

## Sonderbedingungen für die Teilnahme am 3D Secure Verfahren

### Präambel

Diese „Sonderbedingungen für die Teilnahme am 3D Secure Verfahren“ (kurz Sonderbedingungen) ergänzen die „Bedingungen der Oberbank Mastercard“ für die von der Oberbank AG (kurz Kreditinstitut) herausgegebene Oberbank Mastercard (kurz Karte), die dem zwischen dem Kreditinstitut und dem Konto-/Karteninhaber geschlossenen Kreditkartenvertrag zugrunde liegen.

Das PayLife Service Center der easybank AG (kurz PayLife Service Center), die mit der technischen bzw. operativen Abwicklung der Zahlungsverkehrsvorgänge beauftragt ist, bietet im Internet das 3D Secure Verfahren an.

Diese Sonderbedingungen regeln die Registrierung und die Abwicklung des Zahlungsverkehrs in sicheren Systemen.

### 1. Allgemeine Bestimmungen

#### 1.1. Mastercard Kartennummer

Diese 16-stellige Nummer befindet sich auf der Vorderseite der Karte.

#### 1.2. CVC-Daten (Card Verification Code)

Auf der Rückseite der Karte befindet sich im Unterschriftsfeld ein Code. Die letzten 3 Ziffern dieses Codes bilden die CVC-Daten.

#### 1.3. Einmalpasswort

Das Einmalpasswort (kurz EPW) ist ein zufällig vergebenes Passwort (8-stelliger Code), das der Karteninhaber pro Karte erhält. Dieses EPW dient zur Verifizierung des Karteninhabers während der Registrierung zum 3D Secure Verfahren. Im Zuge des 3D Secure Registrierungsprozesses wird das EPW durch die Eingabe eines selbst gewählten, ausschließlich dem Karteninhaber bekannten 3D Secure Passwort (Mastercard Identity Check), ersetzt.

#### 1.4. Starke Kundenauthentifizierung

Die starke Kundenauthentifizierung ist das in der Delegierten Verordnung (EU) 2018/389 geregelte Verfahren zur starken Kundenauthentifizierung. Die starke Kundenauthentifizierung basiert auf (mindestens) zwei Faktoren der Kategorien Wissen (z.B. Passwort), Besitz (z.B. Smartphone) und Inhärenz (z.B. Fingerabdruck, Gesichtserkennung) und zieht die Generierung eines Authentifizierungscodes nach sich.

#### 1.5. 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 Karteninhabers) dynamisch verlinkt ist. Bei der mobileTAN handelt es sich um einen solchen Authentifizierungscode.

#### 1.6. Sichere Systeme

##### 1.6.1. 3D Secure Verfahren

Das 3D Secure Verfahren ist ein für Online Zahlungen eingesetztes sicheres System, das die Voraussetzungen der starken Kundenauthentifizierung erfüllt.

##### 1.6.2. 3D Secure Passwort (Mastercard Identity Check)

Das 3D Secure Passwort ist das vom Karteninhaber 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.

##### 1.6.3. Mobile Transaktionsnummer (kurz mobileTAN)

Die mobileTAN ist eine einmalig verwendbare Transaktionsnummer, die an die vom Karteninhaber für die Zwecke 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. Registrierung zum 3D Secure Verfahren**

### **2.1. Voraussetzung**

Voraussetzung für die Teilnahme am 3D Secure Verfahren ist der vorherige Abschluss eines Kreditkartenvertrages zwischen dem Kontoinhaber und dem Karteninhaber und dem Kreditinstitut, sowie einer Vereinbarung über das Internetbanking (Portalvertrag).

Die Nutzung des 3D Secure Verfahrens setzt die Registrierung des Karteninhabers für 3D Secure Verfahren voraus.

### **2.2. Registrierung**

Die Registrierung kann auf der Website [www.oberbank.at](http://www.oberbank.at) gestartet werden. Auf der Website [www.oberbank.at](http://www.oberbank.at) wird dem Karteninhaber der Ablauf der Registrierung erklärt. Für die Identifizierung des Karteninhabers sind ein gültiges EPW sowie eine mobileTAN erforderlich. Im Zuge der Registrierung zum 3D Secure Verfahren wird dem Karteninhaber eine mobileTAN per SMS an die von ihm für die Zusendung einer mobileTAN bekannt gegebenen Mobiltelefonnummer, geschickt.

Das EPW für neue Karten wird als Umsatz zu seiner Karte im Internetbanking (Oberbank Kundenportal) angezeigt.

