Besondere Bedingungen für die Teilnahme am 3D Secure Verfahren für easybank Kreditkarten

Besondere Bedingungen für die Teilnahme am 3D Secure Verfahren für easybank Kreditkarten (im Folgenden BB 3D Secure) – Fassung Dezember 2019.

Gegenüberstellung Besondere Bedingungen für bargeldlose Zahlungen im Internet mit dem 3D Secure Verfahren – MasterCard SecureCode™/Verified by VISA™ in der zuletzt mit Ihnen vereinbarten Fassung mit der Besondere Bedingungen für die Teilnahme am 3D Secure Verfahren für easybank Kreditkarten in der Fassung Dezember 2019. Die folgenden Klauseln sind geändert; alle übrigen Klauseln sind in beiden Fassungen gleich.

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

BESONDERE BEDINGUNGEN für bargeldlose Zahlungen im Internet mit dem 3D Secure Verfahren - MasterCard SecureCode™/Verified by VISA™ (im Folgenden BB 3D Secure) – Fassung Oktober 2016	**Besondere Bedingungen für ~~bargeldlose Zahlungen im Internet~~ die Teilnahme ~~mit dem~~ am 3D Secure Verfahren – ~~MasterCard SecureCode™/Verified by VISA™~~ für easybank Kreditkarten (im Folgenden BB 3D Secure) – ~~Fassung Oktober 2016~~ Fassung Dezember 2019**
Präambel Diese BB 3D Secure ergänzen die jeweils gültigen Kreditkarten- und Prepaidkartenbedingungen, die dem zwischen dem Karteninhaber (im Folgenden KI) und der easybank AG (im Folgenden easybank) geschlossenen Kreditkarten- bzw. Prepaidkartenvertrag zugrunde liegen, aufgrund dessen der KI berechtigt ist, Leistungen von Vertragsunternehmen (im Folgenden VU) der MasterCard- bzw VISA-Organisation bargeldlos in Anspruch zu nehmen. Das 3D Secure Verfahren (bei Zahlungen mit MasterCard® "MasterCard SecureCode™", bei Zahlungen mit VISA® "Verified by VISA™") ist ein System, das ausnahmslos im Internet für eCommerce-Transaktionen zur Anwendung gelangt und dem Zweck dient, die Daten des KI und seine personalisierten Sicherheitsmerkmale vor der Ausspähung und missbräuchlichen Verwendung durch Dritte zu schützen. Es wird ausnahmslos das Verbindungsprotokoll https (Hyper Text Transfer Protocol Secure) verwendet. Das 3D Secure Verfahren (z.B. MasterCard SecureCode) gilt derzeit als sicheres System iSd Punktes 6.3. der Kreditkarten- und Prepaidkartenbedingungen der easybank. Die Registrierung zum 3D Secure Verfahren ist derzeit z.B. kostenlos auf www.easybank.at/3DSecure möglich. Sofern der Karteninhaber im 3D Secure Verfahren registriert ist, ist ihm die Verwendung dieses sicheren Verfahrens bei Vertragsunternehmen, die ebenfalls das 3D Secure Verfahren anbieten, möglich. Diese BB 3D Secure regeln ausschließlich die Teilnahme des KI am 3D Secure Verfahren. Sie gehen den Kreditkarten- bzw. Prepaidkartenbedingungen, soweit sie den Zahlungsvorgang abweichend regeln, vor.	**Präambel** Diese Besondere Bedingungen für die Teilnahme am 3D Secure Verfahren für easybank Kreditkarten (kurz: BB 3D Secure) regeln die Abwicklung von Zahlungen mit easybank Kreditkarten unter Verwendung des 3D Secure Verfahrens. Die BB 3D Secure gelten, wenn ihre Geltung vereinbart ist. Sie ~~Diese BB 3D Secure~~ ergänzen die Geschäfts-bedingungen für easybank Kreditkarten (im Folgenden kurz Kreditkartenbedingungen) ~~jeweils gültigen Kreditkarten- und Prepaidkartenbedingungen~~, die zu dem zwischen dem Karteninhaber (~~im Folgenden~~ kurz: KI) und der easybank AG (kurz: Bank ~~im Folgenden easybank~~) geschlossenen Kreditkarten~~- bzw. Prepaidkartenvertrag zugrunde liegen~~vertrag vereinbart sind. ~~, aufgrund dessen der KI berechtigt ist, Leistungen von Vertragsunternehmen (im Folgenden VU) der MasterCard- bzw VISA-Organisation bargeldlos in Anspruch zu nehmen.Das 3D Secure Verfahren (bei Zahlungen mit MasterCard® "MasterCard SecureCode™", bei Zahlungen mit VISA® "Verified by VISA™") ist ein System, das ausnahmslos im Internet für eCommerce-Transaktionen zur Anwendung gelangt und dem Zweck dient, die Daten des KI und seine personalisierten Sicherheitsmerkmale vor der Ausspähung und missbräuchlichen Verwendung durch Dritte zu schützen. Es wird ausnahmslos das Verbindungsprotokoll https (Hyper Text Transfer Protocol Secure) verwendet. Das 3D Secure Verfahren (z.B. MasterCard SecureCode) gilt derzeit als sicheres System iSd Punktes 6.3. der Kredit-karten- und Prepaidkartenbedingungen der easybank. Die Registrierung zum 3D Secure Verfahren ist derzeit z.B. kostenlos auf www.easybank.at/3DSecure möglich. Sofern der Karteninhaber im 3D Secure Verfahren registriert ist, ist ihm die Verwendung dieses sicheren Verfahrens bei Vertragsunternehmen, die ebenfalls das 3D Secure Verfahren anbieten, möglich. Diese BB 3D Secure regeln ausschließlich die Teilnahme des KI am 3D Secure Verfahren. Sie gehen den Kreditkarten- bzw. Prepaidkarten-bedingungen, soweit sie den Zahlungsvorgang abweichend regeln, vor.~~
N/A	**1. Definitionen** 1.1. 3D Secure Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das die Voraussetzungen der starken Kundenauthentifizierung erfüllt.
1. Definitionen 1.1. MasterCard SecureCode bzw. Verified by Visa Passwort – „Passwort" Das Passwort ist das im Zuge der Registrierung zum 3D Verfahren vom KI selbst gewählte Passwort. Dieses wird bei MasterCard als „MasterCard SecureCode" und bei Visa als „Verified by Visa Passwort" bezeichnet.	~~**1. Definitionen**~~ 1.~~1.~~2. Master~~C~~card Identity Check ~~SecureCode~~ bzw. ~~Verified by Visa~~ Visa Secure Passwort – „3D Secure Passwort" Das 3D Secure Passwort ist das im Zuge der Registrierung zum 3D Secure Verfahren vom KI selbst gewählte Passwort. Dieses wird bei Master~~C~~card als „Master~~C~~card ~~SecureCode~~ Identity Check" und bei Visa als „~~Verified by Visa~~ Visa Secure" Passwort" bezeichnet und dient der Erteilung von Zahlungsaufträgen im Internet.

