

Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Bezugskarten Fassung August 2021

Gegenüberstellung Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Bezugskarten in der zuletzt mit Ihnen vereinbarten Fassung mit der Fassung August 2021. Die folgenden Klauseln sind geändert; alle übrigen Klauseln sind in beiden Fassungen gleich.

Die Besonderen Geschäftsbedingungen für PayLife Bezugskarten sind aus Gründen der leichteren Lesbarkeit nicht geschlechterspezifisch formuliert und gelten in gleicher Weise für alle Geschlechter.

Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Kreditkarten	Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Kreditkarten Bezugskarten
Fassung Juli 2019, Stand März 2020	Fassung September 2019, Stand März 2020 August 2021
<p>1. Allgemeines: Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Kreditkarten (kurz: BGB) regeln 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 für PayLife Kreditkarten (kurz: AGB), die zu dem zwischen der BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (kurz: Bank) und dem Karteninhaber (kurz: KI) geschlossenen Kreditkartenvertrag über die Ausgabe seiner PayLife Kreditkarte (kurz: Karte) vereinbart sind.</p>	<p>1. Allgemeines: Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Kreditkarten Bezugskarten (kurz: BGB) regeln die Abwicklung von Zahlungen mit PayLife Kreditkarten Bezugskarten (Kreditkarten und wiederaufladbare Wertkarten) unter Verwendung des 3D Secure Verfahrens. Die BGB gelten, wenn ihre Geltung vereinbart ist. Sie ergänzen die Allgemeinen Geschäftsbedingungen für die jeweilige PayLife Kreditkarten Bezugskarte (kurz: AGB), die zu dem zwischen der BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (kurz: Bank) und dem Karteninhaber (kurz: KI) geschlossenen Kreditkartenvertrag Kreditkarten- oder Prepaidkartenvertrag über die Ausgabe seiner PayLife Kreditkarte Bezugskarte (kurz: Karte) vereinbart sind.</p>
<p>2. Definition: 2.2.[...] Dieses wird bei Mastercard als „Mastercard Identity Check“ und bei Visa als „Visa Secure“ Passwort bezeichnet und dient der Erteilung von Zahlungsaufträgen im Internet.</p>	<p>2. Definition: 2.2.[...] Dieses wird bei Mastercard als „Mastercard Identity Check“ und bei Visa als „Visa Secure“ Passwort bezeichnet und dient der Erteilung von Zahlungsaufträgen im Internet. Das 3D Secure Passwort ist nur für KI relevant, die eine Registrierung zum 3D Secure Verfahren bis zum 30.11.2021 durchgeführt haben.</p>
<p>2.3.[...] Auch bei der Registrierung zum 3D Secure Verfahren ist die Eingabe einer mobileTAN erforderlich.</p>	<p>2.3.[...] Auch bei der Registrierung zum 3D Secure Verfahren ist die Eingabe einer mobileTAN erforderlich. Die Freigabe von Transaktionen mittels mobileTAN ist nur für KI möglich, die eine Registrierung zum 3D Secure Verfahren bis zum 30.11.2021 durchgeführt haben.</p>
<p>2.4. PayLife secCheck App Die PayLife secCheck App ist eine Applikation (für die Betriebssysteme iOS und Android), die von der Bank zur Verfügung gestellt wird und dient der Erteilung von Internetzahlungen mittels biometrischem Sicherheitsmerkmal (bspw. Fingerabdruck, Gesichtserkennung) oder App PIN. Im Zuge der Registrierung in der PayLife secCheck App wählt der KI zur Erteilung von Internetzahlungen ein biometrisches Sicherheitsmerkmal und eine Geheimzahl (App PIN). Wenn das mobile Endgerät über keine Funktionen zur Überprüfung der biometrischen Sicherheitsmerkmale (bspw. Fingerabdruck Sensor) verfügt, wählt der KI eine Geheimzahl (App PIN). Die App PIN kann vom KI jederzeit unter my.paylife.at geändert werden</p>	<p>2.4. PayLife secCheck App-myPayLife App Die PayLife secCheck App myPayLife App ist eine Applikation (für die Betriebssysteme iOS und Android), die von der Bank zur Verfügung gestellt wird und dient der Erteilung von Internetzahlungen mittels biometrischem Sicherheitsmerkmal (bspw. Fingerabdruck, Gesichtserkennung) oder App PIN- oder App Code. Im Zuge der Registrierung in der PayLife secCheck App myPayLife App wählt der KI zur Erteilung von Internetzahlungen ein biometrisches Sicherheitsmerkmal und eine Geheimzahl (App PIN App Code). Wenn das mobile Endgerät über keine Funktionen zur Überprüfung der biometrischen Sicherheitsmerkmale (bspw. Fingerabdruck Sensor) verfügt, wählt der KI eine Geheimzahl (App PIN App Code).</p>

	<p>Die App PIN Der App Code kann vom KI jederzeit unter my.paylife.at oder in der myPayLife App geändert werden.</p>
2.5. [...] Bei der mobileTAN handelt es sich um einen solchen Authentifizierungscode.	2.5. [...] Bei der mobileTAN oder App Code handelt es sich um einen solchen Authentifizierungscode.
2.6. [...] 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 Authentifizierungscode nach sich.	2.6. [...] Die starke Kundenauthentifizierung basiert auf (mindestens) zwei Faktoren der Kategorien Wissen (z.B. Passwort, App Code), Besitz (z.B. Smartphone) und Inhärenz (z.B. Fingerabdruck, Gesichtserkennung) und zieht die Generierung eines Authentifizierungscode nach sich.