Im Zuge der Registrierung zu 3D Secure Verfahren werden dem Karteninhaber diese Sonderbedingungen zur Verfügung gestellt. Für den weiteren Registrierungsvorgang ist es notwendig, dass der Karteninhaber diese Sonderbedingungen an der vorgesehenen Stelle akzeptiert, womit eine Vereinbarung über die Teilnahme am 3D Secure Verfahren zustande kommt.

Der Karteninhaber kann seine persönlichen Identifikationsmerkmale jederzeit selbst ändern. Hat der Karteninhaber sein von ihm gewähltes Passwort vergessen, so hat er die Möglichkeit ein neues 3D Secure Passwort über die Registrierungswebsite zu setzen.

Für die Nutzung des 3D Secure Verfahrens ist die Bekanntgabe der Mobiltelefonnummer des Karteninhabers erforderlich. Die technische Einrichtung zum korrekten Empfang der SMS fällt in den Verantwortungsbereich des Karteninhabers. Allfällige aus dem SMS-Empfang entstehende Kosten hat der Karteninhaber selbst zu tragen. Im Übrigen ist die Nutzung des Verfahrens kostenfrei.

## **3. Zahlen mit 3D Secure**

**3.1.** Mit dem vom Karteninhaber selbst gewählten 3D Secure Passwort (Mastercard Identity Check) und der für diesen Zahlungsvorgang generierten mobileTAN kann der Karteninhaber Zahlungstransaktionen in sicheren Systemen durchführen. Die per SMS übermittelten Daten sind vom Karteninhaber vor Verwendung der mobileTAN auf ihre Richtigkeit zu prüfen. Nur bei Übereinstimmung der per SMS übermittelten Daten mit dem gewünschten Auftrag, darf die mobileTAN zur Auftragsbestätigung verwendet werden. Weichen die Daten in der SMS vom beabsichtigten Auftrag ab, hat der Karteninhaber dies PayLife Service Center unverzüglich unter der Telefonnummer +43(0)59906-6220 bekannt zu geben und den Zahlungsvorgang abubrechen. Beendet der Karteninhaber dennoch den Zahlungsvorgang, kann dies ein Mitverschulden für allfällige Schäden begründen.

**3.2.** Mit der Eingabe der Bestätigung des selbst gewählten 3D Secure Passwortes (Mastercard Identity Check) und der für diesen Zahlungsvorgang generierten mobileTAN wird die Zahlungsanweisung unwiderruflich erteilt. Dadurch weist der Karteninhaber das Kreditinstitut unwiderruflich an, den vom Vertragsunternehmen in Rechnung gestellten Betrag an das Vertragsunternehmen zu bezahlen und dem im Kartenantrag angegebenen Konto anzulasten.

Das Kreditinstitut nimmt bereits jetzt die Anweisung an. Der Karteninhaber verpflichtet sich, dem Kreditinstitut den angewiesenen Betrag zu ersetzen, ohne Einwendungen aus dem Grundgeschäft (mit dem Vertragsunternehmen) zu erheben.

## **4. Sperre der Karte / Sperre des 3D Secure Verfahrens**

**4.1.** Die Sperre einer Karte kann vom Kontoinhaber oder vom betreffenden Karteninhaber wie folgt beauftragt werden:

- jederzeit (auch außerhalb der Banköffnungszeiten) über eine für diese Zwecke von PayLife Service Center eingerichtete Sperr-Hotline, deren Telefonnummer das Kreditinstitut dem Karteninhaber bekannt gegeben hat. Diese Telefonnummer ist auch auf der Internetseite [www.paylife.at](http://www.paylife.at) abrufbar und kann auch bei jedem Kreditinstitut erfragt werden oder

- zu den jeweiligen Öffnungszeiten des Kreditinstituts persönlich, schriftlich oder telefonisch beim Kreditinstitut.

Eine beauftragte Sperre wird unmittelbar mit Einlangen des Sperrauftrags wirksam. Bei Kreditkarten ist die 16-stellige Kreditkartennummer anzugeben.

