IHRE DIENSTE FÜR DEN ALLTAG

Informationen über die PSD2 Zahlungsdienste

In diesem Informationsdokument möchten wir Ihnen in einfachen Worten die Funktionsweise und die Neuerungen der„PSD2" erklären, einem Akronym, das sich auf die zweite EU-Richtlinie[1] über Zahlungsdienste innerhalb der Europäischen Union sowie ganz allgemein auf alle damit verbundenen Rechts- oder Verwaltungsvorschriften bezieht.
Dieses Dokument dient nur zu Informationszwecken. Einzelheiten zu den für Sie geltenden Vorschriften finden Sie in Ihrem Vertrag, insbesondere in den entsprechenden Begleitdokumenten. Ihr Vertrag wird insbesondere durch die im Glossar aufgeführten Begriffsbestimmungen ergänzt, und auch die entsprechenden Begleitdokumente wurden aktualisiert (z. B. Zahlungsvorgänge, Online-Banking, Karten usw.).

Vokabular

Englisch		Deutsch	konkret
AISP	account information service provider	Kontoinformationsdienstleister	Bank oder Fintech
AS-PSP	account servicing payment service provider	kontoführender Zahlungsdienstleister	Ihre Bank
PISP	payment initiation service provider	Zahlungsauslösedienstleister	Bank oder Fintech
PSU	payment service user	Zahlungsdienstnutzer	Sie
PSP	payment service provider	Zahlungsdienstleister	Bank oder Fintech
SCA	strong customer authentication	starke Kundenauthentifizierung	sicheres Mittel

Betroffene

Die PSD2 gilt für sogenannte PSP, bei denen es sich hauptsächlich um Banken handelt, die für ihre Kunden Zahlungsdienste bereitstellen (z. B. POST Finance für Sie). Andere Anbieter, wie PISP, AISP oder auch E-Geld-Institute und Zahlungsinstitute, sind jedoch ebenfalls von den Anforderungen der PSD2 betroffen. Die Anwendbarkeit der PSD2 hängt ausschließlich von der Erbringung von Zahlungsdiensten ab und nicht von der Art der Aktivitäten, dem Kundentyp oder der Größe des Unternehmens.

Inhalt

Informationen: Die PSD2 verlangt von den PSP eine größere Transparenz hinsichtlich der Informationen, die für die PSU in Bezug auf die Gebühren, die Ausführungsfristen für Transaktionen, die Nutzung von Zahlungsinstrumenten, Reklamationen, Ihre Erstattungsansprüche usw. bereitgestellt werden.

Transaktionen: Durch das Inkrafttreten der PSD2 müssen alle PSP in Europa grundsätzlich innerhalb eines Werktags (ab dem Empfangsdatum des Zahlungsauftrags) Zahlungen ausführen, die innerhalb der Europäischen Union und in einer europäischen Währung erfolgen. In der Regel verkürzen sich somit die Fristen für die Ausführung und die Bereitstellung der Gelder.

Verantwortung: Die PSD2 stärkt die Verantwortung der PSP für die ordnungsgemäße Ausführung der Zahlungsvorgänge.

Erstattungen: Für die PSU verbessern sich die Erstattungsbedingungen in Zusammenhang mit Zahlungsvorgängen.

Vorfälle: Alle Vorfälle, die als schwerwiegend angesehen werden, sind unmittelbar der zuständigen Behörde (in Luxemburg die CSSF[2]) zu melden und der betroffene PSP muss den PSU benachrichtigen, falls der Vorfall Auswirkungen auf seine finanziellen Interessen haben könnte.

Betrug: Durch die mit der PSD2 auferlegten neuen Pflichten in Bezug auf Risiken, Sicherheit, Überwachung und die Mitteilung von Betrugsstatistiken sollen die PSP dabei unterstützt werden, Sie besser vor Betrug zu schützen. Zur Einschränkung von Betrugsfällen wird den ASPSP durch die PSD2 auch die Einrichtung einer starken Authentifizierung ihrer PSU für den Fernzugriff auf Kontoinformationen bzw. zur Zahlungsauslösung vorgeschrieben.

[1] Richtlinie (EU) 2015/2366 vom 25. November 2015
[2] Finanzaufsichtsbehörde

Starke Authentifizierung

Die starke Authentifizierung ist ein Mittel für die Authentifizierung des PSU, das auf mindestens zwei der drei folgenden Authentifizierungselemente basiert:

- Besitz (z. B.: ein elektronischer Schlüssel/Token);
- Wissen (z. B.: ein Passwort);
- Inhärenz (z. B.: digitaler Fingerabdruck, biometrisches Element).