easybank AG 1100 Wien Wiedner Gürtel 11 www.easybank.at Tel.: 05 70 05-500
Handelsgericht Wien FN 150466z BIC: EASYATW1 easy@easybank.at

1.2. „mobileTAN“ Die mobileTAN ist eine einmal gültige Transaktionsnummer, die auf ein vom KI zu diesem Zweck der easybank bekannt gegebenes mobiles Endgerät (z.B. Mobiltelefon, Tablet) übermittelt wird und dient als zusätzliches Sicherheits-merkmal bei Kartenzahlungen mit dem MasterCard SecureCode bzw. Verified by Visa Passwort. Auch bei der Registerierung zum 3D Secure Verfahren ist die Eingabe einer mobileTAN erforderlich.	1.~~2.~~3.„mobileTAN“ ~~Die mobileTAN ist eine einmal gültige Transaktionsnummer, die auf ein vom KI zu diesem Zweck der easybank bekannt gegebenes mobiles Endgerät (z.B. Mobiltelefon, Tablet) übermittelt wird und dient als zusätzliches Sicherheits-merkmal bei Kartenzahlungen mit dem MasterCard SecureCode bzw. Verified by Visa Passwort.~~ Die mobileTAN ist eine einmalig verwendbare Transaktions-nummer, 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 Zahlungs-auftrages im Internet als zusätzliches Sicherheitsmerkmal zum 3D Secure Passwort. Auch bei der Regist~~e~~rierung zum 3D Secure Verfahren ist die Eingabe einer mobileTAN erforderlich.
	1.4. Authentifizierungscode Der Authentifizierungscode ist ein Code, der bei starker Kundenauthentifizierung im Sinne der Delegierten Verordnung (EU) 2018/389 generiert wird und mit dem zu autorisierenden Schritt (z.B. mit dem zu autorisierenden Auftrag oder mit der abzugebenden Willenserklärung des KI) dynamisch verlinkt ist. Bei der mobileTAN handelt es sich um einen solchen Authentifizierungscode.
	1.5. Starke Kundenauthentifizierung Die starke Kundenauthentifizierung ist das in der Delegierten Verordnung (EU) 2018/389 geregelte Verfahren zur starken Kundenauthentifizierung. Die starke Kundenauthentifizierung basiert auf (mindestens) zwei Faktoren der Kategorien Wissen (z.B. Passwort), Besitz (z.B. Smartphone) und Inhärenz (z.B. Fingerabdruck, Gesichtserkennung) und zieht die Generierung eines Authentifizierungscodes nach sich.
[…]	[…]
2.3. Folgende persönliche Identifikationsmerkmale sind vom KI im Zuge der Registrierung zum 3D Secure Verfahren selbst festzulegen: * Passwort (MasterCard SecureCode bzw. Verified by Visa Passwort) * persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt) […]	2.3. Folgende persönliche Identifikationsmerkmale sind vom KI im Zuge der Registrierung zum 3D Secure Verfahren selbst festzulegen: * Passwort (Master~~C~~card ~~SecureCode~~ Identity Check bzw. ~~Verified by~~ Visa Secure Passwort) * persönliche Begrüßung (wird bei jeder Passwortabfrage zu Kontrollzwecken angezeigt) […]
2.4. Nach Abgabe der diesbezüglichen Willenserklärung durch Eingabe der Daten gem. Punkt 3 der BB 3D Secure durch den KI erfolgt die Zulassung zum 3DSecureVerfahren.	~~2.4. Nach Abgabe der diesbezüglichen Willenserklärung durch Eingabe der Daten gem. Punkt 3 der BB 3D Secure durch den KI erfolgt die Zulassung zum 3D Secure Verfahren.~~