**4.2.** Das Kreditinstitut ist berechtigt, die Karte ohne Mitwirkung des Kontoinhabers oder des Karteninhabers zu sperren, wenn

- objektive Gründe im Zusammenhang mit der Sicherheit der Karte, der Kartendaten oder der Systeme, die mit ihr in Anspruch genommen werden können, dies rechtfertigen;
- der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Karte oder Kartendaten besteht; oder
- wenn der Kontoinhaber seinen gegenüber dem Kreditinstitut aus der Verwendung der Karte oder Kartendaten entstehenden nicht nachgekommen ist, und
  - entweder die Erfüllung dieser Zahlungspflichten aufgrund einer Verschlechterung oder Gefährdung der Vermögensverhältnisse des Karteninhabers oder eines Mitverpflichteten gefährdet ist, oder
  - beim Karteninhabers die Zahlungsunfähigkeit eingetreten ist oder diese unmittelbar droht.

Das Kreditinstitut wird den Karteninhabers - soweit eine Bekanntgabe der Sperre oder der Gründe für die Sperre nicht eine gerichtliche oder verwaltungsbehördliche Anordnung verletzen bzw. österreichischen oder unionsrechtlichen Rechtsnormen oder objektiven Sicherheitserwägungen zuwiderlaufen würde - von einer solchen Sperre und deren Gründen, in der mit dem Kunden vereinbarten Form möglichst vor, spätestens aber unverzüglich nach der Sperre informieren.

Sobald die Gründe für die Sperre nicht mehr vorliegen, hat das Kreditinstitut die Sperre des Zahlungsinstruments aufzuheben oder dieses durch ein neues Zahlungsinstrument zu ersetzen.

**4.3.** Nach fünfmaliger Eingabe eines unrichtigen Passwortes wird aus Sicherheitsgründen der Zugang zum 3D Secure Verfahren gesperrt. Solange der Zugang zum 3D Secure Verfahren gesperrt ist, kann der Karteninhaber keine Zahlungstransaktionen mit dem 3D Secure Verfahren durchführen.

Der Karteninhaber ist in diesem Fall berechtigt, die Aufhebung der Sperre telefonisch bei PayLife Service Center unter der Telefonnummer +43(0)59906-6220 zu veranlassen.

**4.4.** Bei Verlust sowie bei missbräuchlicher Verwendung des 3D Secure Passwortes und/oder der mobileTAN hat der Karteninhaber, sobald er davon Kenntnis erlangt, bei der kontoführenden Stelle oder jederzeit über die Sperr-Hotline von PayLife Service Center eine Sperre des Zugangs zum 3D Secure Verfahren bzw. eine Sperre der Karte unverzüglich zu veranlassen.

Eine Sperre der Karte hat eine Sperre der Teilnahme am 3D Secure Verfahren zur Folge. Eine beauftragte Sperre wird unmittelbar mit Einlangen des Sperrauftrags wirksam. Dem Karteninhaber wird darüber hinaus empfohlen, eine Anzeige bei der dafür zuständigen Behörde zu erstatten.

## **5. Pflichten des Karteninhabers**

Der Karteninhaber hat sein 3D Secure Passwort geheim zu halten und darf dieses nicht an unbefugte Dritte weitergeben. Die Weitergabe der persönlichen Identifikationsmerkmale an Zahlungsauslösedienstleister und Kontoinformationsdienstleister ist jedoch zulässig, soweit sie erforderlich ist, damit diese ihre Dienstleistungen für den Karteninhaber erbringen können.

Der Karteninhaber ist verpflichtet, größte Sorgfalt bei der Aufbewahrung und Verwendung eines 3D Secure Passwortes walten zu lassen. Bei der Verwendung von EPW und 3D Secure Passwort ist darauf zu achten, dass diese nicht von Dritten aus gespäht werden.

## **6. Haftung des Karteninhabers**

**6.1.** Alle Dispositionen des Karteninhabers unter Verwendung der Karte erfolgen auf Rechnung des Kontoinhabers. Bei Gemeinschaftskonten haften alle Kontoinhaber für die im Zusammenhang mit der/den Karten entstehenden Verbindlichkeiten solidarisch.

**6.2.** Beruht der nicht autorisierte Zahlungsvorgang auf der missbräuchlichen Verwendung der Karte oder der Kartendaten, so ist der Kontoinhaber dem Kreditinstitut zum Ersatz des gesamten Schadens verpflichtet, der dem Kreditinstitut infolge des nicht autorisierten Zahlungsvorganges entstanden ist, wenn er oder der Karteninhaber ihn in betrügerischer Absicht ermöglicht hat oder durch vorsätzliche oder grob fahrlässige Verletzung einer oder mehrerer Bestimmungen dieser Sonderbedingungen herbeigeführt hat. Wurden diese Pflichten und Bestimmungen vom Konto-/ Karteninhaber nur leicht fahrlässig verletzt, so ist seine Haftung für den Schaden auf den Betrag von EUR 50,- beschränkt. Bei einer allfälligen Aufteilung der Schadenstragung zwischen dem Kreditinstitut und dem Kontoinhaber sind insbesondere die Art der personalisierten Sicherheitsmerkmale sowie die Umstände, unter denen der Verlust, Diebstahl oder die missbräuchliche Verwendung des Zahlungsinstruments stattgefunden hat, zu berücksichtigen.