Diese Elemente müssen voneinander unabhängig sein, damit durch eine Verletzung der Sicherheit eines Elements die Vertrauenswürdigkeit des anderen Elements nicht beeinträchtigt wird. Die Kombination von zwei dieser Elemente führt zur Erzeugung eines Authentifizierungscodes, der nur einmal akzeptiert wird.
Bei Verwendung einer starken Authentifizierung für die Auslösung von Zahlungen wird der Authentifizierungscode dynamisch mit dem Betrag und dem Zahlungsempfänger verknüpft.
POST Finance bietet mithilfe der LuxTrust-Lösung eine starke Authentifizierung.

Die starke Authentifizierung ist erforderlich, wenn ein PSU (oder ein von ihm bevollmächtigter PISP oder AISP):
- auf sein Online-Zahlungskonto zugreift;
- einen elektronischen Zahlungsvorgang auslöst; oder
- eine Handlung mithilfe eines Fernkommunikationsmittels ausführt, bei der das Risiko eines Zahlungsbetrugs oder einer sonstigen betrügerischen Nutzung besteht.

Unter bestimmten Umständen kann der Zugriff oder das Auslösen von Zahlungsvorgängen jedoch von der starken Authentifizierung ausgenommen sein, z. B.:

- Zugriff auf den Kontostand eines oder mehrerer Zahlungskonten und den Transaktionsverlauf der letzten 90 Tage;
- Auslösung einer Zahlung an einen vertrauenswürdigen Zahlungsempfänger;
- Auslösung einer Zahlung von geringem Wert;
- Auslösung einer Zahlung auf ein eigenes Konto;
- Auslösung einer Zahlung, die als risikoarm gilt.

Neue Akteure

Durch die PSD2 werden im Wesentlichen zwei neue Arten von Akteuren des Zahlungsmarktes (PISP und AISP) eingeführt, die (von der CSSF oder einer anderen zuständigen Behörde der EU) reguliert und überwacht werden. Diese können in Bezug auf Konten der PSU, die bei einem anderen (dann als ASPSP bezeichneten) PSP geführt werden, Zahlungen auslösen oder auf Kontoinformationen zugreifen.
Es handelt sich um Dienstleister, die mit ausdrücklicher und vorheriger Einwilligung des PSU:

- (**PISP**) Zahlungsvorgänge von einem Zahlungskonto auslösen, das bei einer anderen Einrichtung (z. B. Bank) geführt wird; oder
- (**AISP**) Informationen zu einem oder mehreren Zahlungskonten abrufen, das/die bei einer oder mehreren anderen Einrichtungen geführt wird/werden (z. B. Kontoaggregatoren).

Widerruf eines Zahlungsauftrags

Der PSU kann einen Zahlungsauftrag nicht widerrufen, nachdem dieser bei einem PSP eingegangen ist. Wenn der Zahlungsauftrag durch einen PISP oder über den Zahlungsempfänger ausgelöst wird, kann ein PSU den Zahlungsauftrag nicht widerrufen:

- wenn er dem PISP seine Einwilligung in die Auslösung des Zahlungsvorgangs erteilt hat, oder
- nachdem er den Zahlungsauftrag an den Zahlungsempfänger des betreffenden Zahlungsauftrags übermittelt hat, oder
- nachdem er seine Einwilligung zur Ausführung des Zahlungsauftrags direkt an den Zahlungsempfänger des betreffenden Auftrags übermittelt hat.

Haftung bei nicht genehmigten Zahlungsvorgängen

Wenn der Zahlungsvorgang unmittelbar durch den PSU ausgelöst wird und nicht als von dem PSU genehmigt angesehen werden kann – hierin eingeschlossen Fälle, in denen ein PISP in Anspruch genommen wurde –, erstattet der PSP/ASPSP des PSU dem PSU den Betrag des Zahlungsvorgangs unmittelbar nach Kenntnisnahme bzw. nach Benachrichtigung, es sei denn, es liegen gerechtfertigte Gründe für einen Betrugsverdacht vor und er teilt diese Gründe der zuständigen Behörde mit.
Der PSU muss ggf. die Verluste in Zusammenhang mit dem nicht genehmigten Zahlungsvorgang durch Nutzung eines verlorenen, gestohlenen oder missbräuchlich verwendeten Zahlungsinstruments bis zu einer Obergrenze von 50 EUR tragen, es sei denn, der Verlust oder Diebstahl können ihm nicht angelastet werden, oder der ausgelöste Vorgang erfolgte im Rahmen eines Verstoßes gegen die gesetzliche Verpflichtung zur Einrichtung einer starken Authentifizierung durch den PSP/ASPSP. Der PSU ist in jedem Fall verpflichtet, alle Verluste im Zusammenhang mit dem Zahlungsvorgang zu tragen, wenn ein Betrug seinerseits vorliegt.
Sollte der PISP für den nicht genehmigten Zahlungsvorgang verantwortlich sein, hat er den PSP/ASPSP nach den gesetzlichen Bestimmungen zu entschädigen. Der PSU ist in dieses Prozedere nicht involviert, das ausschließlich zwischen dem PISP und dem ASPSP abgewickelt wird.

