

# DYREKTYWA PSD2 ZWIĘKSZY BEZPIECZEŃSTWO ELEKTRONICZNYCH TRANSAKCJI PŁATNICZYCH [WYWIAD]

---

O tym czym są Third Party Providers i małe instytucje płatnicze, znaczeniu technologii dla ich działalności oraz o dyrektywie PSD2 mówią eksperci EY.

## Czym są Third Party Providers i małe instytucje płatnicze?

Third Party Providers (TPP) zostały zdefiniowane przez Komisję Nadzoru Finansowego (KNF) jako podmioty trzecie, niepodlegające dotychczas nadzorowi ostrożnościowemu, które po spełnieniu wymogów prawnych, będą mogły w imieniu użytkownika usług płatniczych uzyskać dostęp do informacji o jego rachunku (AIS) lub zlecać realizację płatności (PIS). Innymi słowy, są to te podmioty, które po otrzymaniu odpowiedniego statusu np. krajowej instytucji płatniczej (KIP) będą mogły skorzystać z możliwości jakie dają wspomniane usługi PSD2.

Równolegle do rozszerzenia zakresu usług płatniczych, wprowadzono definicję małej instytucji płatniczej (MIP). Interesujące jest to, że powstała ona jako alternatywa do KIP jednak z zastrzeżeniem, że nie może świadczyć nowo dodanych usług PSD2, tj. AIS i PIS. Uzyskanie statusu MIP nie wymaga zezwolenia KNF, a jedynie spełnienia wymagań pozwalających na wpisanie do rejestru dostawców usług płatniczych. MIP jest zatem instytucją płatniczą działającą w ramach zdefiniowanych przez regulatora ograniczeń, świadczącą usługi dotychczas zarezerwowane dla KIP.

## Jakie przepisy prawne regulują ich działalność?

Czynnikiem inicjującym zmiany prawne w Polsce, było wprowadzenie regulacji PSD2 w Unii Europejskiej. Została ona wdrożona do polskiego systemu prawnego w 2018 roku poprzez nowelizację ustawy o usługach płatniczych. To właśnie ta ustawa definiuje dostawców i zakres usług płatniczych jakie mogą świadczyć. Przy czym trzeba pamiętać, że zasady prowadzenia działalności w przypadku niektórych dostawców (np. banków lub oddziałów banków zagranicznych) regulują odnoszące się do nich ustawy sektorowe (np. prawo bankowe).

W ramach aktualizacji ustawy o usługach płatniczych, dodana została również definicja małej instytucji płatniczej, której zakres usług jest odpowiednikiem krajowej instytucji płatniczej z zastosowaniem pewnych ograniczeń. Należą do nich wyłączenie z wspomnianych usług AIS i PIS, funkcjonowanie jedynie na rynku polskim, brak możliwości emisji pieniądza elektronicznego i inwestowania przechowywanych środków.

## Jakie usługi świadczą?

TPP może działać na polskim rynku w ramach m.in. statutów: krajowej instytucji płatniczej - która

może świadczyć obie wspomniane usługi PSD2, "Dostawcy świadczącego wyłącznie usługę dostępu do informacji o rachunku" - co jak sama nazwa wskazuje, ogranicza się do usługi AIS, banku krajowego, czy oddziału banku zagranicznego - które mogą świadczyć zarówno usługę AIS, jak i PIS. TPP otrzymując status KIP nie musi się oczywiście ograniczać do świadczenia usług AIS i PIS, gdyż ustawa zapewnia w tym przypadku dostęp do pełnego zestaw usług płatniczych, które były zdefiniowane w ustawie jeszcze przed jej nowelizacją.

Przykładowymi KIP w Polsce są takie firmy jak First Data, Blue Media czy PayU. Niestety, na moment publikacji tego materiału, nie ma w rejestrze KNF i EBA żadnego podmiotu zarejestrowanego w Polsce dla usług PIS i AIS. Wiadomo jednak, że część obecnie zarejestrowanych KIP wystąpiła do KNF o zmianę zezwolenia celem dodania usług PIS i AIS do swojego katalogu i już niebawem powinny pojawić się w rejestrze.

Mała instytucja płatnicza, jako ta, która została wyłączona z usług PSD2, otrzymała możliwość świadczenia pełnego zestawu dotychczas zarezerwowanych dla KIP usług, tj. usługi przekazu pieniężnego, rozliczania i autoryzacji płatności, wydawania instrumentów płatniczych, realizacji transakcji płatniczych objętych linią kredytową, poleceń przelewu i zapłaty, transakcji kartą płatniczą oraz usług umożliwiających wpłatę i wypłatę środków z rachunku płatniczego.

### **Jaka jest różnica między nimi a ich większymi odpowiednikami (np. bankami)?**

Przede wszystkim działalność banków krajowych lub oddziałów banków zagranicznych jest uregulowana niezależną ustawą sektorową, która „domyślnie” zalicza świadczenie usług płatniczych (m.in. AIS i PIS) do czynności przez nie wykonywanych. Wydaje się więc, że podmioty te mają lepszą pozycję, jeżeli chodzi o możliwość skorzystania z usług AIS i PIS. W tym przypadku może być ewentualnie wymagana zmiana statutu banku krajowego lub regulaminu oddziału banku zagranicznego zatwierdzona przez KNF, o ile świadczenie usług AIS lub PIS nie było objęte przedmiot działania i zakresem działalności banku krajowego lub oddziału banku zagranicznego. Bank może zostać agregatorem danych z innych banków (usługa AIS) oraz inicjować przelewy z rachunków innych banków w Polsce (usługa PIS). Staje się wtedy głównym kanałem obsługi finansów użytkownika posiadającego rachunki w wielu bankach.

