Zahlungsdiensterichtlinie II (PSD 2) und starke Kundenauthentifizierung

Die Zahlungsdiensterichtlinie II (PSD 2) ist eine EU-Richtlinie zur Regulierung von Zahlungsdiensten und soll den Kreditkartenbetrug eindämmen sowie Online-Zahlungen sicherer machen. Obgleich Reisebüros und Reiseveranstalter nicht direkter Adressat der Richtlinie sind, können sie trotzdem von den Neuerungen, insbesondere der sogenannten starken Kundenauthentifizierung, welche für die Abwicklung von Zahlungen relevant ist, betroffen sein. Die betreffenden Gesetzesbestimmungen (§ 87 Zahlungsdienstegesetz) treten am **14. September 2019** in Kraft.

Welche Vorgänge bedürfen einer starken Kundenauthentifizierung?

Die PSD 2 führt zur Absicherung von Zahlungen die sogenannte starke Kundenauthentifizierung ein. Es wird somit geprüft, ob ein bestimmter Zahlungsauftrag tatsächlich von der berechtigten Person erteilt wurde.

Eine starke Kundenauthentifizierung durch einen Zahlungsdienstleister ist erforderlich, wenn der Kunde

- online auf sein Zahlungskonto zugreift
- einen elektronischen Zahlungsvorgang auslöst oder
- über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt.

Ein elektronischer Zahlungsvorgang liegt beispielsweise vor, wenn der Kunde im Internet oder an einem POS-Terminal mit Bankomat-/Kreditkarte Zahlungen tätigt.

Was versteht man unter einer starken Kundenauthentifizierung?

Eine starke Kundenauthentifizierung ist eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien

- Wissen (etwas, das nur der Nutzer weiß; z.B. Passwörter, TANs etc.),
- Besitz (etwas, das nur der Nutzer besitzt; z.B. Kreditkarte, Handy etc.) oder
- Inhärenz (etwas, das nur der Nutzer ist; z.B. Fingerabdruck, Stimmerkennung, etc.)

In der Praxis kann eine starke Kundenauthentifizierung an einem POS-Terminal durch Zahlung mit Kreditkarte (Element Besitz) und PIN-Eingabe (Element Wissen) erfolgen. Ab 14.9.2019 verlangt Art 4 der delegierten Verordnung (EU) 2018/389 außerdem, dass die starke Kundenauthentifizierung, die auf mindestens zwei Elementen der Kategorien Wissen, Besitz und Inhärenz beruht, auch eine Generierung eines Authentifizierungscodes nach sich zieht. Bei Zahlungen an POS-Terminals kann der Authentifizierungscode aus der verwendeten gültigen Karte und dem korrekten PIN generiert und direkt vom Gerät an den Zahlungsdienstleister übermittelt werden. Dadurch muss vom Kunden kein zusätzlicher Authentifizierungsschritt abverlangt werden.

Bei Zahlungen im Internet muss der Authentifizierungscode dynamisch mit dem Zahlungsbetrag und dem Empfänger des Zahlungsvorganges verknüpft werden (z.B.

Übersendung einer TAN mittels SMS inklusive Information, für welchen Betrag und Zahlungsempfänger dieser TAN gelten soll).

Zu welchem Zeitpunkt ist die starke Kundenauthentifizierung durchzuführen?

Maßgebend für die starke Kundenauthentifizierung ist der Zeitpunkt der Zahlung. Buchung einer Reiseleistung und Zahlung inklusive starker Kundenauthentifizierung können zeitlich auseinanderfallen (z.B. Annahme einer Buchung, Leistung einer Anzahlung [starke Kundenauthentifizierung] erfolgt erst zu einem späteren Zeitpunkt).

Ausnahmen von der starken Kundenauthentifizierung:

Zahlungsdienstleister können beispielsweise in folgenden Fällen von einer starken Kundenauthentifizierung absehen:

- Kontaktlose Zahlungen von max. 50 Euro (sofern bestimmte Kriterien der früheren Nutzung der Karte eingehalten werden; z.B. elektronische Zahlungsvorgänge von nicht mehr als 150 Euro seit Durchführung der letzten starken Kundenauthentifizierung)

- Kleinbetragszahlungen von max. 30 Euro (sofern bestimmte Kriterien der früheren Zahlungsvorgänge eingehalten werden)

- Zahlungen an unbeaufsichtigten Terminals für Nutzungsentgelte und Parkgebühren

- Wiederkehrende Zahlungsvorgänge mit demselben Betrag und Empfänger (z.B. Abonnement)

- Zahlungen an vertrauenswürdige Empfänger. Hier gibt der Zahler seinem kontoführenden Zahlungsdienstleister eine Liste vertrauenswürdiger Empfänger bekannt.

Was sollten Reisebüros/Reiseveranstalter tun, um sich auf die starke Kundenauthentifizierung vorzubereiten?

Reisebüros und Reiseveranstalter sollten sich mit ihren jeweiligen Zahlungsdienstleistern (Acquirer=Schnittstelle zwischen Reisebüro/Reiseveranstalter und Kreditkartenausgabestelle; Issuer/Kreditkartenausgabestelle) in Verbindung setzen und abklären, mit welchen technischen Verfahren die starke Kundenauthentifizierung konkret durchgeführt werden wird.

Stand: Juli 2019

Impressum:
Fachverband der Reisebüros
Wiedner Hauptstraße 63, 1045 Wien
T: 05 90 900-3409
E: reisebueros@wko.at W: www.reisebueros.at