



# ANHANG: NUTZUNGSBEDINGUNGEN FÜR 3D SECURE

## Gegenstand:

3D Secure ist ein international anerkannter Standard zur Identifizierung des Inhabers einer Debit- oder Kreditkarte für Online-Zahlungen unter der Bezeichnung „MasterCard® SecureCode™“ für Zahlungen mit MasterCard® und „VERIFIED by VISA“ für Zahlungen mit Visa-Karte. 3D Secure soll die Sicherheit von Transaktionen im Internet erhöhen. Der Karteninhaber kann direkt auf der Website des Händlers überprüfen, ob dieser den Standard 3D Secure zur Absicherung von Online-Einkäufen anwendet.

In den vorliegenden Bedingungen sind die Nutzungsbedingungen für die neueste Version der 3D Secure-Technologie festgelegt. Sie sind eine Ergänzung und integraler Bestandteil der allgemeinen Bedingungen der ausgebenden Bank für die Nutzung der Visa- oder Mastercard-Karten (nachfolgend die „Allgemeinen Bedingungen für die Kartennutzung“) zwischen der Bank (nachfolgend „die ausgebende Bank“), welche die Kredit- oder Debitkarte (nachfolgend die „Karte“) ausgegeben hat, und dem Inhaber und/oder Nutzer der Karte (nachfolgend der „Kunde“).

### § 1: Aktivierung von 3D Secure für eine Karte

- (1) Die Bank behält sich das Recht vor, die 3D Secure-Technologie für die zugelassenen Karten des Kunden automatisch zu aktivieren.
- (2) Ohne die Aktivierung von 3D Secure kann eine Transaktion bei einem Online-Händler, die eine 3D Secure-Identifizierung voraussetzt, nicht ausgeführt werden.

### § 2: Nutzung der Karte und Genehmigung

- a) Ausführung einer 3D Secure-Transaktion mit einem dem LuxTrust-Zertifikat zugeordneten Token (nachfolgend das „LuxTrust-Zertifikat“):

Der Kunde muss die Ausführung der 3D Secure-Transaktion durch Eingabe seiner LuxTrust-Kennung, seines LuxTrust-Passwortes sowie des Einmalpasswortes, das auf seinem LuxTrust-Token angezeigt wird, bestätigen.

- b) Ausführung einer 3D Secure-Transaktion mit LuxTrust Mobile:

Der Kunde muss die Ausführung der 3D Secure-Transaktion mit seiner LuxTrust Mobile-App, die er zuvor auf seinem Smartphone installiert und nach dem vorgesehenen Verfahren aktiviert hat, bestätigen. Im Rahmen des Bestätigungsprozesses wird der Kunde aufgefordert, die Transaktion in der App durch Eingabe des Passworts für LuxTrust Mobile bzw. mittels biometrischer Daten zu bestätigen.

Durch die Eingabe der erforderlichen Sicherheitsdaten wird die Genehmigung der Kartenzahlung gemäß den Allgemeinen Bedingungen für die Kartennutzung der ausgebenden Bank bestätigt.

### § 3: Sorgfaltspflicht

- (1) Der Kunde muss die Sicherheit und die Geheimhaltung seiner Sicherheitsdaten und aller Mittel oder Geräte für die Bestätigung

einer Transaktion (Kredit- oder Debitkarte, LuxTrust-Token) gewährleisten

Der Kunde darf insbesondere die Sicherheitsdaten weder vollständig noch abgeändert aufschreiben oder elektronisch speichern – ob kodifiziert oder nicht – noch einem Dritten mitteilen.

