FAQ Richtlinie PSD2 Zahlungsverkehr

Häufige Fragestellungen in Verbindung mit der neuen Zahlungsdienstrichtlinie PSD2

Die in diesem FAQ enthaltenen Informationen dienen der allgemeinen Orientierung.

Rechtshinweis:

Die Inhalte wurden mit großer Sorgfalt recherchiert. Dennoch kann Sage keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Informationen übernehmen. Die Informationen sind insbesondere auch allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar.

Stand: August 2019

Inhaltsverzeichnis

1.0 Fragen zu PSD2

1.1 Woher kommen die neuen Regeln?

Grundlage der Neuerungen ist die zweite EU-Zahlungsdiensterichtlinie, kurz PSD2. Sie soll den Zahlungsverkehr in der EU für Verbraucher bequemer und sicherer machen und zugleich den Wettbewerb fördern. Schon am 13. Januar 2018 wurde die Richtlinie in nationales Recht umgesetzt. Einige Vorgaben entfalten aber erst jetzt ihre Wirkung.

1.2 Was genau regelt die PSD2?

Banken müssen Drittanbietern Zugriff auf Zahlungskonten gewähren. Außerdem ist die PSD2 dafür verantwortlich, dass Händler seit Anfang 2018 für einzelne Bezahlmethoden wie Überweisung, Lastschrift oder Kreditkarte keine Extragebühren mehr verlangen dürfen.

Ab 14. September 2019 ist zudem bei Onlinezahlungen und beim Zugriff auf das Onlinebanking die „Zwei-Faktor-Authentifizierung“ vorgeschrieben. Das heißt, zusätzlich zum Benutzernamen und zum Passwort müssen Kunden dann in vielen Fällen auch eine Tan-Nummer eingeben – so wie heute schon bei Onlineüberweisungen. Tan-Listen (iTan) sind künftig allerdings nicht mehr erlaubt, die Codes müssen jedes Mal neu erzeugt werden.

1.3 Was ändert sich bei der Kundenauthentifizierung für das Online Banking?

Bei Zahlungen im Internet ist die sogenannte Zwei-Faktor-Authentifizierung bereits heute Pflicht. Das bedeutet, dass die Authentifizierung des Kunden über zwei Faktoren erfolgen muss, die durch Wissen (z.B. PIN), Besitz (z.B. Smartphone) oder Inhärenz (z.B. Fingerabdruck) vermittelt werden. Die PSD2 verlangt dieses Verfahren künftig auch beim Einloggen im Online-Banking oder sonstigen Handlungen, die das Risiko eines Missbrauchs bergen. Die neuen Vorschriften zur „starken Kundenauthentifizierung“, treten ab 14. September 2019 in Kraft und die iTAN wird damit abgeschafft.

1.4 Welche Rechte des Bankkunden wurden gestärkt?

- Die Erstattungsfrist bei nicht autorisierten Zahlungen wird verkürzt.
- Die Ansprüche bei verspäteter Ausführung einer Zahlung werden geregelt.
- Die Haftungsgrenze im Fall von Missbrauch bei Karten- und Online-Banking-Zahlungen wird gesenkt.
- Kartenzahlungen können künftig nur noch mit Zustimmung des Kunden vorreserviert werden.
- Zahlungen innerhalb des Europäischen Wirtschaftsraums in einer Drittstaatenwährung (zum Beispiel US-Dollar) werden stärker vom Zahlungsdiensterecht erfasst.

1.5 Was bedeuten diese neuen Vorschriften zu Drittdienstleistern für den Kunden?

Kunden können im Online-Banking Drittdienstleister damit beauftragen, Zahlungen vorzunehmen oder Kontoinformationen abzurufen (beispielsweise für ihre Finanzplanung). Da diese Dienstleister nunmehr gesetzlich anerkannt sind und der Bankenaufsicht unterliegen, dürfen Kunden gegenüber diesen Diensten auch ihre PIN und TAN einsetzen.

1.6 Welche Rechte und Pflichten haben die Drittdienste?

Die Drittdienstleister unterliegen zukünftig der Aufsicht. So benötigen Zahlungsauslösedienste für ihre Tätigkeit eine Zulassung von der der nationalen Aufsichtsbehörde. Das ist in Deutschland die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Kontoinformationsdienste müssen sich bei der Aufsicht registrieren lassen. Für die Zulassung und Registrierung wird bei Zahlungsauslöse- und Kontoinformationsdiensten eine Berufshaftpflichtversicherung oder eine gleichwertige Garantie vorausgesetzt.

1.7 Gibt es für die Banken eine gesetzliche Regelung zur Umsetzung der starken Kundenauthentifizierung?

Nein, jede Bank kann selbst entscheiden, wie die gesetzliche Vorgabe zur starken Kundenauthentifizierung umsetzt bzw. in welchem zeitlichen Intervall sie vom Kunden eine starke Authentifizierung verlangt.

1.8 Welche Änderungen sind besonders wichtig??

Mit der PSD2 werden neue Vorschriften für Drittdienste geschaffen. Das sind Zahlungsauslösedienste und Kontoinformationsdienste. Wenn der Kunde im Rahmen des Online-Banking solche Drittdienste nutzt, ist die Bank verpflichtet, diesen Zugang zum Zahlungskonto des Kunden zu gewähren. Die Drittdienste unterliegen nunmehr der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht.

