Dyrektywa PSD2 i zmiany w obrocie pieniądzem elektronicznym z perspektywy konsumenta

Krzysztof Stępień

WSTĘP

Jednym z głównych celów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego[1] (*Payment Services Directive 2,* dalej: „**PSD2**") jest wprowadzenie odpowiednich standardów bezpieczeństwa i procedur kontroli zapobiegających nadużyciom ze strony banków oraz kradzieżom elektronicznych środków płatniczych czy też danych rachunków i ich właścicieli.

Na wstępie należy wyjaśnić, dlaczego projekt PSD2 został wniesiony pod obrady Parlamentu Europejskiego. Poprzednio obowiązująca dyrektywa w sprawie usług płatniczych w ramach rynku wewnętrznego z dnia 13 listopada 2007 r.[2] (*Payment Services Directive 1,* dalej: „**PSD1**") była pierwszym tak kompleksowym unijnym ujęciem regulującym bezpieczeństwo w bankach i instytucjach płatniczych. Podobnie polska ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (dalej: „**UUP**")[3] implementująca tę dyrektywę była pierwszą ustawą w polskim systemie prawnym, której celem było uregulowanie zagadnień związanych z płatnościami bezgotówkowymi. Wprowadziła jednolite zasady dokonywania płatności bezgotówkowych w ramach rynku europejskiego, jak chociażby terminy uznawania rachunków bankowych czy odpowiedzialność przy płatnościach kartami debetowymi i kredytowymi, co miało zapewnić równy dostęp do rynku usług płatniczych. Konieczne było także ujęcie nowych regulacji dotyczących rozwiązań technologicznych dostosowanych do wielu rodzajów metod i form płatności elektronicznych. Trzecim ważnym postulatem PSD1 było zapewnienie odpowiedniego nadzoru nad podmiotami obsługującymi transakcje płatnicze. Zgodnie z przyjętymi regulacjami wszystkie podmioty rynku płatniczego podlegają nadzorowi Komisji Nadzoru Finansowego (**KNF**), który w zależności od skali oraz rodzaju działalności gospodarczej przedsiębiorstwa prowadzonej w związku z płatnościami elektronicznymi może przybierać różne formy (np. zakres kontroli KNF nad bankami jest bardzo szeroki, a w przypadku instytucji płatniczych ogranicza się do podstawowych aspektów działalności). W praktyce spowodowało to, że wiele podmiotów z branży usług technologicznych i start-upów zaczęło podlegać nadzorowi KNF.

---

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG).

[2] Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Tekst mający znaczenie dla EOG).

[3] Tekst jedn.: Dz. U. 2019 poz 659 z późn. zm.

Krótko po zaimplementowaniu PSD1 w ustawodawstwach państw członkowskich w środowisku biznesu zaczęto zauważać, że dyrektywa przestaje być aktualna w stosunku do stanu wiedzy i rozwoju technologii. Co więcej, postanowienia PSD1 zobowiązały Komisję Europejską do przeglądu jej realizacji do 1 listopada 2012 roku, a wyniki tego przeglądu wywołały dyskusję na temat skuteczności dyrektywy w stosunku do nowych usług elektronicznych na rynku płatniczym. W związku z powyższym Komisja Europejska we współpracy z innymi instytucjami UE oraz państwami członkowskimi przystąpiła do rewizji PSD1 w celu opracowania projektu nowej dyrektywy, która miała być dostosowana do szybkiego rozwoju technologii na rynku finansowym.

W grudniu 2015 roku Europejski Urząd Nadzoru Bankowego (**EBA** – *European Banking Authority*) opublikował tzw. *Discussion Paper*, którego celem było przedstawienie projektu nowej dyrektywy i poddanie go publicznej debacie. EBA rozpowszechniało dokument na wielu konferencjach w obrębie Unii Europejskiej, aby zyskać jak najwięcej opinii i wskazówek co do potrzeb zainteresowanych podmiotów. Ze strony branży padła rekordowa liczba odpowiedzi na *Discussion Paper* – dotyczyły one łącznie ok. 300 różnych, nierzadko sprzecznych z sobą, zagadnień i wniosków o doprecyzowanie. PSD2 okazało się dla świata finansowego jednym z najbardziej dyskutowanych i wzbudzających największe zainteresowanie tematów w ostatnich latach.