3. Vertragsdauer und Beendigung **3.1. Vertragsdauer** Diese Vereinbarung über das 3D Secure Verfahren wird auf unbestimmte Zeit geschlossen. Sie endet spätestens mit dem Ende des zugrunde liegenden Kartenvertrages.	**3. Vertragsdauer, Kündigung und Beendigung** ~~**3.1. Vertragsdauer**~~ 3.1. Diese Vereinbarung über das 3D Secure Verfahren wird auf unbestimmte Zeit geschlossen. Sie endet spätestens mit dem Ende des zugrunde liegenden Kartenvertrages**.**
3.2. Kündigung durch den KI Der KI ist jederzeit berechtigt, das 3D Secure Verfahren ohne Angabe von Gründen unter Einhaltung einer Kündigungsfrist von einem Monat zu kündigen. Bestehende Verpflichtungen werden durch die Kündigung nicht berührt und sind zu erfüllen. Die Möglichkeit einer sofortigen Beendigung des 3D Secure Verfahrens durch den KI aus wichtigem Grund und das Recht zur Kündigung anlässlich einer von der easybank vorgeschlagenen Änderung der Leistung oder der BB 3D Secure (Punkt 6. und 7.) bleiben unberührt.	~~**3.2. Kündigung durch den KI**~~ 3.2. Der KI ist ~~jederzeit~~ berechtigt, ~~das 3D Secure Verfahren~~ die Vereinbarung jederzeit ohne Angabe von Gründen ~~unter Einhaltung einer Kündigungsfrist von einem Monat~~ zu kündigen. Nach Einlangen der Kündigung wird die Bank den Zugriff auf das 3D Secure Verfahren sperren. ~~Bestehende Verpflichtungen werden durch die Kündigung nicht berührt und sind zu erfüllen. Die Möglichkeit einer sofortigen Beendigung des 3D Secure Verfahrens durch den KI aus wichtigem Grund und das Recht zur Kündigung anlässlich einer von der easybank vorgeschlagenen Änderung der Leistung oder der BB 3D Secure (Punkt 6. und 7.) bleiben unberührt.~~
3.3. Kündigung durch die easybank Die easybank ist berechtigt, das 3D Secure Verfahren unter Einhaltung einer Frist von zwei Monaten zu kündigen. Bei Vorliegen eines wichtigen Grundes ist die easybank berechtigt, das 3D Secure Verfahren jederzeit mit sofortiger Wirkung zu kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn der KI seinen Zahlungs-verpflichtungen nicht nachgekommen ist.	~~**3.3. Kündigung durch die easybank**~~ 3.3. Die Bank ist berechtigt, ~~das 3D Secure Verfahren~~ die Vereinbarung jederzeit unter Einhaltung einer Frist von zwei Monaten ohne Angabe von Gründen zu kündigen. ~~Bei Vorliegen eines wichtigen Grundes ist die easybank berechtigt, das 3D Secure Verfahren jederzeit mit sofortiger Wirkung zu kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn der KI seinen Zahlungs-verpflichtungen nicht nachgekommen ist.~~
	3.4. Sowohl der KI als auch die Bank sind berechtigt, die Vereinbarung jederzeit bei Vorliegen eines wichtigen Grundes mit sofortiger Wirkung aufzulösen.
	3.5. Die Beendigung der Vereinbarung lässt den Kredit-kartenvertrag unberührt, falls der KI bzw. die Bank nicht gleichzeitig auch dessen Beendigung erklären.

easybank AG 1100 Wien Wiedner Gürtel 11 www.easybank.at Tel.: 05 70 05-500
Handelsgericht Wien FN 150466z BIC: EASYATW1 easy@easybank.at