<p>3. Registrierung zum 3D Secure Verfahren:</p> <p>3.1. Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KI für 3D Secure voraus. Die Registrierung wird in den Online Services („my.paylife.at“) durchgeführt. Auf der Website www.paylife.at/3dsecure wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KI im Zuge der Registrierung zum 3D Secure Verfahren wird dem KI eine mobileTAN per SMS an die von ihm für die Zusendung einer mobileTAN bekannt gegebenen Mobiltelefonnummer, geschickt.</p>	<p>3. Registrierung zum 3D Secure Verfahren:</p> <p>3.1. Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KI für 3D Secure voraus. Möglichkeit für Registrierungen bis 30.11.2021 (Registrierung über my.paylife.at): Die Registrierung wird in den Online Services („my.paylife.at“) durchgeführt. Auf der Website www.paylife.at/3dsecure wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KI im Zuge der Registrierung zum 3D Secure Verfahren wird dem KI eine mobileTAN per SMS an die von ihm für die Zusendung einer mobileTAN bekannt gegebenen Mobiltelefonnummer, geschickt. Möglichkeit ab August 2021 (Registrierung über die myPayLife App): Die Registrierung wird in der myPayLife App durchgeführt. Auf der Website www.paylife.at/3dsecure wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KI im Zuge der Registrierung für die myPayLife App muss der KI seine Kundennummer und 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.</p>
<p>3.2. Der KI hat im Zuge der Registrierung persönliche Identifikationsmerkmale selbst festzulegen:</p> <ul style="list-style-type: none"> • 3D Secure Passwort (Mastercard Identity Check bzw. Visa Secure Passwort) oder • unter Zuhilfenahme der PayLife secCheck App ein biometrisches Sicherheitsmerkmal (bspw. Fingerabdruck) und die App PIN. <p>Der KI kann seine persönlichen Identifikationsmerkmale jederzeit selbst ändern. Hat der KI sein von ihm gewähltes Passwort vergessen, so hat er die Möglichkeit ein neues 3D Secure Passwort bzw. eine neue App PIN über die Registrierungswebsite zu setzen. [...]</p>	<p>3.2. Der KI hat im Zuge der Registrierung persönliche Identifikationsmerkmale selbst festzulegen:</p> <p>Gilt für alle Registrierungen über my.paylife.at bis 30.11.2021:</p> <ul style="list-style-type: none"> • 3D Secure Passwort (Mastercard Identity Check bzw. Visa Secure Passwort) oder • unter Zuhilfenahme der PayLife secCheck App ein biometrisches Sicherheitsmerkmal (bspw. Fingerabdruck) und die App PIN. <p>Gilt für alle Registrierungen über die myPayLife App ab August 2021:</p> <ul style="list-style-type: none"> • unter Zuhilfenahme der myPayLife App ein biometrisches Sicherheitsmerkmal (z.B. Fingerabdruck) oder • unter Zuhilfenahme der myPayLife App einen App Code. <p>Der KI kann seine persönlichen Identifikationsmerkmale jederzeit selbst unter my.paylife.at oder in der myPayLife App ändern. Hat der KI sein von ihm gewähltes Passwort vergessen, so hat er die Möglichkeit ein neues 3D Secure Passwort bzw. eine neue App PIN über die Registrierungswebsite zu setzen. [...]</p>
<p>4. Zahlen mit 3D Secure:</p> <p>Zahlungstransaktionen im Internet kann der KI entweder mit seinem selbst festgelegten 3D Secure Passwort und einer mobileTAN oder durch Verwendung der PayLife secCheck App mit seinem biometrischen Sicherheitsmerkmal oder der App PIN durchführen.</p>	<p>4. Zahlen mit 3D Secure:</p> <p>Gilt für alle Registrierungen bis 30.11.2021: Zahlungstransaktionen im Internet kann der KI entweder mit seinem selbst festgelegten 3D Secure Passwort und einer mobileTAN oder durch Verwendung der PayLife secCheck App mit seinem</p>

	<p>biometrischen Sicherheitsmerkmal oder der App-PIN durchführen.</p> <p>Gilt für alle Registrierungen ab August 2021: Zahlungstransaktionen im Internet kann der KI durch Verwendung der myPayLife App mit seinem biometrischen Sicherheitsmerkmal oder dem App Code durchführen.</p>
<p>5. Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen bei der Verwendung von 3D Secure</p>	<p>5. Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen bei der Verwendung von 3D Secure</p>
<p>5.2. Geheimhaltungs- und Sperrverpflichtung: 5.2.1. Der KI hat sein 3D Secure Passwort und die App PIN geheim zu halten und darf diese nicht an unbefugte Dritte weitergeben; die E-Mail-Adresse ist von der Geheimhaltungsverpflichtung ausgenommen. [...]</p>	<p>5.2. Geheimhaltungs- und Sperrverpflichtung: 5.2.1. Der KI hat sein 3D Secure Passwort und die App-PIN seinen App Code geheim zu halten und darf diese nicht an unbefugte Dritte weitergeben; die E-Mail-Adresse ist von der Geheimhaltungsverpflichtung ausgenommen. [...]</p>
<p>5.2.2. Der KI ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung seines 3D Secure Passworts und der App PIN walten zu lassen, um einen Missbrauch zu vermeiden. Der KI hat insbesondere darauf zu achten, dass sein 3D Secure Passwort und die App-PIN bei deren Verwendung nicht ausgespäht werden; er darf sie auch nicht in seinem mobilen Endgerät, auf welchem er die PayLife secCheck App installiert hat, speichern bzw. elektronisch notieren, etwa in einer App für Notizen.</p>	<p>5.2.2. Der KI ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung seines 3D Secure Passworts und der App-PIN App Code walten zu lassen, um einen Missbrauch zu vermeiden. Der KI hat insbesondere darauf zu achten, dass sein 3D Secure Passwort und die App-PIN App Code bei deren Verwendung nicht ausgespäht werden; er darf sie auch nicht in seinem mobilen Endgerät, auf welchem er die PayLife secCheck App myPayLife App installiert hat, speichern bzw. elektronisch notieren, etwa in einer App für Notizen.</p>
<p>5.2.3. Bei Verlust von 3D Secure Passwort und/oder App-PIN sowie dann, wenn der KI von einer missbräuchlichen Verwendung oder einer sonstigen nicht autorisierten Nutzung des 3D Secure Verfahren Kenntnis erlangt hat, hat der KI die Sperre des 3D Secure Verfahrens unverzüglich zu veranlassen.</p>	<p>5.2.3. Bei Verlust von 3D Secure Passwort und/oder App-PIN App Code sowie dann, wenn der KI von einer missbräuchlichen Verwendung oder einer sonstigen nicht autorisierten Nutzung des 3D Secure Verfahren Kenntnis erlangt hat, hat der KI die Sperre des 3D Secure Verfahrens unverzüglich zu veranlassen.</p>