**6.3.** Die dem Konto aufgrund eines nicht autorisierten Zahlungsvorgangs, der nach einer Sperrmeldung (Punkt 4.1. und 4.4.) stattgefunden hat, angelasteten Beträge, werden dem Kontoinhaber, außer bei betrügerischer Absicht des Konto-/ Karteninhaber, erstattet. Ebenso ist der Betrag zu erstatten, wenn dem Konto-/ Karteninhaber die unverzügliche Sperrmeldung aus von dem Kreditinstitut zu vertretenden Gründen nicht möglich gewesen sein sollte.

## **7. Sicherheitshinweise**

**7.1.** Zur Vermeidung von Risiken, die mit der Kenntnis des Passwortes verbunden sind, empfiehlt das Kreditinstitut das 3D Secure Passwort regelmäßig (z. B. jeden Monat) zu ändern.

**7.2.** Dem Karteninhaber 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.

**7.3.** Es wird empfohlen, den Zugang zum Gebrauch der mobilen Datenendgeräte zu sichern. Bei Verlust oder Diebstahl des mobilen Datenendgerätes empfiehlt das Kreditinstitut die Kontaktaufnahme mit dem Mobilfunkanbieter zur Sperre der SIM Karte.

**7.4.** Zu beachten ist, dass die Verwendung von Passwörtern an gemeinsam benutzten Computern und mobilen Datenendgeräten (z. B. in einem Internetcafé, einem Hotel, am Arbeitsplatz) unbefugten Dritten die Ausspähung von Passwörtern möglich macht.

**7.5.** Der Computer und mobile Datenendgeräte sollten über einen aktuellen Malware- und Virenschutz, aktualisierte Betriebssoftware sowie eine Firewall verfügen. Dadurch kann das Risiko der Ausspähung und missbräuchlichen Verwendung durch Dritte minimiert werden. Die Online Services von Vertragsunternehmen sollten jedes Mal mit der Logout-Funktion beendet werden.

## **8. Dauer und Kündigung der Vereinbarung über die Teilnahme am 3D Secure Verfahren**

**8.1.** Die Vereinbarung über die Teilnahme am 3D Secure Verfahren wird auf unbestimmte Zeit abgeschlossen.

Sie endet jedenfalls mit der Beendigung des Kartenvertrags bzw. der Kontoverbindung oder mit Kündigung der Vereinbarung über die Teilnahme am 3D Secure Verfahren.

**8.2.** Sowohl der Kontoinhaber als auch der Karteninhaber können den Kartenvertrag und/oder die Vereinbarung über die Teilnahme am 3D Secure Verfahren jederzeit unter Einhaltung einer Kündigungsfrist von einem Monat kündigen.

Das Kreditinstitut kann den Kartenvertrag und/oder die Vereinbarung über die Teilnahme am 3D Secure Verfahren unter Einhaltung einer Kündigungsfrist von zwei Monaten kündigen.

Bei Vorliegen eines wichtigen Grundes kann der Kartenvertrag und/oder die Vereinbarung über die Teilnahme am 3D Secure Verfahren sowohl vom Kontoinhaber und/oder vom Karteninhaber als auch vom Kreditinstitut mit sofortiger Wirkung gekündigt werden.

**8.3.** Ein wichtiger Grund, der das Kreditinstitut zur Kündigung des Kartenvertrags und/oder der Vereinbarung über die Teilnahme am 3D Secure Verfahren berechtigt, kann insbesondere vorliegen, wenn

- eine Verschlechterung oder Gefährdung der Vermögensverhältnisse des Kunden (Konto-/ Karteninhabers) oder eines Mitverpflichteten eintritt und dadurch die Erfüllung von Verbindlichkeiten gegenüber dem Kreditinstitut gefährdet ist,

- der Kunde in wesentlichen Belangen unrichtige Angaben über seine Vermögensverhältnisse (Vermögen und Verbindlichkeiten) oder sonstige wesentliche Umstände gemacht hat und das Kreditinstitut bei Kenntnis der wahren Vermögensverhältnisse bzw. Umstände die Geschäftsverbindung oder einzelne Teile davon nicht eingegangen wäre, oder
- der Kontoinhaber eine Verpflichtung zur Bestellung oder Verstärkung von Sicherheiten nicht erfüllt oder nicht erfüllen kann und dadurch die Erfüllung von Verbindlichkeiten gegenüber dem Kreditinstitut gefährdet ist.