	3.6. Die Vereinbarung endet automatisch mit dem Ende des Kreditkartenvertrages.
4. Abgabe von Willenserklärungen und Anweisung von Zahlungen Im 3D Secure Verfahren erfolgt die Abgabe von Willenserklärungen sowie Anweisung einer Zahlung gemäß Punkt 6.1. der Kreditkarten- bzw. Prepaidkartenbedingungen der easybank durch die Eingabe der 16-stelligen Kartennummer, des Ablaufdatums der Karte, des rückseitigen dreistelligen CVC- bzw. CVV-Codes, die Eingabe eines nur dem KI bekannten selbstgewählten Passwortes sowie eine dem KI auf sein mobiles Endgerät zugesendete mobileTAN.	**4. ~~Abgabe von Willenserklärungen und Anweisung von Zahlungen~~ Zahlen mit 3D Secure** ~~Im 3D Secure Verfahren erfolgt die Abgabe von Willenserklärungen sowie Anweisung einer Zahlung gemäß Punkt 6.1. der Kreditkarten- bzw. Prepaidkarten-bedingungen der easybank durch die Eingabe der 16-stelligen Kartennummer, des Ablaufdatums der Karte, des rückseitigen dreistelligen CVC- bzw. CVV-Codes, die Eingabe eines nur dem KI bekannten selbstgewählten Passwortes sowie eine dem KI auf sein mobiles Endgerät zugesendete mobileTAN.~~ Zahlungstransaktionen im Internet führt der KI mit seinem selbst festgelegten 3D Secure Passwort und einer mobileTAN durch.
5. Sperre des Zugangs zum 3D Secure Verfahren 5.1. Die easybank ist berechtigt, den Zugang des KI zum 3D Secure Verfahren zu sperren, wenn - objektive Gründe im Zusammenhang mit der Sicherheit der Karte oder des 3D Secure Verfahrens dies rechtfertigen; oder - der Verdacht einer nicht autorisierten oder betrügerischen Verwendung des 3D Secure Verfahrens besteht; oder - wenn der KI seinen Zahlungspflichten gegenüber der easybank im Zusammenhang mit der Verwendung der Karte im 3D Secure Verfahren nicht nachgekommen ist und - entweder die Erfüllung dieser Zahlungspflichten aufgrund einer Verschlechterung oder Gefährdung der Vermögens-verhältnisse des KI oder eines Mitverpflichteten gefährdet ist oder - beim KI die Zahlungsunfähigkeit eingetreten ist oder diese unmittelbar droht.	**5. Sperre des Zugangs zum 3D Secure Verfahren** ~~5.1. Die easybank ist berechtigt, den Zugang des KI zum 3D Secure Verfahren zu sperren, wenn~~ ~~- objektive Gründe im Zusammenhang mit der Sicherheit der Karte oder des 3D Secure Verfahrens dies rechtfertigen; oder~~ ~~- der Verdacht einer nicht autorisierten oder betrügerischen Verwendung des 3D Secure Verfahrens besteht; oder~~ ~~- wenn der KI seinen Zahlungspflichten gegenüber der easybank im Zusammenhang mit der Verwendung der Karte im 3D Secure Verfahren nicht nachgekommen ist und~~ ~~- entweder die Erfüllung dieser Zahlungspflichten aufgrund einer Verschlechterung oder Gefährdung der Vermögens-verhältnisse des KI oder eines Mitverpflichteten gefährdet ist oder~~ ~~- beim KI die Zahlungsunfähigkeit eingetreten ist oder diese unmittelbar droht.~~ 5.1. Automatische Sperre Aus Sicherheitsgründen wird nach fünf Mal aufeinander-folgender falscher Eingabe des 3D Secure Passworts das 3D Secure Verfahren von der Bank gesperrt. Solange die Sperre aufrecht ist, kann der KI keine Zahlungsanweisungen mit dem 3D Secure Verfahren durchführen.
5.2. Der KI kann die easybank auffordern, seinen Zugang zum 3D Secure Verfahren zu sperren. Die easybank wird den Zugang zum 3D Secure Verfahren unverzüglich nach Eingang einer solchen Aufforderung sperren.	5.2. Sperre durch den KI ~~Der KI kann die easybank auffordern, seinen Zugang zum 3D Secure Verfahren zu sperren. Die easybank wird den Zugang zum 3D Secure Verfahren unverzüglich nach Eingang einer solchen Aufforderung sperren.~~ Der KI kann die Sperre des 3D Secure Verfahrens durch die fünf Mal aufeinanderfolgende falsche Eingabe des 3D Secure Passworts selbst vornehmen oder telefonisch unter +43 (0)5 70 05-514 veranlassen.
5.3. Sollte der KI wissen, oder den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen erlangt haben, empfiehlt die easybank, die Identifikationsmerkmale zu ändern oder die Sperre des Zugangs zum 3D Secure Verfahren unverzüglich zu beauftragen.	5.3. Sperre durch die Bank ~~Sollte der KI wissen, oder den Verdacht haben, dass Dritte Kenntnis von seinen Identifikationsmerkmalen erlangt haben, empfiehlt die easybank, die Identifikationsmerkmale zu ändern oder die Sperre des Zugangs zum 3D Secure Verfahren unverzüglich zu beauftragen.~~ 5.3.1. 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.
	5.3.2. 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 Sicherheitserwägungen zuwiderlaufen würde.
5.4. Ist eine Sperre erfolgt, ist der KI nicht berechtigt, die Karte im Internet für Zahlungen bei VU, die das 3D Secure Verfahren anbieten, zu verwenden.	5.4. Bekanntgabe und Aufhebung der Sperre ~~Ist eine Sperre erfolgt, ist der KI nicht berechtigt, die Karte im Internet für Zahlungen bei VU, die das 3D Secure Verfahren anbieten, zu verwenden.~~ 5.4.1. Bevor eine Sperre dauerhaft wird, erhält der KI eine Warnung.
	5.4.2. Die Bank wird eine Sperre gemäß Punkt 5.3. aufheben, sobald die Gründe für die Sperre nicht mehr vorliegen. Die