<p>5.2.4. Bei Verlust oder Diebstahl jenes mobilen Endgerätes des KI, auf welchem die PayLife secCheck App installiert ist, hat der KI unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen.</p>	<p>5.2.4. Bei Verlust oder Diebstahl jenes mobilen Endgerätes des KI, auf welchem die PayLife secCheck App myPayLife App installiert ist, hat der KI unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen.</p>
<p>5.3. Sorgfaltspflichten zur Sperre des Endgeräts und bei der Installation: 5.3.1. Der KI ist verpflichtet, den Zugang zum Gebrauch des mobilen Endgerätes, auf welchem PayLife secCheck App installiert ist, bzw. den Zugriff auf dort gespeicherte Daten für Nichtberechtigte zu sperren, wenn er das Endgerät nicht benutzt.</p>	<p>5.3. Sorgfaltspflichten zur Sperre des Endgeräts und bei der Installation: 5.3.1. Der KI ist verpflichtet, den Zugang zum Gebrauch des mobilen Endgerätes, auf welchem PayLife secCheck App die myPayLife App installiert ist, bzw. den Zugriff auf dort gespeicherte Daten für Nichtberechtigte zu sperren, wenn er das Endgerät nicht benutzt.</p>
<p>5.3.2. Der KI darf die PayLife secCheck App ausschließlich aus dem Apple App Store oder dem Google Play Store installieren.</p>	<p>5.3.2. Der KI darf die PayLife secCheck App myPayLife App ausschließlich aus dem Apple App Store oder dem Google Play Store installieren.</p>
<p>5.4. Sorgfaltspflichten bei Aufträgen: 5.4.2. Zahlungsfreigabe mittels PayLife secCheckApp Die in die PayLife secCheck App übermittelten Daten sind vom KI vor der Zahlungsfreigabe auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit dem gewünschten Zahlungsauftrag darf die Zahlungsfreigabe erfolgen.</p>	<p>5.4. Sorgfaltspflichten bei Aufträgen: 5.4.2. Zahlungsfreigabe mittels PayLife secCheck App myPayLife App Die in die PayLife secCheck App myPayLife App übermittelten Daten sind vom KI vor der Zahlungsfreigabe auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit dem gewünschten Zahlungsauftrag darf die Zahlungsfreigabe erfolgen.</p>
<p>5.5. Empfohlene Sicherheitsmaßnahmen bei der Verwendung des 3D Secure Zahlungsverfahrens: 5.5.1. Dem KI wird empfohlen, das 3D Secure Passwort und die App PIN regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.</p>	<p>5.5. Empfohlene Sicherheitsmaßnahmen bei der Verwendung des 3D Secure Zahlungsverfahrens: 5.5.1. Dem KI wird empfohlen, das 3D Secure Passwort und die App-PIN den App Code regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.</p>

<p>5.5.2 Dem KI wird empfohlen, unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis von Passwort und/oder App PIN erlangt haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen könnten.</p>	<p>5.5.2 Dem KI wird empfohlen, unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis von Passwort und/oder App PIN App Code erlangt haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen könnten.</p>
<p>5.5.3. Dem KI wird empfohlen, sein mobiles Endgerät, auf welchem er die mobileTAN bekommt und/oder die PayLife secCheck App installiert ist, hinsichtlich Risiken aus dem Internet abzusichern, insbesondere einen aktuellen Virenschutz zu verwenden und diesen am aktuellen Stand zu halten, sowie Sicherheitsupdates des Betriebssystems des mobilen Endgeräts durchzuführen.</p>	<p>5.5.3. Dem KI wird empfohlen, sein mobiles Endgerät, auf welchem er die mobileTAN bekommt und/oder die PayLife secCheck App myPayLife App installiert ist, hinsichtlich Risiken aus dem Internet abzusichern, insbesondere einen aktuellen Virenschutz zu verwenden und diesen am aktuellen Stand zu halten, sowie Sicherheitsupdates des Betriebssystems des mobilen Endgeräts durchzuführen.</p>
<p>7. Sperre des 3D Secure Verfahrens: 7.1. Automatische Sperre Aus Sicherheitsgründen wird nach fünf Mal aufeinanderfolgender falscher Eingabe der persönlichen Identifikationsmerkmale, das 3D Secure Verfahren von der Bank gesperrt. Solange die Sperre aufrecht ist, kann der KI keine Zahlungsanweisungen mit dem 3D Secure Verfahren durchführen.</p>	<p>7. Sperre des 3D Secure Verfahrens: 7.1. Automatische Sperre Aus Sicherheitsgründen wird nach fünf Mal aufeinanderfolgender falscher Eingabe der des persönlichen Identifikationsmerkmale Identifikationsmerkmals (Passwort) oder nach drei Mal aufeinanderfolgender falscher Eingabe des App Codes, das 3D Secure Verfahren von der Bank gesperrt. Solange die Sperre aufrecht ist, kann der KI keine Zahlungsanweisungen mit dem 3D Secure Verfahren durchführen.</p>
<p>7.2. Sperre durch den KI Der KI kann die Sperre des 3D Secure Verfahrens durch die fünf Mal aufeinanderfolgende falsche Eingabe der persönlichen Identifikationsmerkmale selbst vornehmen oder telefonisch unter +43 (0)5 99 06-6220 veranlassen.</p>	<p>7.2. Sperre durch den KI Der KI kann die Sperre des 3D Secure Verfahrens durch die fünf bzw. drei Mal aufeinanderfolgende falsche Eingabe der persönlichen Identifikationsmerkmale selbst unter my.paylife.at vornehmen oder telefonisch unter +43 (0)5 99 06-6220 veranlassen.</p>
<p>7.4. Bekanntgabe und Aufhebung der Sperre 7.4.3 Der KI kann die Aufhebung einer Sperre telefonisch unter +43 (0)5 99 06-6220 beauftragen. Der KI kann die Sperre auch selbstständig in den Online Services („myPayLife“) durch Setzen eines neuen Passworts aufheben.</p>	<p>7.4. Bekanntgabe und Aufhebung der Sperre 7.4.3 Der KI kann die Aufhebung einer Sperre telefonisch unter +43 (0)5 99 06-6220 beauftragen. Der KI kann die Sperre auch selbstständig in den Online Services („myPayLife“) durch Setzen eines neuen Passworts aufheben.</p>
<p>8. Änderungen der Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Kreditkarten:</p>	<p>8. Änderungen der Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für PayLife Kreditkarten Bezugskarten:</p>
<p>8.1. [...]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 zur Teilnahme am 3D Secure als auch den Kreditkartenvertrag vor Inkrafttreten der Änderungen kostenlos fristlos zu kündigen. [...]</p>	<p>8.1. [...]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 zur Teilnahme am 3D Secure als auch den Kreditkartenvertrag Kreditkarten- oder Prepaidkartenvertrag vor Inkrafttreten der Änderungen kostenlos fristlos zu kündigen. [...]</p>
