Fragen und Antworten zu PSD2 und RTS

Drittdienstleister

- **Was sind Drittdienstleister?**
  Als „Dritte“ bezeichnet man Nicht-Banken, die Zahlungsauslöse- und Kontoinformationsdienste anbieten. Dazu benötigen sie Ihre Zustimmung zum Zugriff auf Ihr Bankkonto. Sie stehen dabei zwischen Ihnen und Ihrer Bank - als Dritte. Ein Drittdienstleister kann ein FinTech-, Telekommunikations- oder Großhandelsunternehmen sein. Diese müssen sich zunächst als Zahlungsauslösedienstleister oder Kontoinformationsdienstleister etablieren und die entsprechende Genehmigung der Aufsichtsbehörden einholen bzw. sich dort registrieren. Auch Banken und Sparkassen dürfen Zahlungsauslöse- und Kontoinformationsdienste im Rahmen ihrer Banklizenz anbieten.

- **Was ist ein Zahlungsauslösedienstleister?**
  Kauft ein Kunde im E-Commerce ein, so kann er für die Zahlungsabwicklung einen auf der Homepage des Verkäufers angebotenen Zahlungsauslösedienstleister nutzen. Dieser reicht für den Kunden den Überweisungsauftrag bei der Bank ein, wenn der Kunde dem vorher zugestimmt hat und sein Konto am Online-Banking seiner Bank teilnimmt.

- **Was ist ein Kontoinformationsdienstleister?**
  Kontoinformationsdienstleister rufen Kontoinformationen der vergangenen 90 Tage wie Umsätze, Salden und Vormerkposten bei der kontoführenden Bank oder Sparkasse ab und bereiten diese für den Kunden auf. Voraussetzung ist, dass das Kundenkonto am Online-Banking seiner Bank teilnimmt und der Kunde seine Zustimmung erteilt hat. Dies ist insbesondere für Kunden interessant, die Konten bei mehreren Banken haben und sich damit einen besseren Überblick über ihre Kontenlage verschaffen wollen.

- **Werden Drittdienstleister überwacht?**
  Drittdienstleister unterliegen zukünftig der Aufsicht. So benötigen Zahlungsauslösedienstleister für ihre Tätigkeit eine Zulassung von der nationalen Aufsichtsbehörde. Das ist in Deutschland die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Kontoinformationsdienstleister müssen sich bei der Aufsicht registrieren lassen. Für die Zulassung und Registrierung wird bei Zahlungsauslöse- und Kontoinformationsdienstleistern eine Berufshaftpflichtversicherung oder eine gleichwertige Garantie vorausgesetzt.

- **Was bedeuten die neuen Vorschriften zu Drittdienstleistern für den Kunden?**
  Kunden können im Online-Banking Drittdienstleister damit beauftragen, Zahlungen auszulösen oder Kontoinformationen abzurufen (beispielsweise für ihre Finanzplanung). Da diese Dienstleister nunmehr gesetzlich anerkannt sind und der Aufsicht unterliegen, dürfen Kunden gegenüber diesen Diensten auch ihre PIN und TAN einsetzen.

- **Muss ich Drittdienstleistern den Zugriff auf mein Konto gewähren?**
  Nein, Sie müssen Dritten keinen Zugang zu Ihrem Konto gewähren – die PSD2 gibt Ihnen nur das Recht dazu. Um genau zu sein: Die PSD2 gibt Ihnen das Recht, die Dienste eines neuen Anbieters zu nutzen, der Zugang zu Ihrem Online-Konto benötigt, um diese Dienste anbieten zu können.
  Wenn Sie Ihre Zustimmung geben, bedeutet dies, dass Sie dem Dritten Zugang zu Ihrem Bankkonto gewähren.
  Wenn Sie Ihre Zustimmung nicht geben, wird sich nichts ändern. Der Dritte erhält keinen Zugang zu Ihrem Bankkonto.