- (2) Bei der Bestätigung der 3D Secure-Transaktion muss sich der Kunde vergewissern, dass das betreffende Portal den nachfolgenden Sicherheitskriterien entspricht:
  - die Adresse des Portals beginnt mit „https“,
  - die Adresszeile des Portals zeigt ein Schloss-Symbol an,
  - das Portal zeigt das Logo „Master-Card® SecureCode™“ oder „VERIFIED by VISA“ an,
  - das vom Kunden ausgewählte LuxTrust-Sicherheitsbild wird angezeigt, wenn er sich für die Bestätigung per LuxTrust-Token entscheidet,
  - die Informationen zur Transaktion erscheinen im Sicherheitsbild oder auf der LuxTrust Mobile-App. Dabei handelt es sich um die Transaktionsdaten, die der Kunde bestätigen möchte.

Sollte das Portal einer dieser Sicherheitsanforderungen nicht entsprechen, darf der Kunde die Transaktion nicht bestätigen und er haftet allein für Schäden, die aufgrund der Eingabe seiner Sicherheitsdaten und einer eventuellen Bestätigung der Transaktion entstehen können.

- (3) Sollte das Portal einer dieser Sicherheitsanforderungen nicht entsprechen oder sollte ein Verdacht hinsichtlich einer betrügerischen Nutzung der Sicherheitsdaten des Kunden bestehen, muss der Kunde die Bank, welche die Karte ausgegeben hat, unverzüglich informieren und die Karte gemäß den Allgemeinen Bedingungen für die Kartennutzung der ausgebenden Bank sperren lassen.

### § 4: Verarbeitung von personenbezogenen Daten

- (1) Der Kunde bevollmächtigt die ausgebende Bank, seine personenbezogenen Daten zu verarbeiten, um das ordnungsgemäße Funktionieren der Karte sowie die Vorbeugung, Feststellung und Analyse von betrügerischen Transaktionen zu gewährleisten.
- (2) Abgesehen von den Bestimmungen in Bezug auf die Verarbeitung der personenbezogenen Daten in den Allgemeinen Bedingungen für die Kartennutzung der ausgebenden Bank berechtigt der Kunde die ausgebende Bank ausdrücklich zur Weitergabe seiner personenbezogenen Daten an Dritte, deren Mitwirkung im Rahmen von 3D Secure notwendig ist.

In diesem Zusammenhang bestätigt der Kunde ausdrücklich, darüber in Kenntnis gesetzt worden zu sein, dass die Nutzung von 3D Secure die Mitwirkung von Drittunternehmen im Rahmen der Bestätigung per LuxTrust-Zertifikat erforderlich macht. Die übermittelten Daten können von diesen Drittunternehmen im In- und Ausland gespeichert werden.

- (3) Die ausgebende Bank, die für die Verarbeitung der personenbezogenen Daten verantwortlich ist, verpflichtet sich, diese Daten gemäß der geltenden Gesetzgebung zum Schutz

von Personen bei der Verarbeitung personenbezogener Daten zu verarbeiten.

(4) Der Kunde kann die Übermittlung der Informationen im Rahmen von 3D Secure ablehnen, indem er den Kundenservice kontaktiert.

## **§ 5: Haftung**

(1) Die Haftungsklauseln in den Allgemeinen Bedingungen für die Kartennutzung sowie in den Allgemeinen Geschäftsbedingungen der ausgebenden Bank gelten ebenfalls für die Nutzung von 3D Secure.

Die ausgebende Bank gewährleistet nicht die systematische Verfügbarkeit von 3D Secure und kann nicht für Schäden, die aus einer Störung, einer Unterbrechung (einschließlich im Falle notwendiger Wartungseingriffe) oder einer Überlastung der Systeme der ausgebenden Bank oder eines von der ausgebenden Bank beauftragten Dritten resultieren, haftbar gemacht werden.

(2) Die ausgebende Bank übernimmt keine Haftung für ein Versagen der 3D Secure-Technologie beziehungsweise für Schäden, die aus einer Störung, der mangelhaften Funktionsfähigkeit oder Unterbrechung der elektronischen Kommunikationsnetzwerke (Internet, Mobilfunknetz) und von öffentlichen Servern, einem Arbeitskampf oder anderen Ereignissen außerhalb ihrer Kontrolle resultieren.