<p>10. Sicherheitshinweise: 10.2. Zur Vermeidung von Risiken, die mit der Kenntnis der Identifikationsmerkmale (insbesondere des 3D Secure Passworts) verbunden sind, empfiehlt die Bank, diese regelmäßig (z. B. jeden Monat) zu ändern.</p>	<p>10. Sicherheitshinweise: 10.2. Zur Vermeidung von Risiken, die mit der Kenntnis der Identifikationsmerkmale (insbesondere des 3D Secure Passworts und des App Codes) verbunden sind, empfiehlt die Bank, diese regelmäßig (z. B. jeden Monat) zu ändern.</p>
<p>10.3. Sollte der KI den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen (insbesondere dem 3D Secure Passwort) erlangt haben, so empfiehlt die Bank die Identifikationsmerkmale zu ändern.</p>	<p>10.3. Sollte der KI den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen (insbesondere dem 3D Secure Passwort und dem App Code) erlangt haben, so empfiehlt die Bank die Identifikationsmerkmale zu ändern.</p>

<p>11. Vertragsdauer, Kündigung und Beendigung: 11.5. Die Beendigung der Vereinbarung lässt den Kreditkartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.</p>	<p>11. Vertragsdauer, Kündigung und Beendigung: 11.5. Die Beendigung der Vereinbarung lässt den Kreditkartenvertrag Kreditkarten- oder Prepaidkartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.</p>
<p>11.6. Die Vereinbarung endet automatisch mit dem Ende des Kreditkartenvertrages.</p>	<p>11.6. Die Vereinbarung endet automatisch mit dem Ende des Kreditkartenvertrages Kreditkarten- oder Prepaidkartenvertrages.</p>
<p>Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten</p>	<p>Besondere Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten</p>
<p>1. Allgemeines Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten (kurz: BGB 3DS) regeln die Abwicklung von Zahlungen mit wiederaufladbaren PayLife Wertkarten unter Verwendung des 3D Secure Verfahrens. Die BGB 3DS gelten, wenn ihre Geltung vereinbart ist. Sie ergänzen die Allgemeinen Geschäftsbedingungen für wiederaufladbare PayLife Wertkarten (kurz: AGB), die zu dem zwischen der BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (kurz: Bank) und dem Karteninhaber (kurz: KI) geschlossenen Prepaidkartenvertrag über die Ausgabe seiner wiederaufladbaren PayLife Wertkarte (kurz: Karte) vereinbart sind.</p>	<p>1. Allgemeines Diese Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten (kurz: BGB 3DS) regeln die Abwicklung von Zahlungen mit wiederaufladbaren PayLife Wertkarten unter Verwendung des 3D Secure Verfahrens. Die BGB 3DS gelten, wenn ihre Geltung vereinbart ist. Sie ergänzen die Allgemeinen Geschäftsbedingungen für wiederaufladbare PayLife Wertkarten (kurz: AGB), die zu dem zwischen der BAWAG P.S.K. Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse Aktiengesellschaft (kurz: Bank) und dem Karteninhaber (kurz: KI) geschlossenen Prepaidkartenvertrag über die Ausgabe seiner wiederaufladbaren PayLife Wertkarte (kurz: Karte) vereinbart sind.</p>
<p>2. Definitionen 2.1. 3D Secure Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das die Voraussetzungen der starken Kundenauthentifizierung erfüllt. 2.2. "3D Secure Passwort": Mastercard Identity Check Das 3D Secure Passwort ist das vom KI bei der Registrierung zum 3D Secure Verfahren festgelegte Geheimwort (Kombination aus Zeichen). Dieses wird bei Mastercard als „Mastercard Identity Check“ bezeichnet und dient der Erteilung von Zahlungsaufträgen im Internet. 2.3. Mobile Transaktionsnummer (kurz: mobileTAN) Die mobileTAN ist eine einmalig verwendbare Transaktionsnummer, die an die vom KI für die Zecke der Zustellung der mobileTAN bekannt gegebene Mobiltelefonnummer, per SMS gesendet wird. Die mobileTAN dient der Erteilung eines Zahlungsauftrages im Internet als zusätzliches Sicherheitsmerkmal zum 3D Secure Passwort. Auch bei der Registrierung zum 3D Secure Verfahren ist die Eingabe einer mobileTAN erforderlich. 2.4. PayLife secCheckApp Die PayLife secCheck App ist eine Applikation (für die Betriebssysteme iOS und Android), die von der Bank zur Verfügung gestellt wird und dient der Erteilung von Internetzahlungen mittels biometrischem Sicherheitsmerkmal (bspw. Fingerabdruck, Gesichtserkennung) oder App PIN. Im Zuge der Registrierung in der PayLife secCheck App wählt der KI zur Erteilung von Internetzahlungen ein biometrisches Sicherheitsmerkmal und eine Geheimzahl (App PIN). Wenn das mobile Endgerät über keine Funktionen zur Überprüfung der biometrischen Sicherheitsmerkmale (bspw. Fingerabdruck Sensor) verfügt, wählt der KI eine</p>	<p>2. Definitionen 2.1. 3D Secure Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das die Voraussetzungen der starken Kundenauthentifizierung erfüllt. 2.2. "3D Secure Passwort": Mastercard Identity Check Das 3D Secure Passwort ist das vom KI bei der Registrierung zum 3D Secure Verfahren festgelegte Geheimwort (Kombination aus Zeichen). Dieses wird bei Mastercard als „Mastercard Identity Check“ bezeichnet und dient der Erteilung von Zahlungsaufträgen im Internet. 2.3. Mobile Transaktionsnummer (kurz: mobileTAN) Die mobileTAN ist eine einmalig verwendbare Transaktionsnummer, die an die vom KI für die Zecke der Zustellung der mobileTAN bekannt gegebene Mobiltelefonnummer, per SMS gesendet wird. Die mobileTAN dient der Erteilung eines Zahlungsauftrages im Internet als zusätzliches Sicherheitsmerkmal zum 3D Secure Passwort. Auch bei der Registrierung zum 3D Secure Verfahren ist die Eingabe einer mobileTAN erforderlich. 2.4. PayLife secCheckApp Die PayLife secCheck App ist eine Applikation (für die Betriebssysteme iOS und Android), die von der Bank zur Verfügung gestellt wird und dient der Erteilung von Internetzahlungen mittels biometrischem Sicherheitsmerkmal (bspw. Fingerabdruck, Gesichtserkennung) oder App PIN. Im Zuge der Registrierung in der PayLife secCheck App wählt der KI zur Erteilung von Internetzahlungen ein biometrisches Sicherheitsmerkmal und eine Geheimzahl (App PIN). Wenn das mobile Endgerät über keine Funktionen zur Überprüfung der biometrischen Sicherheitsmerkmale (bspw. Fingerabdruck Sensor) verfügt, wählt der KI eine</p>