### **Kto jest ich głównym klientem?**

W przypadku TPP, klientami mogą być zarówno osoby fizyczne jak i przedsiębiorstwa. Na przykładzie rynków zagranicznych najbardziej popularnymi usługami świadczonymi w oparciu o AIS i PIS są usługi zarządzania finansami (narzędzia agregujące wydatki i pomagające w zarządzaniu budżetem domowym), platformy do realizacji płatności (np. automatyzacja procesu opłat mieszkaniowych), czy narzędzia wymiany danych pomiędzy systemami. W tym ostatnim przypadku, TPP oferują komponent typu "plug and play" pozwalający na wykorzystanie danych bankowych bez konieczności budowy i utrzymania infrastruktury zapewniającej odpowiednie połączenie z interfejsami (API) banków.

Zupełnie inna sytuacja jest w przypadku MIP. Na koniec kwietnia 2019, widniały w rejestrze 22 podmioty, których profile działalności znacznie się między sobą różnią i należą do takich sektorów jak IT, reklama, handel czy telekomunikacja. Niektóre z tych firm wskazują uzyskanie statusu MIP jako element wzmocnienia wizerunku obecnie świadczonych usług, inne jako weryfikacja nowego modelu biznesowego i próby swoich sił na rynku płatności w ograniczonym, ale łatwiejszym do uzyskania statusie.

### **Jaką rolę w ich działaniu odgrywa technologia?**

Dyrektywa PSD2, jak i sama ustawa o usługach płatniczych ją implementująca, odnoszą się do tego

kto i jakie usługi może świadczyć. Nie odpowiadają jednak na pytanie, jak technicznie ma być realizowany transfer danych i jakimi metodami TPP powinny się uwierzytelniać, aby uzyskać do nich dostęp. Rozwiązania w tym zakresie zawierają "Regulacyjne Standardy Techniczne" (RTS) przyjęte w postaci rozporządzenia Komisji Europejskiej, które określają ramy wzajemnej komunikacji i uwierzytelniania. RTS nie definiują jednak szczegółów technologicznych takich jak struktura i format danych, czy architektura interfejsu. Te pozostały w gestii banków.

Powstały jednak w Europie grupy robocze, które postawiły sobie za cel, stworzenie standardów międzybankowych. Polską inicjatywą w tym zakresie jest grupa robocza o nazwie "Polish API", której uczestnikami są Związek Banków Polskich wraz ze stowarzyszonymi bankami komercyjnymi i spółdzielczymi, Spółdzielcze Kasy Oszczędnościowo-Kredytowe, Polska Organizacja Nie bankowych Instytucji Płatności wraz ze stowarzyszonymi firmami, Polska Izba Informatyki i Telekomunikacji, Polska Izba Ubezpieczeń, Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej, Polski Standard Płatności. W tym przypadku, grupa postawiła na format wiadomości JSON z kodowaniem UTF-8, specyfikując dokładnie format danych dla komunikatu.

### **Czy ich usługi są bezpieczne? W jaki sposób takie instytucje chronią się przed zagrożeniami?**

Sam fakt uregulowania działalności TPP oraz otwartych standardów komunikacji zwiększa bezpieczeństwo i zaufanie do świadczonych przez strony trzecie usług. Pomimo jednak, że RTS dopuszczają komunikację pomiędzy TPP a dostawcą usług płatniczych prowadzącego rachunek (ASPSP) z wykorzystaniem zarówno dedykowanego interfejsu (tzw. API), jak i odpowiednio zmodyfikowanego interfejsu udostępnionego użytkownikowi przez ASPSP (tzw. screen scraping plus), KNF uznał pierwszy interfejs za bezpieczniejszy i preferowany – komunikat UKNF z dnia 12 stycznia 2018 r. dot. wybranych oczekiwań nadzorczych w odniesieniu do okresu przejściowego związanego z implementacją Dyrektywy PSD2. KNF określił również wymogi związane z wykorzystywaniem drugiego z interfejsów na potrzeby tzw. opcji fallback – komunikat UKNF z dnia 1 lipca 2019 r. w sprawie zwolnienia z tzw. opcji fallback.

TPP poza faktem bycia podmiotem podlegającym nadzorowi KNF, musi dysponować odpowiednim kwalifikowanym certyfikatem pieczęci lub kwalifikowanym certyfikatem uwierzytelnienia witryn internetowych pozwalającym mu zidentyfikować się w momencie uzyskiwania dostępu do rachunku płatniczego m.in. w zakresie roli (AISP, PISP) oraz zezwoleniem udzielonym przez użytkownika. Operuje on również w ramach dedykowanego dla niego interfejsu bezpośredniego dostępu do rachunku płatniczego użytkownika.

Również sam właściciel rachunku płatniczego (w większości przypadków bank) musi zapewnić bezpieczny kanał komunikacji do realizacji usług AIS i PIS, w tym przeprowadzić procedury uwierzytelniające TPP.

Dyrektywa PSD2, jak i ustawa o usługach płatniczych ją implementująca, wprowadzają również pojęcie silnego uwierzytelniania dla dostępu do rachunku on-line, inicjacji elektronicznej transakcji płatniczej oraz przeprowadzania czynności za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć. Silne uwierzytelnianie wymusza zastosowanie co najmniej dwóch elementów z trzech należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik). Niemniej jednak nie zawsze będzie istniał obowiązek stosowania silnego uwierzytelniania, gdyż RTS przewiduje wyłączenia w tym zakresie.

Wywiadu udzieli:

Łukasz Kąpielewski, Menedżer, EY

Marcin Grott, Radca prawny, EY

Wywiad został przeprowadzony podczas konferencji FinTech & InsurTech Digital Congress