- **Was bedeutet es, wenn ich Zugriff auf mein Konto gewähre?**
  Wenn Sie dem Zugang zu Ihrem/Ihren Bankkonto/Bankkonten zustimmen, kann ein Kontoinformationsdienstleister beispielsweise den Saldo und die Kontoumsätze der vergangenen 90 Tage von Ihren Zahlungskonten bei einer oder mehreren Banken abrufen und für Sie übersichtlich aufbereiten. Zahlungsauslösedienstleister können Ihre Bank auffordern, in Ihrem Namen eine Zahlung oder Überweisung von Ihrem Konto zu veranlassen. Sie sollten beachten, dass Ihre Zustimmung zu einem Zahlungsauslösungsdienst grundsätzlich nur für eine einzige Zahlung gilt. Ihre Zustimmung zu den Kontoinformationsdiensten kann für einen Zeitraum von 90 Tagen gelten. Während dieses Zeitraums kann der Dienstleister für Kontoinformationen auf Ihr Bankkonto oder Ihre Bankkonten zugreifen, um die Übersicht über Zahlungen und Kontostände zu aktualisieren. Spätestens nach 90 Tagen müssen Sie erneut Ihre ausdrückliche Zustimmung zum Zugriff auf Ihr Bankkonto erteilen.

- **Wie gewähre ich den Zugriff auf mein Konto?**
  Sie können einem Zahlungsauslösedienst- oder Kontoinformationsdienstleister die Zustimmung erteilen, auf Ihr Bankkonto zuzugreifen. Unter der PSD2 dürfen diese Anbieter das Überprüfungsverfahren Ihrer Bank verwenden. Die PSD2 schreibt vor, dass dies immer ein zweistufiges Verfahren sein muss (starke Kundenauthentifizierung), die genauen Details können jedoch je nach Bank/Sparkasse oder Zahlungsinstitut variieren.

  Wenn Sie einem Zahlungsauslösungsdienstleister die Einwilligung zur Ausführung einer Zahlung erteilen, ähnelt dies dem Einleiten eines Zahlungsauftrags bei Ihrer Bank/Sparkasse. Das Verfahren für Anbieter von Kontoinformationsdiensten unterscheidet sich geringfügig.

  In beiden Fällen überprüft Ihre Bank/Sparkasse oder Ihr Zahlungsinstitut zunächst, ob Sie der Kontoinhaber sind. Dazu wird nach einer Kombination von mindestens zwei der folgenden Elemente gefragt:
  - etwas, das Sie besitzen (z. B. eine Debitkarte, einen TAN-Rechner oder ein Mobiltelefon),
  - etwas, das nur Sie kennen (Zugangscode),
  - biometrische Identifizierung (z. B. Fingerabdruck, Iris-Scan).

Zahlungsauslösedienst

Zur Auslösung einer Zahlung wird nach Überprüfung Ihrer Identität ein eindeutiger Code (TAN) generiert, der mit der vorgeschlagenen Transaktion (Betrag und Begünstigter) verknüpft ist. Diese TAN kann nur für diese bestimmte Zahlung verwendet werden: Wenn sich der Betrag oder der Begünstigte ändert, ändert sich auch die TAN. Mit der Eingabe der TAN erklären Sie sich einverstanden, die Zahlung zu veranlassen.

In Kombination mit anderen Sicherheitsmaßnahmen wird so sichergestellt, dass der Zahlungsdienstleister Transaktionen nur mit Ihrer Zustimmung durchführen kann.

Kontoinformationsdienst

Nach der erfolgten Identitätsprüfung bittet der Kontoinformationsdienstleister Sie um Ihre ausdrückliche Zustimmung zur Verwendung Ihrer Kontoinformationen.

- **Ich möchte die neuen Zahlungsmethoden nicht verwenden. Was soll ich machen?**
  Sie sind nicht dazu verpflichtet, die neue Zahlungsmethode zu verwenden. Wenn Sie Ihre Zustimmung nicht geben, erhält der Dritte keinen Zugang zu Ihrem Konto.

Sicherheit und Privatsphäre

- **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.

- **Was ändert sich bei der Kundenauthentifizierung für das Online-Banking und bei Zahlungen im Internet?**
  Beim Einloggen im Online-Banking und bei Zahlungen im Internet ist die sogenannte Zwei-Faktor-Authentifizierung oder auch Starke Kundenauthentifizierung Pflicht. Das bedeutet, dass die Authentifizierung des Kunden über zwei voneinander unabhängige Faktoren erfolgen muss, die aus Wissen (z.B. PIN), Besitz (z.B. Smartphone) oder Inhärenz (z.B. Fingerabdruck) bestehen. Die PSD2 verlangt dieses Verfahren auch bei sonstigen Handlungen, die das Risiko eines Missbrauchs bergen wie beispielsweise die Änderung eines Dauerauftrags.
  Durch die Zwei-Faktor-Authentifizierung erhöht sich die Sicherheit beim Online-Banking und bei Internetzahlungen. Ein Betrüger müsste beide Faktoren kennen, um Zugang zum Konto zu bekommen. Bei der Auslösung einer Zahlung ist ein Faktor an den Zahlungsbetrag und den Empfänger gekoppelt, dieses Sicherheitselement kann also nur zur Freigabe dieser bestimmten Zahlung genutzt werden.