<p>Geheimzahl (App PIN). Die App PIN kann vom KI jederzeit auf der Registrierungsseite geändert werden.</p> <p>2.5. 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 3D Secure Passwortes bzw. bei Verwendung der PayLife secCheck App durch die Definition eines biometrischen Sicherheitsmerkmals und App PIN, ersetzt.</p> <p>2.6. 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.</p> <p>2.7. 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 Authentifizierungscode nach sich.</p>	<p>Geheimzahl (App PIN). Die App PIN kann vom KI jederzeit auf der Registrierungsseite geändert werden.</p> <p>2.5. 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 3D Secure Passwortes bzw. bei Verwendung der PayLife secCheck App durch die Definition eines biometrischen Sicherheitsmerkmals und App PIN, ersetzt.</p> <p>2.6. 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.</p> <p>2.7. 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 Authentifizierungscode nach sich.</p>
<p>3. Registrierung zum 3D Secure Verfahren</p> <p>3.1. Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KI für 3D Secure voraus. Die Registrierung kann auf der Website www.paylife.at/3dsecure gestartet werden. Auf der Website www.paylife.at/3dsecure wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KI sind ein gültiges Einmalpasswort sowie eine mobileTAN erforderlich. Im Zuge der Registrierung zum 3D Secure Verfahren wird dem KI eine mobileTAN per SMS an die von ihm für die Zusendung einer mobileTAN bekannt gegebenen Mobiltelefonnummer, geschickt.</p> <p>3.2. Der KI hat im Zuge der Registrierung persönliche Identifikationsmerkmale selbst festzulegen:</p> <ul style="list-style-type: none"> • 3D Secure Passwort (Mastercard Identity Check Passwort) oder • unter Zuhilfenahme der PayLife secCheck App ein biometrisches Sicherheitsmerkmal (bspw. Fingerabdruck) und die App PIN. <p>Der KI kann seine persönlichen Identifikationsmerkmale jederzeit selbst ändern. Hat der KI sein von ihm gewähltes Passwort vergessen, so hat er die Möglichkeit ein neues 3D Secure Passwort bzw. eine neue App PIN über die Registrierungswebsite zu setzen. Im Rahmen der Registrierung zum 3D Secure Verfahren hat der KI seine E-Mailadresse bekannt zu geben. Die technische Einrichtung zum korrekten Empfang der SMS und die daraus entstehenden Kosten fallen in den Verantwortungsbereich des KI.</p>	<p>3. Registrierung zum 3D Secure Verfahren</p> <p>3.1. Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des KI für 3D Secure voraus. Die Registrierung kann auf der Website www.paylife.at/3dsecure gestartet werden. Auf der Website www.paylife.at/3dsecure wird dem KI der Ablauf der Registrierung erklärt. Für die Identifizierung des KI sind ein gültiges Einmalpasswort sowie eine mobileTAN erforderlich. Im Zuge der Registrierung zum 3D Secure Verfahren wird dem KI eine mobileTAN per SMS an die von ihm für die Zusendung einer mobileTAN bekannt gegebenen Mobiltelefonnummer, geschickt.</p> <p>3.2. Der KI hat im Zuge der Registrierung persönliche Identifikationsmerkmale selbst festzulegen:</p> <ul style="list-style-type: none"> • 3D Secure Passwort (Mastercard Identity Check Passwort) oder • unter Zuhilfenahme der PayLife secCheck App ein biometrisches Sicherheitsmerkmal (bspw. Fingerabdruck) und die App PIN. <p>Der KI kann seine persönlichen Identifikationsmerkmale jederzeit selbst ändern. Hat der KI sein von ihm gewähltes Passwort vergessen, so hat er die Möglichkeit ein neues 3D Secure Passwort bzw. eine neue App PIN über die Registrierungswebsite zu setzen. Im Rahmen der Registrierung zum 3D Secure Verfahren hat der KI seine E-Mailadresse bekannt zu geben. Die technische Einrichtung zum korrekten Empfang der SMS und die daraus entstehenden Kosten fallen in den Verantwortungsbereich des KI.</p>
<p>4. Zahlen mit 3D Secure Zahlungstransaktionen im Internet kann der KI entweder mit seinem selbst festgelegten 3D Secure</p>	<p>4. Zahlen mit 3D Secure Zahlungstransaktionen im Internet kann der KI entweder mit seinem selbst festgelegten 3D Secure</p>

<p>Passwort und einer mobilen TAN oder durch Verwendung der PayLife secCheck App mit seinem biometrischen Sicherheitsmerkmal oder der App PIN durchführen.</p>	<p>Passwort und einer mobilen TAN oder durch Verwendung der PayLife secCheck App mit seinem biometrischen Sicherheitsmerkmal oder der App PIN durchführen.</p>
<p>5. Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen bei der Verwendung von 3D Secure</p> <p>5.1. Einhaltung und Rechtsfolgen Jeder KI ist zur Einhaltung der in Punkt 5.4. enthaltenen Sorgfaltspflichten verpflichtet. KI sind zusätzlich zur Einhaltung der in Punkt 5.5 empfohlenen Sicherheitsmaßnahmen verpflichtet. KI, die Verbraucher sind, empfiehlt die Bank die Einhaltung der empfohlenen Sicherheitsmaßnahmen, ohne dass Verbraucher zur Einhaltung verpflichtet sind. Eine Verletzung dieser Verpflichtungen kann gemäß Punkt 6 zu Schadenersatzpflichten des KI oder zum Entfall bzw. zur Minderung seiner Schadenersatzansprüche gegenüber der Bank führen.</p> <p>5.2. Geheimhaltungs- und Sperrverpflichtung 5.2.1 Der KI hat sein 3D Secure Passwort und die App PIN geheim zu halten und darf diese nicht an unbefugte Dritte weitergeben; die E-Mail-Adresse ist von der Geheimhaltungsverpflichtung ausgenommen. Die Weitergabe der persönlichen Identifikationsmerkmale an Zahlungsauslösedienstleister und Kontoinformationsdienstleister ist jedoch zulässig, soweit sie erforderlich ist, damit diese ihre Dienstleistungen für den KI erbringen können. 5.2.2. Der KI ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung seines 3D Secure Passworts und der App PIN zu walten, um einen Missbrauch zu vermeiden. Der KI hat insbesondere darauf zu achten, dass sein 3D Secure Passwort und die App-PIN bei deren Verwendung nicht ausgespäht werden; er darf sie auch nicht in seinem mobilen Endgerät, auf welchem er die PayLife secCheck App installiert hat, speichern bzw. elektronisch notieren, etwa in einer App für Notizen. 5.2.3. Bei Verlust von 3D Secure Passwort und/oder App-PIN sowie dann, wenn der KI von einer missbräuchlichen Verwendung oder einer sonstigen nicht autorisierten Nutzung des 3D Secure Verfahrens Kenntnis erlangt hat, hat der KI die Sperre des 3D Secure Verfahrens unverzüglich zu veranlassen. 