlossen.
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.	9.5. ~~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.	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.	~~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	~~Fassung Juli 2016, Stand Mai 2018~~ Fassung Juli 2019