easybank AG 1100 Wien Wiedner Gürtel 11 www.easybank.at Tel.: 05 70 05-500
Handelsgericht Wien FN 150466z BIC: EASYATW1 easy@easybank.at

	Bank wird den KI über die Aufhebung der Sperre unverzüglich informieren.
	5.4.3 Der KI kann die Aufhebung einer Sperre telefonisch unter +43 (0)5 70 05-514 beauftragen.
5.5. Will der KI nach einer erfolgten Sperre wieder am 3D Secure Verfahren teilnehmen, muss er sich erneut registrieren.	~~5.5. Will der KI nach einer erfolgten Sperre wieder am 3D Secure Verfahren teilnehmen, muss er sich erneut registrieren.~~
6. Sorgfaltspflichten und empfohlene Sicherheits-maßnahmen **6.1. Sorgfaltspflichten** Der KI ist verpflichtet sein 3D Secure Passwort geheim zu halten. Kommt dem KI das 3D Secure Passwort aus welchem Grund auch immer abhanden oder treten Umstände ein, die Kenntnis eines Dritten vom 3D Secure Passwort vermuten lassen, ist der KI verpflichtet, unverzüglich die Sperre seiner Registrierung oder seiner Karte zu veranlassen oder sein 3D Secure Passwort selbständig zu ändern und zu kontrollieren, ob es bereits zu missbräuchlicher Verwendung seiner Daten gekommen ist.	**6. Sorgfaltspflichten~~, und~~ empfohlene Sicherheits-maßnahmen und Haftung** ~~**6.1. Sorgfaltspflichten**~~ ~~Der KI ist verpflichtet sein 3D Secure Passwort geheim zu halten. Kommt dem KI das 3D Secure Passwort aus welchem Grund auch immer abhanden oder treten Umstände ein, die Kenntnis eines Dritten vom 3D Secure Passwort vermuten lassen, ist der KI verpflichtet, unverzüglich die Sperre seiner Registrierung oder seiner Karte zu veranlassen oder sein 3D Secure Passwort selbständig zu ändern und zu kontrollieren, ob es bereits zu missbräuchlicher Verwendung seiner Daten gekommen ist.~~ 6.1. Einhaltung und Rechtsfolgen Jeder KI ist zur Einhaltung der in den Punkten 6.2. bis 6.4. enthaltenen Sorgfaltspflichten verpflichtet. KI, die Unternehmer sind, sind zusätzlich zur Einhaltung der in Punkt 6.5 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 6.6 zu Schadenersatzpflichten des KI oder zum Entfall bzw. zur Minderung seiner Schadenersatzansprüche gegenüber der Bank führen.
6.2. Empfohlene Sicherheitsmaßnahmen Die easybank empfiehlt dem KI, die von ihm im Zuge des Zahlvorganges verwendeten Internetseiten so zu schließen, dass es einem unberechtigten Dritten nicht möglich ist, auf diese zugreifen zu können. Die easybank empfiehlt dem KI, darauf zu achten, das 3D Secure Passwort nur dann einzugeben, wenn bei der Eingabe die lokale, räumliche, technische und persönliche Umgebung so beschaffen ist, dass kein Dritter in der Lage ist, Kartennummer, 3D Secure Passwort oder andere transaktionsrelevanten Daten auszuspähen. Die easybank empfiehlt dem KI, sein 3D Secure Passwort in elektronischen Medien nur dann zu speichern, wenn sie durch geeignete Vorkehrungen (z.B. durch ein Passwort) vor einem unberechtigten Zugriff Dritter geschützt sind.	6.2. ~~Empfohlene Sicherheitsmaßnahmen~~ Geheimhaltungs- und Sperrverpflichtung ~~Die easybank empfiehlt dem KI, die von ihm im Zuge des Zahlvorganges verwendeten Internetseiten so zu schließen, dass es einem unberechtigten Dritten nicht möglich ist, auf diese zugreifen zu können. Die easybank empfiehlt dem KI, darauf zu achten, das 3D Secure Passwort nur dann einzugeben, wenn bei der Eingabe die lokale, räumliche, technische und persönliche Umgebung so beschaffen ist, dass kein Dritter in der Lage ist, Kartennummer, 3D Secure Passwort oder andere transaktionsrelevanten Daten auszuspähen. Die easybank empfiehlt dem KI, sein 3D Secure Passwort in elektronischen Medien nur dann zu speichern, wenn sie durch geeignete Vorkehrungen (z.B. durch ein Passwort) vor einem unberechtigten Zugriff Dritter geschützt sind.~~ 6.2.1 Der KI hat sein 3D Secure Passwort geheim zu halten und darf dieses nicht an unbefugte Dritte weitergeben; Die Weitergabe des 3D Secure Passworts an Zahlungsauslöse-dienstleister und Kontoinformationsdienstleister ist jedoch zulässig, soweit sie erforderlich ist, damit diese ihre Dienst-leistungen für den KI erbringen können.
	6.2.2. Der KI ist verpflichtet, größte Sorgfalt bei der Aufbe-wahrung und Verwendung seines 3D Secure Passworts walten zu lassen, um einen Missbrauch zu vermeiden. Der KI hat insbesondere darauf zu achten, dass sein 3D Secure Passwort bei deren Verwendung nicht ausgespäht wird.
	6.2.3. Bei Verlust des 3D Secure Passworts 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.
	6.3. Sorgfaltspflichten zur Sperre des Endgeräts Der KI ist verpflichtet, den Zugang zum Gebrauch des mobilen Endgerätes bzw. den Zugriff auf dort gespeicherte Daten für Nichtberechtigte zu sperren, wenn er das End-gerät nicht benutzt.
	6.4. Sorgfaltspflichten bei Aufträgen 6.4.1.Zahlungsfreigabe mit mobileTAN Die in der mobileTAN angezeigten Daten sind vom KI vor der Verwendung auf ihre Richtigkeit hin zu überprüfen. Nur bei Übereinstimmung der angezeigten Daten mit dem gewünschten Zahlungsauftrag darf die mobileTAN zur Erteilung von Aufträgen verwendet werden.