5.2.4. Bei Verlust oder Diebstahl jenes mobilen Endgerätes des KI, auf welchem die PayLife secCheck App installiert ist, hat der KI unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen.</p> <p>5.3. Sorgfaltspflichten zur Sperre des Endgeräts und bei der Installation 5.3.1. Der KI ist verpflichtet, den Zugang zum Gebrauch des mobilen Endgerätes, auf welchem PayLife secCheck App installiert ist, bzw. den Zugriff auf dort gespeicherte Daten für Nichtberechtigte zu sperren, wenn er das Endgerät nicht benutzt. 5.3.2. Der KI darf die PayLife secCheck App ausschließlich aus dem Apple App Store oder dem Google Play Store installieren.</p> <p>5.4. Sorgfaltspflichten bei Aufträgen 5.4.1. Zahlungsfreigabe mit mobiler TAN Die in der mobilen TAN angezeigten Daten sind vom KI vor der Verwendung auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit</p>	<p>5. Sorgfaltspflichten und empfohlene Sicherheitsmaßnahmen bei der Verwendung von 3D Secure</p> <p>5.1. Einhaltung und Rechtsfolgen Jeder KI ist zur Einhaltung der in Punkt 5.4. enthaltenen Sorgfaltspflichten verpflichtet. KI sind zusätzlich zur Einhaltung der in Punkt 5.5 empfohlenen Sicherheitsmaßnahmen verpflichtet. KI, die Verbraucher sind, empfiehlt die Bank die Einhaltung der empfohlenen Sicherheitsmaßnahmen, ohne dass Verbraucher zur Einhaltung verpflichtet sind. Eine Verletzung dieser Verpflichtungen kann gemäß Punkt 6 zu Schadenersatzpflichten des KI oder zum Entfall bzw. zur Minderung seiner Schadenersatzansprüche gegenüber der Bank führen.</p> <p>5.2. Geheimhaltungs- und Sperrverpflichtung 5.2.1 Der KI hat sein 3D Secure Passwort und die App PIN geheim zu halten und darf diese nicht an unbefugte Dritte weitergeben; die E-Mail-Adresse ist von der Geheimhaltungsverpflichtung ausgenommen. Die Weitergabe der persönlichen Identifikationsmerkmale an Zahlungsauslösedienstleister und Kontoinformationsdienstleister ist jedoch zulässig, soweit sie erforderlich ist, damit diese ihre Dienstleistungen für den KI erbringen können. 5.2.2. Der KI ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung seines 3D Secure Passworts und der App PIN zu walten, um einen Missbrauch zu vermeiden. Der KI hat insbesondere darauf zu achten, dass sein 3D Secure Passwort und die App-PIN bei deren Verwendung nicht ausgespäht werden; er darf sie auch nicht in seinem mobilen Endgerät, auf welchem er die PayLife secCheck App installiert hat, speichern bzw. elektronisch notieren, etwa in einer App für Notizen. 5.2.3. Bei Verlust von 3D Secure Passwort und/oder App-PIN sowie dann, wenn der KI von einer missbräuchlichen Verwendung oder einer sonstigen nicht autorisierten Nutzung des 3D Secure Verfahrens Kenntnis erlangt hat, hat der KI die Sperre des 3D Secure Verfahrens unverzüglich zu veranlassen. 5.2.4. Bei Verlust oder Diebstahl jenes mobilen Endgerätes des KI, auf welchem die PayLife secCheck App installiert ist, hat der KI unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen.</p> <p>5.3. Sorgfaltspflichten zur Sperre des Endgeräts und bei der Installation 5.3.1. Der KI ist verpflichtet, den Zugang zum Gebrauch des mobilen Endgerätes, auf welchem PayLife secCheck App installiert ist, bzw. den Zugriff auf dort gespeicherte Daten für Nichtberechtigte zu sperren, wenn er das Endgerät nicht benutzt. 5.3.2. Der KI darf die PayLife secCheck App ausschließlich aus dem Apple App Store oder dem Google Play Store installieren.</p> <p>5.4. Sorgfaltspflichten bei Aufträgen 5.4.1. Zahlungsfreigabe mit mobiler TAN Die in der mobilen TAN angezeigten Daten sind vom KI vor der Verwendung auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit</p>

<p>dem gewünschten Zahlungsauftrag darf die mobile TAN zur Erteilung von Aufträgen verwendet werden.</p> <p>5.4.2. Zahlungsfreigabe mittels PayLife secCheck App Die in die PayLife secCheck App übermittelten Daten sind vom KI vor der Zahlungsfreigabe auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit dem gewünschten Zahlungsauftrag darf die Zahlungsfreigabe erfolgen.</p> <p>5.5. Empfohlene Sicherheitsmaßnahmen bei der Verwendung des 3D Secure Zahlungsverfahrens</p> <p>5.5.1. Dem KI wird empfohlen, das 3D Secure Passwort und die App PIN regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.</p> <p>5.5.2 Dem KI wird empfohlen, unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis von Passwort und/oder App PIN erlangt haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen könnten.</p> <p>5.5.3. Dem KI wird empfohlen, sein mobiles Endgerät, auf welchem er die mobile TAN bekommt und/oder die PayLife secCheck App installiert ist, hinsichtlich Risiken aus dem Internet abzusichern, insbesondere einen aktuellen Virenschutz zu verwenden und diesen am aktuellen Stand zu halten, sowie Sicherheitsupdates des Betriebssystems des mobilen Endgeräts durchzuführen.</p>	<p>dem gewünschten Zahlungsauftrag darf die mobile TAN zur Erteilung von Aufträgen verwendet werden.</p> <p>5.4.2. Zahlungsfreigabe mittels PayLife secCheck App Die in die PayLife secCheck App übermittelten Daten sind vom KI vor der Zahlungsfreigabe auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit dem gewünschten Zahlungsauftrag darf die Zahlungsfreigabe erfolgen.</p> <p>5.5. Empfohlene Sicherheitsmaßnahmen bei der Verwendung des 3D Secure Zahlungsverfahrens</p> <p>5.5.1. Dem KI wird empfohlen, das 3D Secure Passwort und die App PIN regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.</p> <p>5.5.2 Dem KI wird empfohlen, unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis von Passwort und/oder App PIN erlangt haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen könnten.</p> <p>5.5.3. Dem KI wird empfohlen, sein mobiles Endgerät, auf welchem er die mobile TAN bekommt und/oder die PayLife secCheck App installiert ist, hinsichtlich Risiken aus dem Internet abzusichern, insbesondere einen aktuellen Virenschutz zu verwenden und diesen am aktuellen Stand zu halten, sowie Sicherheitsupdates des Betriebssystems des mobilen Endgeräts durchzuführen.</p>