Haftung bei Nichtausführung, fehlerhafter Ausführung oder verspäteter Ausführung von Zahlungsvorgängen

Wenn der Zahlungsvorgang nicht oder fehlerhaft ausgeführt wurde (einschließlich mit Verspätung) und der PSU den Zahlungsauftrag ausgelöst hat – auch wenn er dafür einen PISP in Anspruch genommen hat –, erstattet der PSP/ASPSP des PSU diesem den Betrag des nicht oder fehlerhaft ausgeführten Zahlungsvorgangs, sofern:

- die Nichtausführung oder fehlerhafte Ausführung nicht auf die Angabe einer falschen eindeutigen Kennung durch den PSU zurückzuführen ist;
- die Nichtausführung oder fehlerhafte Ausführung nicht auf höhere Gewalt zurückzuführen ist; und
- der PSU den PSP/ASPSP über die Nichtausführung oder fehlerhafte Ausführung gemäß den vom PSP/ASPSP eingerichteten Verfahren informiert hat.

Wenn der PSP/ASPSP des PSU nachweist, dass der Zahlungsempfänger des Zahlungsvorgangs die Gelder erhalten hat, haftet indessen der PSP des Zahlungsempfängers.
Sollte der PISP für den nicht oder fehlerhaft ausgeführten Zahlungsvorgang verantwortlich sein, hat er den PSP/ASPSP nach den gesetzlichen Bestimmungen zu entschädigen. Der PSU ist in dieses Prozedere nicht involviert, das ausschließlich zwischen dem PISP und dem ASPSP abgewickelt wird.

Auswirkungen auf Ihre Dienste

Sind die Zahlungsauslöse- und Kontoinformationsdienste neue Dienste?

Nein. Sie haben bereits Zugang zu Zahlungsauslösediensten und Kontoinformationsdiensten, da Sie über das Online-Banking von POST Finance auf Informationen über Ihr POST Finance-Konto zugreifen und Zahlungen auslösen können. Die Neuheit beruht auf der Tatsache, dass nunmehr POST Finance und auch andere regulierte Unternehmen Ihnen diese Zahlungsauslöse- und Kontoinformationsdienste mithilfe der Dienste von LUXHUB in Bezug auf Ihre bei POST Finance und bei anderen ASPSP/TPP geführten Konten anbieten können. Sie müssen jedoch Ihren Zugang zum Online-Banking aktiviert haben, um diese Dienste nutzen zu können, und POST Finance haftet nicht, wenn dies nicht der Fall ist.
Sie können die Zahlungsauslöse- und Kontoinformationsdienste, die von PISP oder AISP bereitgestellt werden, die hierfür in Luxemburg oder einem anderen EU-Mitgliedstaat ordnungsgemäß zugelassen sind, in Zusammenhang mit Ihrem von POST-Finance geführten Konto nutzen.
Sie haben Anspruch auf dasselbe Niveau der Dienste, unabhängig davon, ob Sie diese direkt über Online-Banking von POST Finance oder über AISP/PISP nutzen.

Und was ist mit Ihren Konten, die anderswo geführt werden?

POST Finance bietet Ihnen neue Funktionen zur Aggregation externer Zahlungskonten und zum Auslösen von Zahlungen von diesen Konten an. Sie tritt dann selbst als AISP und/oder PISP auf. Sie können somit zwei neue Dienste nutzen: Zahlungsauslösedienst und Kontoinformationsdienst für Konten, die andere Finanzinstitute für Sie führen. Wenn Sie sich in Ihre Online-Banking-Anwendung von POST Finance einloggen und Ihre Einwilligung hierzu erteilt haben, können Sie Zahlungen von Ihren Zahlungskonten bei einem anderen Finanzinstitut auslösen und Informationen zu Ihren POST Finance-Konten und den Konten des anderen Finanzinstituts abrufen. POST Finance kann ohne Angabe von Gründen beschließen, ein Finanzinstitut von ihrer Liste zu streichen oder den Kontoaggregationsdienst einzustellen. POST Finance kann außerdem den Zugriff ohne Vorankündigung für einen bestimmten Zeitraum aussetzen, um die Funktionen des Kontoaggregationsdienstes zu verbessern und Wartungsarbeiten durchzuführen.
Sie können die Einstellungen jederzeit ändern (Konten Ihrer Wahl anzeigen oder ausblenden, hinzugefügte Finanzinstitute löschen oder den Kontoaggregationsdienst deaktivieren). Eine Liste der betreffenden Finanzinstitute finden Sie in der Online-Banking-Anwendung von POST Finance.