Nowa dyrektywa PSD2 została uchwalona pod koniec 2015 r. W Polsce jej regulacje zaimplementowano do krajowego porządku prawnego ustawą z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz. U. 2018 poz. 1075), obowiązującą od 20 czerwca 2018 r., mimo że większość przepisów PSD2 weszła w życie 13 stycznia 2018 r. Niektóre z nich, w szczególności przepisy o standardach i procedurach bezpieczeństwa, wejdą w życie dopiero we wrześniu 2019 r. z uwagi na trwającą w czasie uchwalania PSD2 dyskusję na temat *Regulatory Technical Standards*(**RTS**), czyli rozporządzeń dotyczących technicznych standardów, które powinny spełniać systemy obsługujące transakcje płatnicze w UE[4]. Z tego względu banki i instytucje płatnicze mają czas na wdrożenie rozwiązań w dziedzinie bezpieczeństwa przyjętych w RTS do 14 września 2019 r.

GŁÓWNE ZAŁOŻENIA PSD2

Jednym z kluczowych celów PSD2 jest uregulowanie nowych usług płatniczych, które rozwinęły się w ciągu ostatnich kilku lat. Szczególnie ważne było wprowadzenie przez UE ram regulacyjnych dla dostawców usług informacji o rachunkach (**AISP** –*Account Information Service Provider*) i dostawców usług inicjowania płatności (**PISP** –*PaymentInitiation Service Provider*), którzy

[4]Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Tekst mający znaczenie dla EOG).

korzystają z infrastruktury rachunków płatniczych dostawców usług płatniczych obsługujących rachunki (głównie banki), w celu uzyskiwania niezbędnego dostępu do kont klientów.

W ramach tej regulacji UE wprowadziła między innymi:

- definicje usług informacji o rachunkach i usług inicjowania płatności odpowiednio w art. 4 ust. 15 i ust. 16 PSD2;
- licencjonowanie PISP i ich rejestrację;
- zasady postępowania dla dostawców usług płatniczych, które mają na celu zapewnienie niedyskryminacyjnego (bezpłatnego) dostępu do rachunków przez AISP i PISP;
- wymagane zasady dotyczące *Account Payment Interface* (**API**) w celu zapewnienia dostępności kont użytkowników oraz wysokiego stopnia bezpieczeństwa IT (regulowane głównie przez art. 30 i nast. RTS);
- obowiązek dostawcy usług płatniczych zezwolenia dostawcom usług informacji o rachunkach i usług inicjowania płatności na korzystanie z procedury uwierzytelniania klientów banku;
- możliwość pojawienia się na rynku tzw. małej instytucji płatniczej, celem zniesienia monopolu bankowego i wprowadzenia innowacji produktowych w usługach bankowych i płatniczych. Mała instytucja płatnicza będzie mogła prowadzić rachunki płatnicze, obsługiwać transakcje na ściśle określoną skalę, a nawet wydawać karty lub oferować płatności mobilne. Dyrektywa dopuszcza też możliwość deponowania środków w małych instytucjach płatniczych, lecz tylko do 2 tys. euro;
- ułatwienia dla innych podmiotów, które mogą pośredniczyć w usługach finansowych – tzw. *Third Party Provider* (TPP). Dla przeciętnego konsumenta to przede wszystkim podmioty takie jak PayU czy PayPal. Obecnie już mało kto w Polsce, robiąc zakupy w sklepie internetowym, nie korzysta z usługi inicjowania płatności – czyli po prostu szybkiego przelewu *pay-by-link*, Blika czy innych podobnych form płatności. Tym samym jako klienci zgadzamy się, aby pośrednik w płatnościach (np. PayU) uzyskiwał od naszego banku dane dotyczące środków na naszym koncie w celu upewnienia się, że jesteśmy w stanie zapłacić za dokonane zakupy;
- rozszerzenie praw konsumenta m.in. co do reklamacji, odpowiedzialności przy kradzieży karty i wypowiedzenia umowy z bankiem.