<p>6. Haftung des KI</p> <p>6.1. 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 5. zugefügt hat. Hat der KI die Sorgfaltspflichten gemäß Punkt 5. 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.</p> <p>6.2. 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 6.1. bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 5. nicht. Der KI haftet bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 5. auch dann nicht, wenn die Bank den Verlust der persönlichen Identifikationsmerkmale verursacht hat.</p> <p>6.3. Abweichend von Punkt 6.1. 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.</p> <p>6.4. Der KI haftet nicht, wenn der Schaden aus einer nicht autorisierten Nutzung der Karte bei einer Onlinezahlung nach Beauftragung der Sperre gemäß</p>	<p>6. Haftung des KI</p> <p>6.1. 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 5. zugefügt hat. Hat der KI die Sorgfaltspflichten gemäß Punkt 5. 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.</p> <p>6.2. 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 6.1. bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 5. nicht. Der KI haftet bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß Punkt 5. auch dann nicht, wenn die Bank den Verlust der persönlichen Identifikationsmerkmale verursacht hat.</p> <p>6.3. Abweichend von Punkt 6.1. 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.</p> <p>6.4. Der KI haftet nicht, wenn der Schaden aus einer nicht autorisierten Nutzung der Karte bei einer Onlinezahlung nach Beauftragung der Sperre gemäß</p>

<p>Punkt 7. entstanden ist, es sei denn, der KI hat in betrügerischer Absicht gehandelt.</p>	<p>Punkt 7. entstanden ist, es sei denn, der KI hat in betrügerischer Absicht gehandelt.</p>
<p>7. Sperre des 3D Secure Verfahrens</p> <p>7.1. Automatische Sperre Aus Sicherheitsgründen wird nach fünf Mal aufeinanderfolgender falscher Eingabe der persönlichen Identifikationsmerkmale, das 3D Secure Verfahren von der Bank gesperrt. Solange die Sperre aufrecht ist, kann der KI keine Zahlungsanweisungen mit dem 3D Secure Verfahren durchführen.</p> <p>7.2. Sperre durch den KI Der KI kann die Sperre des 3D Secure Verfahrens durch die fünf Mal aufeinanderfolgende falsche Eingabe der persönlichen Identifikationsmerkmale selbst vornehmen oder telefonisch unter +43 (0)5 99 06-6220 veranlassen.</p> <p>7.3. Sperre durch die Bank</p> <p>7.3.1. Die Bank ist berechtigt, das 3D Secure Verfahren für den KI zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit dies rechtfertigen oder der Verdacht einer nicht autorisierten oder betrügerischen Verwendung besteht.</p> <p>7.3.2. Die Bank wird den KI über eine Sperre des 3D Secure Verfahrens und deren Gründe möglichst vor, spätestens aber unverzüglich nach der Sperre informieren, soweit die Bekanntgabe der Sperre oder die Gründe für die Sperre nicht eine gerichtliche oder verwaltungsbehördliche Anordnung verletzen bzw. österreichischen oder gemeinschaftsrechtlichen Rechtsnormen oder objektiven Sicherheitsabwägungen zuwiderlaufen würde.</p> <p>7.4. Bekanntgabe und Aufhebung der Sperre</p> <p>7.4.1. Bevor eine Sperre dauerhaft wird, erhält der KI eine Warnung.</p> <p>7.4.2. Die Bank wird eine Sperre gemäß Punkt 7.3. aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen. Die Bank wird den KI über die Aufhebung der Sperre unverzüglich informieren.</p> <p>7.4.3. Der KI kann die Aufhebung einer Sperre telefonisch unter +43 (0)5 99 06-6220 beauftragen.</p>	<p>7. Sperre des 3D Secure Verfahrens</p> <p>7.1. Automatische Sperre Aus Sicherheitsgründen wird nach fünf Mal aufeinanderfolgender falscher Eingabe der persönlichen Identifikationsmerkmale, das 3D Secure Verfahren von der Bank gesperrt. Solange die Sperre aufrecht ist, kann der KI keine Zahlungsanweisungen mit dem 3D Secure Verfahren durchführen.</p> <p>7.2. Sperre durch den KI Der KI kann die Sperre des 3D Secure Verfahrens durch die fünf Mal aufeinanderfolgende falsche Eingabe der persönlichen Identifikationsmerkmale selbst vornehmen oder telefonisch unter +43 (0)5 99 06-6220 veranlassen.</p> <p>7.3. Sperre durch die Bank</p> <p>7.3.1. Die Bank ist berechtigt, das 3D Secure Verfahren für den KI zu sperren, wenn objektive Gründe im Zusammenhang mit der Sicherheit dies rechtfertigen oder der Verdacht einer nicht autorisierten oder betrügerischen Verwendung besteht.</p> <p>7.3.2. Die Bank wird den KI über eine Sperre des 3D Secure Verfahrens und deren Gründe möglichst vor, spätestens aber unverzüglich nach der Sperre informieren, soweit die Bekanntgabe der Sperre oder die Gründe für die Sperre nicht eine gerichtliche oder verwaltungsbehördliche Anordnung verletzen bzw. österreichischen oder gemeinschaftsrechtlichen Rechtsnormen oder objektiven Sicherheitsabwägungen zuwiderlaufen würde.</p> <p>7.4. Bekanntgabe und Aufhebung der Sperre</p> <p>7.4.1. Bevor eine Sperre dauerhaft wird, erhält der KI eine Warnung.</p> <p>7.4.2. Die Bank wird eine Sperre gemäß Punkt 7.3. aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen. Die Bank wird den KI über die Aufhebung der Sperre unverzüglich informieren.</p> <p>7.4.3. Der KI kann die Aufhebung einer Sperre telefonisch unter +43 (0)5 99 06-6220 beauftragen.</p>
<p>8. Änderungen der Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten</p> <p>8.1. 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, sowohl die Vereinbarung zur Teilnahme am 3D</p>	<p>8. Änderungen der Besonderen Geschäftsbedingungen für die Teilnahme am 3D Secure Verfahren für wiederaufladbare PayLife Wertkarten</p> <p>8.1. 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, sowohl die Vereinbarung zur Teilnahme am 3D</p>