easybank AG 1100 Wien Wiedner Gürtel 11 www.easybank.at Tel.: 05 70 05-500
Handelsgericht Wien FN 150466z BIC: EASYATW1 easy@easybank.at

	6.5. Empfohlene Sicherheitsmaßnahmen bei der Verwendung des 3D Secure Zahlungsverfahrens 6.5.1. Dem KI wird empfohlen, das 3D Secure Passwort regelmäßig, spätestens alle zwei Monate, selbstständig zu ändern.
	6.5.2. Dem KI wird empfohlen, unverzüglich die Sperre des 3D Secure Verfahrens zu veranlassen, wenn Anlass zur Befürchtung besteht, dass unbefugte Dritte Kenntnis vom Passwort erlangt haben, oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen könnten.
	6.5.3. Dem KI wird empfohlen, sein mobiles Endgerät, auf welchem er die mobileTAN bekommt, 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.
	6.6. Haftung des KI 6.6.1. Der KI haftet für den gesamten Schaden einer nicht autorisierten Onlinezahlung, welche er der Bank durch die vorsätzliche oder grob fahrlässige Verletzung der Sorgfalts-pflichten gemäß den Punkten 6.2. bis 6.4. zugefügt hat. Hat der KI die Sorgfaltspflichten gemäß den Punkten 6.2. bis 6.4. weder in betrügerischer Absicht noch vorsätzlich verletzt, sind bei einer allfälligen Schadensteilung zwischen dem KI und der Bank insbesondere die Art der personalisierten Sicherheitsmerkmale sowie die besonderen Umstände, unter denen die missbräuchliche Verwendung der Karte stattgefunden hat, zu berücksichtigen.
	6.6.2. War für den KI vor der Zahlung der Verlust oder Diebstahl seines 3D Secure Passworts oder die missbräuchliche Verwendung seiner Karte nicht bemerkbar, haftet er abweichend von Punkt 6.6.1. bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß den Punkten 6.2. bis 6.4. nicht. Der KI haftet bei leicht fahrlässiger Verletzung der Sorgfaltspflichten gemäß den Punkten 6.2. bis 6.4. auch dann nicht, wenn die Bank den Verlust des 3D Secure Passworts verursacht hat.
	6.6.3. Abweichend von Punkt 6.6.1. 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.
	6.6.4. Der KI haftet nicht, wenn der Schaden aus einer nicht autorisierten Nutzung der Karte bei einer Onlinezahlung nach Beauftragung der Sperre gemäß Punkt 5. entstanden ist, es sei denn, der KI hat in betrügerischer Absicht gehandelt.
7. Änderungen der vereinbarten Leistungen 7.1. Änderungen der von der easybank dem KI zu erbringenden Dauerleistungen werden dem KI von der easybank spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens angeboten. Die Zustimmung des KI zu diesen Änderungen gilt als erteilt, wenn bei der easybank vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens kein schriftlicher Widerspruch des KI einlangt. Darauf wird die easybank den KI im Änderungsangebot hinweisen. Der Kunde hat das Recht, diese Vereinbarung über die Teilnahme am 3D Secure Verfahren bis zum Inkrafttreten der Änderung kostenlos fristlos zu kündigen. Auch darauf wird die easybank im Änderungsangebot hinweisen. Das Änderungsangebot ist dem KI von der easybank mitzuteilen. Die Mitteilung an den KI kann schriftlich (insbesondere durch Benachrichtigung auf einer Kreditkartenabrechnung bzw. eines Kontoauszuges), durch Einstellen einer elektronischen Nachricht in das elektronische Postfach oder über die elektronische Kreditkartenabrechnung bzw. den elektronischen Kontoauszug erfolgen.	