**Achtung:** Die Kündigung der Vereinbarung über die Teilnahme am 3D Secure Verfahren bewirkt nicht eine Kündigung des zugrunde liegenden Kartenvertrages. Die Karte kann im Umfang des Kartenvertrages weiter verwendet werden.

## 9. Änderungen der Sonderbedingungen

### 9.1.

Änderungen dieser Sonderbedingungen werden dem Kunden (Konto-/Karteninhaber) vom Kreditinstitut spätestens zwei Monate vor dem vorgeschlagenen Zeitpunkt ihres Inkrafttretens angeboten. Dabei werden die vom Änderungsangebot betroffenen Bestimmungen und die vorgeschlagenen Änderungen in einer Gegenüberstellung dargestellt. Die Zustimmung des Kunden gilt als erteilt, wenn beim Kreditinstitut vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens kein Widerspruch des Kunden einlangt. Darauf wird das Kreditinstitut den Kunden im Änderungsangebot hinweisen.

Außerdem wird das Kreditinstitut eine Gegenüberstellung über die von der Änderung betroffenen Bestimmungen sowie die vollständige Fassung der neuen Sonderbedingungen auf seiner Homepage veröffentlichen und diese in Schriftform dem Kunden auf dessen Verlangen in den Geschäftsstellen aushändigen oder postalisch übermitteln. Auch darauf wird das Kreditinstitut im Änderungsangebot hinweisen. Das Änderungsangebot ist einem Kunden, der Verbraucher ist, mitzuteilen. Dies erfolgt auf dem Postweg oder - sofern mit dem Kunden derartige Änderungsangebote im Wege des Internetbanking (Oberbank Kundenportal) vereinbart wurden - durch Bereitstellung im elektronischen Postfach. Über diese Bereitstellung wird der Verbraucher gesondert per Post informiert oder - wenn mit dem Kunden vereinbart - mittels E-Mail an die von ihm im Internetbanking-Vertrag (Portalvertrag) bekanntgegebene E-Mail-Adresse für Alerting oder mittels SMS an die von ihm dafür bekanntgegebene Rufnummer des Mobiltelefons. Das Änderungsangebot und im Falle der Bereitstellung im elektronischen Postfach auch die Information über diese Bereitstellung haben dem Kunden spätestens 2 Monate vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der Änderungen zuzugehen. Gegenüber einem Unternehmer ist es ausreichend, das Änderungsangebot spätestens 2 Monate vor dem vorgeschlagenen Zeitpunkt des Inkrafttretens der Änderungen auf eine mit dem Unternehmer vereinbarte Weise (daher bei entsprechender Vereinbarung Bereitstellung im elektronischen Postfach) zum Abruf bereit zu halten.

### 9.2.

Änderungen der Sonderbedingungen müssen unter Berücksichtigung aller Umstände (gesetzliche, aufsichtsbehördliche und sonstige behördliche Anforderungen, Gerichtsurteile, die Sicherheit des Bankbetriebs und die technische Entwicklung) sachlich gerechtfertigt sein.

Bei einem Änderungsangebot, das sich auf in diesen Sonderbedingungen enthaltene Leistungen des Kreditinstituts bezieht, ist überdies erforderlich, dass sich dadurch eine Ausweitung der Leistungen des Kreditinstituts oder eine für den Kunden zumutbare Einschränkung der Leistungen des Kreditinstituts und keine unverhältnismäßigen Änderungen wesentlicher Rechte und Pflichten zu Gunsten des Kreditinstituts ergeben.

### 9.3.

Im Falle einer beabsichtigten Änderung der Sonderbedingungen hat der Kunde, der Verbraucher ist, das Recht, seinen Rahmenvertrag für Zahlungsdienste vor dem Inkrafttreten der Änderung kostenlos fristlos zu kündigen.

Darauf wird das Kreditinstitut im Änderungsangebot hinweisen.

## 10. Rechtswahl

Für alle Rechtsbeziehungen zwischen dem Kontoinhaber bzw. dem Karteninhaber und dem Kreditinstitut gilt österreichisches Recht.