- **Wieso wird das iTan Verfahren zum September 2019 eingestellt?**
  Die Zweite Zahlungsdiensterichtlinie (PSD2) verpflichtet Zahlungsdienstleister ab dem 14. September 2019 eine starke Kundenauthentifizierung u. a. bei im Online-Banking ausgelösten Überweisungen durchzuführen. Das iTAN-Verfahren erfüllt die vorgegebenen Voraussetzungen dafür nicht mehr und darf daher ab diesem Datum nicht mehr genutzt werden. Ein Fachartikel der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1806_Starke_Kundenauthentifizierung.html), der hier auszugsweise wiedergegeben wird, erhält näherer Informationen zu den Änderungen zum 14. September 2019 und zur Einstellung des iTAN-Verfahrens:
  „Wenn es sich bei der ausgelösten elektronischen Zahlung um einen Fernzahlungsvorgang handelt, zum Beispiel die Beauftragung einer Überweisung im Online-Banking oder die Zahlung mit Kreditkarte im Internet, ist die Starke Kundenauthentifizierung mit einer sogenannten dynamischen Verknüpfung in Bezug auf Empfänger und Betrag zu erweitern. Was das heißt, lässt sich am besten an einem Beispiel erläutern. Bei der Übersendung einer TAN mittels SMS muss dem Nutzer mitgeteilt werden, für welchen Betrag und Zahlungsempfänger diese TAN gelten soll; jede Änderung der Zahlungsdaten würde die übermittelte TAN ungültig machen. Die bisher noch manchmal verwendeten iTAN-Listen erfüllen diese Anforderung nicht, denn die dort aufgedruckten TANs sind für beliebige Zahlungen verwendbar. Darüber hinaus sind die Listen leicht kopierbar. Damit besteht die Gefahr, dass Betrüger in den Besitz der TANs kommen und diese dann für Zahlungen zu ihren Gunsten verwenden.“

- **Ist eine Sitzung im Online –Banking zeitlich begrenzt?**
  Aus Sicherheitsgründen sind die Zahlungsdienstleister verpflichtet, einen Online-Zugriff des Kunden auf sein Zahlungskonto spätestens 5 Minuten nach der Authentifizierung des Kunden zu beenden, wenn keine Aktivität des Kunden festzustellen ist. Damit möchte man verhindern, dass ein Fremder Zugang zum Konto bekommt, wenn beispielsweise der Kunde sich angemeldet aber nicht abgemeldet hat.

- **Wie schützt die PSD2 meine Privatsphäre?**
  Die PSD2 stellt mehrere Anforderungen an die Anbieter von Zahlungsauslöse- und Kontoinformationsdiensten, um Ihre Privatsphäre zu schützen. Die Allgemeine Datenschutzverordnung gilt auch für diese Dienstleister.

  Der Zahlungsauslösedienstleister darf dem Begünstigten nur mit Ihrer ausdrücklichen Zustimmung Informationen über Sie zur Verfügung stellen. Es ist ihm nicht gestattet, sensible Zahlungsdaten zu speichern (d. h. Daten, die zu Betrugszwecken missbraucht werden könnten; der Name des Kontoinhabers und die Kontonummer gelten nicht als sensible Zahlungsdaten). Außerdem darf er nicht mehr Informationen von Ihnen anfordern, als für die Erbringung der Dienstleistung unbedingt erforderlich ist. Dem Zahlungsauslösedienstleister ist es nicht gestattet, auf Ihre Daten zuzugreifen, sie zu verwenden

oder für andere Zwecke als den spezifischen Dienst, dem Sie zugestimmt haben, zu speichern.

Der Kontoinformationsdienstleister darf mit Ihrer ausdrücklichen Zustimmung nur auf Informationen über das oder die von Ihnen angegebenen Konten zugreifen. Er darf keine sensiblen Zahlungsdaten anfordern (d. h. Daten, die zu Betrugszwecken missbraucht werden könnten; der Name des Kontoinhabers und die Kontonummer gelten nicht als sensible Zahlungsdaten). Es ist ihm nicht gestattet, für andere Zwecke als den spezifischen Dienst auf Ihre Daten zuzugreifen, sie zu verwenden oder zu speichern.