**7. Änderungen ~~der vereinbarten Leistungen~~ der Besondere Bedingungen für die Teilnahme am 3D Secure Verfahren für easybank Kreditkarten** 7.1. ~~Änderungen der von der easybank dem KI zu erbringenden Dauerleistungen werden dem KI von der easybank spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens angeboten. Die Zustimmung des KI zu diesen Änderungen gilt als erteilt, wenn bei der easybank vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens kein schriftlicher Widerspruch des KI einlangt. Darauf wird die easybank den KI im Änderungsangebot hinweisen. Der Kunde hat das Recht, diese Vereinbarung über die Teilnahme am 3D Secure Verfahren bis zum Inkrafttreten der Änderung kostenlos fristlos zu kündigen. Auch darauf wird die easybank im Änderungsangebot hinweisen. Das Änderungsangebot ist dem KI von der easybank mitzuteilen. Die Mitteilung an den KI kann schriftlich (insbesondere durch Benachrichtigung auf einer Kreditkartenabrechnung bzw. eines Kontoauszuges), durch Einstellen einer elektronischen Nachricht in das elektronische Postfach oder~~

easybank AG 1100 Wien Wiedner Gürtel 11 www.easybank.at Tel.: 05 70 05-500
Handelsgericht Wien FN 150466z BIC: EASYATW1 easy@easybank.at

	~~über die elektronische Kreditkartenabrechnung bzw. den elektronischen Kontoauszug erfolgen.~~ Änderungen der BB 3D Secure 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 e-Postfach im easybank electronic banking) 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 Secure Verfahren 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.
7.2. Auf dem in Punkt 7.1. vereinbarten Weg dürfen nur Leistungsänderungen vorgenommen werden, die unter Berücksichtigung aller Umstände sachlich gerechtfertigt sind. Als sachlich gerechtfertigt gelten Leistungsänderungen aufgrund der Änderung der vorherrschenden Kundenbedürfnisse, gesetzlicher und aufsichtsbehördlicher Anforderungen, der Sicherheit des Bankbetriebs oder der technischen Entwicklung.	7.2. ~~Auf dem in Punkt 7.1. vereinbarten Weg dürfen nur Leistungsänderungen vorgenommen werden, die unter Berücksichtigung aller Umstände sachlich gerechtfertigt sind. Als sachlich gerechtfertigt gelten Leistungsänderungen aufgrund der Änderung der vorherrschenden Kundenbedürfnisse, gesetzlicher und aufsichtsbehördlicher Anforderungen, der Sicherheit des Bankbetriebs oder der technischen Entwicklung.~~ 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 in das e-Postfach im easybank electronic banking, wobei der KI über das Vorhandensein des Änderungsangebots in seinem e-Postfach auf die mit ihm vereinbarte Weise (Push-Nachricht, SMS, E-Mail, Post oder sonst vereinbarte Form) informiert werden wird.
	7.3. Die Änderung dieser Bedingungen ist auf sachlich gerechtfertigte Fälle beschränkt; eine sachliche Rechtfertigung liegt dann vor, (i) wenn die Änderung durch eine Änderung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen gesetzlichen Bestimmungen oder durch Vorgaben der Finanzmarktaufsicht, der Europäischen Bankenaufsichtsbehörde, der Europäischen Zentralbank oder der Österreichischen Nationalbank erforderlich ist, (ii) wenn die Änderung durch die Entwicklung der für Zahlungsdienste sowie ihre Abwicklung maßgeblichen Judikatur erforderlich ist, (iii) wenn die Änderung die Sicherheit des Bankbetriebs oder die Sicherheit der Abwicklung der Geschäftsverbindung mit dem KI über die Teilnahme am 3D Secure Verfahren fördert, (iv) wenn die Änderung zur Umsetzung technischer Entwicklungen oder zur Anpassung an neue Programme zur Nutzung von Endgeräten erforderlich ist, (v) wenn die Änderung durch eine Änderung der gesetzlichen Bestimmungen für die Erteilung von Aufträgen und für die Abgabe von Erklärungen über die Teilnahme am 3D Secure erforderlich ist, (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