1.9 Wer darf auf die Kontodaten zugreifen?

Ohne die Zustimmung des Kunden geht es nicht! Sie ist die Voraussetzung dafür, dass Dritte auf die Kontodaten zugreifen dürfen. Die Richtlinie unterscheidet zwei Typen:

- Kontoinformationsdienste (KID) analysieren die Kontobuchungen – beispielsweise mit Blick auf Verträge oder die Bonität der Kunden
  Kontoinformationsdienste sind in der Lage, für den Kunden Kontoinformationen wie Umsätze, Salden und Vormerkposten abzurufen, sofern der Kunde am Online-Banking seiner Bank teilnimmt. Dies ist insbesondere für Kunden interessant, die Konten bei mehreren Banken haben und sich damit einen besseren Überblick über ihre Kontenlage verschaffen wollen.
- Zahlungsauslösedienste (ZAD) stoßen im Namen der Kunden Zahlungen von deren Konten an. Kauft ein Kunde im E-Commerce ein, so kann er für die Zahlungsabwicklung einen Dienstleister nutzen. Dieser reicht für den Kunden den Überweisungsauftrag bei der Bank ein, wenn der Kunde dem vorher zugestimmt hat.

Um solche Geschäftsmodelle betreiben zu dürfen, müssen Anbieter sich bei der Finanzaufsicht Bafin als KID registrieren lassen oder eine Erlaubnis als ZAD beantragen. Ab 14. September 2019 ist der Kontozugriff ohne Bafin-Zustimmung nicht mehr erlaubt. Wollen Banken oder E-Geldinstitute solche Dienste erbringen, reicht dafür ihre bestehende Bafin-Erlaubnis.

1.10 Wie genau funktioniert der Datenaustausch?

Um die Angebote eines Zahlungsauslöse- oder Kontoinformationsdienstes überhaupt nutzen zu können, benötigen Kunden einen Onlinebanking-Zugang. Bisher wurden die Daten häufig über das sogenannte Screen-Scraping übertragen. Dabei haben die Anbieter mit den Log-in-Daten der Kunden auf deren Onlinebanking zugegriffen.

Die Banken konnten dabei nicht erkennen, ob der Kunde selbst auf das Konto schaut oder ein Fremder. Zudem erhielten die Anbieter breite Einblicke. Im Zuge der PSD2 dürfen die Daten ab 14. September 2019 nur noch über spezielle Datenschnittstellen (APIs) ausgetauscht werden. Diese bieten eine Art Einlasskontrolle, bei der Drittanbieter ihre Erlaubnis der Finanzaufsicht vorweisen müssen. Auch der Umfang der übermittelten Daten wurde beschränkt.

1.11 Was hat es mit Screen Scraping auf sich?

Die Europäische Kommission hat am 27. November 2017 die Technischen Regulierungsstandards (RTS, Regulatory Technical Standards) für die sichere Kommunikation und die starke Kundenauthentifizierung zur PSD2 veröffentlicht. Damit hat sich die Europäische Kommission eindeutig für den Zugriff auf Zahlungskonten über Schnittstellen (APIs) ausgesprochen. Screen Scraping (eine Technik zum Auslesen von Informationen aus Internetseiten) ist damit grundsätzlich nicht mehr erlaubt. Dies ist im Sinne des Kunden und stärkt sowohl die Sicherheit des Online Banking als auch die Transparenz über die Weitergabe von Daten.

1.12 Welche Daten werden über eine API übermittelt?

Grundsätzlich können Banken selbst entscheiden, welche Daten sie über ihre Schnittstellen zur Verfügung stellen. Die Formulierung in der Richtlinie lässt Raum für Interpretationen. Zu den Mindestanforderungen zählen viele Banken die Kontoumsätze, den Kontostand, die Währung, in der das Konto geführt wird, die Kontonummer und die Produktbezeichnung des Kontos.

1.13 Wie verändert sich der Datenzugriff ab September 2019?

Technisch und rechtlich bedeutet die Umstellung auf die neuen Schnittstellen eine große Veränderung. Beim Ablauf ändert sich für den Anwender jedoch wenig – zumindest im ersten Schritt. Sie müssen weiterhin ihre Log-in-Daten für das Onlinebanking eingeben. Soll eine Zahlung angestoßen werden, erhalten sie im nächsten Schritt eine Tan von ihrer Bank. Diesen Sicherheitscode müssen sie ebenfalls eingeben.

Neu hierbei ist, dass auch bei Kontoinformationsdiensten in vielen Fällen eine Tan eingegeben weren muss. Die Bank kann entscheiden, ob sie bei jedem Zugriff einen Code abfragt oder nur alle 90 Tage.

1.14 Unterliegen die Drittanbieter der DSGVO?

Ja, wie alle Firmen müssen sich auch Kontoinformations- und Zahlungsauslösedienste an die Vorgaben der europäischen Datenschutz-Grundverordnung (DSGVO) halten.

1.15 Welche Erstattungsfrist gilt künftig bei nicht autorisierten Zahlungen?

Sollte auf dem Zahlungskonto eine Zahlung gebucht worden sein, ohne dass der Kontoinhaber diese veranlasst oder dieser zugestimmt hat, kann er Erstattung von der Bank verlangen. Die Erstattungsfrist ist auf einen Geschäftstag verkürzt worden, außer die Bank stellte eine

Autorisierung der Zahlung durch den Kontoinhaber fest oder hat einen Betrugsverdacht gegen den Kunden.

1.16 Welche Ansprüche hat der Kunde künftig bei verspäteter Ausführung einer Zahlung?

Sollte eine Zahlung einmal verspätet beim Empfänger ankommen, sind die beteiligten Zahlungsdienstleister verpflichtet, diese Verspätung beim Zahlungsempfänger auszugleichen.