<p>Secure als auch den Prepaidkartenvertrag 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.</p> <p>8.2. 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.</p> <p>8.3. Die Änderung dieser Bedingungen ist auf sachlich gerechtfertigte Fälle beschränkt; eine sachliche Rechtfertigung liegt dann vor,</p> <p>(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,</p> <p>(ii) wenn die Änderung durch die Entwicklung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen Judikatur erforderlich ist,</p> <p>(iii) wenn die Änderung die Sicherheit des Bankbetriebs oder die Sicherheit der Abwicklung der Geschäftsverbindung mit dem KI über die Teilnahme am 3D Secure Verfahren fördert,</p> <p>(iv) wenn die Änderung zur Umsetzung technischer Entwicklungen oder zur Anpassung an neue Programme zur Nutzung von Endgeräten erforderlich ist,</p> <p>(v) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für die Erteilung von Aufträgen und für die Abgabe von Erklärungen über die Teilnahme am 3D Secure erforderlich ist,</p> <p>(vi) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für jene Bankgeschäfte, welche der KI über das 3D Secure Verfahren abwickeln kann, erforderlich ist. Die Einführung von Entgelten oder die Änderung vereinbarter Entgelte durch eine Änderung dieser BGB ist ausgeschlossen.</p>	<p>Secure als auch den Prepaidkartenvertrag 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.</p> <p>8.2. 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.</p> <p>8.3. Die Änderung dieser Bedingungen ist auf sachlich gerechtfertigte Fälle beschränkt; eine sachliche Rechtfertigung liegt dann vor,</p> <p>(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,</p> <p>(ii) wenn die Änderung durch die Entwicklung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen Judikatur erforderlich ist,</p> <p>(iii) wenn die Änderung die Sicherheit des Bankbetriebs oder die Sicherheit der Abwicklung der Geschäftsverbindung mit dem KI über die Teilnahme am 3D Secure Verfahren fördert,</p> <p>(iv) wenn die Änderung zur Umsetzung technischer Entwicklungen oder zur Anpassung an neue Programme zur Nutzung von Endgeräten erforderlich ist,</p> <p>(v) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für die Erteilung von Aufträgen und für die Abgabe von Erklärungen über die Teilnahme am 3D Secure erforderlich ist,</p> <p>(vi) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für jene Bankgeschäfte, welche der KI über das 3D Secure Verfahren abwickeln kann, erforderlich ist. Die Einführung von Entgelten oder die Änderung vereinbarter Entgelte durch eine Änderung dieser BGB ist ausgeschlossen.</p>
<p>9. Änderung der E-Mail-Adresse und der Mobiltelefonnummer des KI</p> <p>Der KI verpflichtet sich, jede Änderung seiner 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</p>	<p>9. Änderung der E-Mail-Adresse und der Mobiltelefonnummer des KI</p> <p>Der KI verpflichtet sich, jede Änderung seiner 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</p>
<p>10. Sicherheitshinweise</p> <p>10.1. Solange der Zugang zum 3D Secure Verfahren gesperrt ist, kann die Karte nicht im Internet bei Händlern zur Zahlung verwendet werden, wenn diese das 3D Secure Verfahren anbieten.</p> <p>10.2. Zur Vermeidung von Risiken, die mit der Kenntnis der Identifikationsmerkmale (insbesondere des 3D Secure Passworts) verbunden sind, empfiehlt die Bank, diese regelmäßig (z. B. jeden Monat) zu ändern.</p> <p>10.3. Sollte der KI den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen (insbesondere dem 3D Secure Passwort) erlangt</p>	<p>10. Sicherheitshinweise</p> <p>10.1. Solange der Zugang zum 3D Secure Verfahren gesperrt ist, kann die Karte nicht im Internet bei Händlern zur Zahlung verwendet werden, wenn diese das 3D Secure Verfahren anbieten.</p> <p>10.2. Zur Vermeidung von Risiken, die mit der Kenntnis der Identifikationsmerkmale (insbesondere des 3D Secure Passworts) verbunden sind, empfiehlt die Bank, diese regelmäßig (z. B. jeden Monat) zu ändern.</p> <p>10.3. Sollte der KI den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen (insbesondere dem 3D Secure Passwort) erlangt</p>

<p>haben, so empfiehlt die Bank die Identifikationsmerkmale zu ändern.</p> <p>10.4. Es wird empfohlen, den Zugang zum Gebrauch der mobilen Datenendgeräte zu sichern. Bei Verlust oder Diebstahl des mobilen Datenendgeräts empfiehlt die Bank die Kontaktaufnahme mit dem Mobilfunkanbieter zur Sperre der SIM Karte.</p> <p>10.5. 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.</p> <p>10.6. Die Bank stellt auf der Website www.paylife.at unter dem Menüpunkt „Service“ weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.</p>	<p>haben, so empfiehlt die Bank die Identifikationsmerkmale zu ändern.</p> <p>10.4. Es wird empfohlen, den Zugang zum Gebrauch der mobilen Datenendgeräte zu sichern. Bei Verlust oder Diebstahl des mobilen Datenendgeräts empfiehlt die Bank die Kontaktaufnahme mit dem Mobilfunkanbieter zur Sperre der SIM Karte.</p> <p>10.5. 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.</p> <p>10.6. Die Bank stellt auf der Website www.paylife.at unter dem Menüpunkt „Service“ weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.</p>
<p>11. Vertragsdauer, Kündigung und Beendigung</p> <p>11.1. Die Vereinbarung über die Teilnahme am 3D Secure Verfahren wird auf unbestimmte Zeit geschlossen.</p> <p>11.2. 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.</p> <p>11.3. Die Bank ist berechtigt, die Vereinbarung jederzeit unter Einhaltung einer Frist von zwei Monaten ohne Angabe von Gründen zu kündigen.</p> <p>11.4. Sowohl der KI als auch die Bank sind berechtigt, die Vereinbarung jederzeit bei Vorliegen eines wichtigen Grundes mit sofortiger Wirkung aufzulösen. Die Beendigung der Vereinbarung lässt den Prepaidkartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.</p> <p>11.5. Die Vereinbarung endet automatisch mit dem Ende des Prepaidkartenvertrages.</p>	<p>11. Vertragsdauer, Kündigung und Beendigung</p> <p>11.1. Die Vereinbarung über die Teilnahme am 3D Secure Verfahren wird auf unbestimmte Zeit geschlossen.</p> <p>11.2. 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.</p> <p>11.3. Die Bank ist berechtigt, die Vereinbarung jederzeit unter Einhaltung einer Frist von zwei Monaten ohne Angabe von Gründen zu kündigen.</p> <p>11.4. Sowohl der KI als auch die Bank sind berechtigt, die Vereinbarung jederzeit bei Vorliegen eines wichtigen Grundes mit sofortiger Wirkung aufzulösen. Die Beendigung der Vereinbarung lässt den Prepaidkartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.</p> <p>11.5. Die Vereinbarung endet automatisch mit dem Ende des Prepaidkartenvertrages.</p>