easybank AG 1100 Wien Wiedner Gürtel 11 www.easybank.at Tel.: 05 70 05-500
Handelsgericht Wien FN 150466z BIC: EASYATW1 easy@easybank.at

	vereinbarter Entgelte durch eine Änderung dieser BB 3D Secure ist ausgeschlossen.
8. Änderungen der BB 3D Secure 8.1. Änderungen dieser BB 3D Secure gelten nach Ablauf von zwei Monaten ab Zugang der Mitteilung der angebotenen Änderungen an den KI als vereinbart, sofern bis dahin kein Widerspruch des KI bei der easybank einlangt. Die easybank wird den KI in der Mitteilung auf die Änderungen hinweisen und darauf aufmerksam machen, dass sein Stillschweigen nach Ablauf der zwei Monate ab Zugang der Mitteilung als Zustimmung zur Änderung gilt. Außerdem wird die easybank eine Gegenüberstellung über die von der Änderung der BB 3D Secure betroffenen Bestimmungen sowie die vollständige Fassung der neuen BB 3D Secure auf ihrer Internetseite veröffentlichen und die Gegenüberstellung dem KI auf sein Verlangen zur Verfügung stellen. Darauf wird die easybank in der Mitteilung hinweisen.	**8. ~~Änderungen der BB 3D Secure~~ Änderung der Mobiltelefonnummer des KI** ~~8.1. Änderungen dieser BB 3D Secure gelten nach Ablauf von zwei Monaten ab Zugang der Mitteilung der angebotenen Änderungen an den KI als vereinbart, sofern bis dahin kein Widerspruch des KI bei der easybank einlangt. Die easybank wird den KI in der Mitteilung auf die Änderungen hinweisen und darauf aufmerksam machen, dass sein Stillschweigen nach Ablauf der zwei Monate ab Zugang der Mitteilung als Zustimmung zur Änderung gilt. Außerdem wird die easybank eine Gegenüberstellung über die von der Änderung der BB 3D Secure betroffenen Bestimmungen sowie die vollständige Fassung der neuen BB 3D Secure auf ihrer Internetseite veröffentlichen und die Gegenüberstellung dem KI auf sein Verlangen zur Verfügung stellen. Darauf wird die easybank in der Mitteilung hinweisen.~~ Der KI verpflichtet sich, jede Änderung seiner Mobiltelefonnummer der Bank schriftlich oder per E-Mail bekannt zu geben. Die Bestimmung des Punktes 17. der Geschäftsbedingungen für easybank Kreditkarten bleibt hiervon unberührt.
8.2. Im Falle einer solchen beabsichtigten Änderung der BB 3D Secure hat der KI, das Recht, seinen Vertrag über die Teilnahme am 3D Secure Verfahren vor dem Inkrafttreten der Änderung kostenlos fristlos zu kündigen.	~~8.2. Im Falle einer solchen beabsichtigten Änderung der BB 3D Secure hat der KI, das Recht, seinen Vertrag über die Teilnahme am 3D Secure Verfahren vor dem Inkrafttreten der Änderung kostenlos fristlos zu kündigen.~~
	9. Sicherheitshinweise 9.1. 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.
	9.2. Zur Vermeidung von Risiken, die mit der Kenntnis des 3D Secure Passworts verbunden sind, empfiehlt die Bank, dieses regelmäßig (z. B. jeden Monat) zu ändern.
	9.3. Sollte der KI den Verdacht haben, dass Dritte Kenntnis von seinem 3D Secure Passwort erlangt haben, so empfiehlt die Bank dieses zu ändern.
	9.4. 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.
	9.5. Zu beachten ist, dass die Verwendung von Passwörtern an gemeinsam benutzten Computern und mobilen Datenendgeräten (z. B. in einem Internetcafé, in einem Hotel, am Arbeitsplatz) unbefugten Dritten die Ausspähung von Passwörtern möglich macht.
	9.6. Die Bank stellt auf der Website www.easybank.at/3DSecure weitere Informationen zu den sicheren Systemen und Sicherheitstipps zur Verfügung.

easybank AG 1100 Wien Wiedner Gürtel 11 www.easybank.at Tel.: 05 70 05-500
Handelsgericht Wien FN 150466z BIC: EASYATW1 easy@easybank.at