Najbardziej odczuwalne dla klienta będą zmiany dotyczące transakcji płatniczych, dlatego druga część artykułu będzie dotyczyć regulacji związanych z kwestiami bezpieczeństwa i procedurami dokonywania płatności elektronicznych przez osoby fizyczne, wchodzących w życie 14 września 2019 r., oraz praw konsumentów, których rozszerzenie weszło w życie 20 grudnia 2018 r.

PSD2 I ZMIANY DLA KONSUMENTA

1. Silne uwierzytelnianie

Dzięki PSD2 konsumenci będą znacznie lepiej chronieni podczas wykonywania płatności elektronicznych lub przekazów pieniężnych, takich jak transakcje bezgotówkowe czy zakupy *online*. Silne uwierzytelnienie klienta (**SCA** – *Strong Client Authorisation*) stanie się podstawą uzyskania przez użytkownika większości usług bankowości elektronicznej, w tym dostępu do rachunku płatniczego i dokonywania płatności *online*.

Oznacza to, że aby zostać zidentyfikowanym przez system zabezpieczeń, użytkownik będzie musiał dostarczyć co najmniej dwa niezależne od siebie elementy weryfikacyjne z trzech określonych w dyrektywie:

- coś, co zna tylko zindywidualizowany użytkownik (hasło, kod PIN etc.);
- coś, co posiada tylko zindywidualizowany użytkownik (karta, telefon komórkowy, pager etc.); lub
- coś, czym jest tylko zindywidualizowany użytkownik (odcisk palca, skan tęczówki).

Z tego względu po 14 września 2019 r. bank wymusi na kliencie zalogowanie do konta w bankowości elektronicznej z użyciem minimum dwóch z trzech składników wymienionych powyżej. Silne uwierzytelnianie klientów jest już powszechnie stosowane w ograniczonym zakresie w całej UE. Na przykład gdy klienci płacą kartą w sklepach stacjonarnych, muszą potwierdzić transakcję poprzez wpisanie kodu PIN w czytnikach kart. Nie dotyczy to jednak np. elektronicznych transakcji typu *paypass*– w tym przypadku silne uwierzytelnianie użytkownika jest stosowane tylko w niektórych krajach UE (w tym w Belgii, Holandii i Szwecji). W innych krajach UE niektórzy dostawcy usług płatniczych stosują SCA na zasadzie dobrowolności lub w przypadkach transakcji szczególnych, np. powyżej określonej kwoty.

Rozporządzenie *Regulatory Technical Standards* wymaga, żeby silne uwierzytelnienie klienta było używane do uzyskiwania dostępu do własnego rachunku płatniczego i dokonywania płatności *online*. Banki i inni dostawcy usług płatniczych będą musiały zbudować niezbędną infrastrukturę dla procesu SCA, a także poprawić scenariusze wyłudzeń i oszustw. Konsumenci i kupcy będą musieli być wyposażeni w systemy weryfikacji i zostać przeszkoleni z ich obsługi, aby móc działać w środowisku SCA – wszystko za sprawą nowych przepisów dotyczących bezpieczeństwa transakcji[5].

Można przewidywać, że początkowo zmiany wywołane wdrożeniem PSD2 w bankach spotkają się z niechęcią klientów – proces logowania i zlecania płatności stanie się bezpieczniejszy, ale przez to też bardziej złożony i dłuższy. Mimo to w dalszej perspektywie modyfikacje te niewątpliwie przyczynią się do ochrony konsumenta poprzez minimalizację liczby transakcji oszukańczych

[5]Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC.

oraz transakcji uwierzytelnionych z wykorzystaniem danych skradzionych, przywłaszczonych lub wykorzystanych niezgodnie z przeznaczeniem lub bez zgody klienta.

Obecnie wiele banków wysyła kody potwierdzenia transakcji w wiadomościach SMS. Telefon stanowi element weryfikacyjny posiadany przez zindywidualizowanego użytkownika (właściciela rachunku), dlatego wydawałoby się, że ten sposób będzie odpowiadał wymogom PSD2, jednak zgodnie z postanowieniami zawartymi w RTS w wiadomości SMS musiałyby się znajdować szczegóły dotyczące transakcji, takie jak np. wysokość przekazywanej kwoty czy odbiorca. Wszystkie te dane powinny być odpowiednio zabezpieczone, żeby nie zostały celowo lub przypadkiem zmienione, niestety SMS-y nie spełniają tego warunku, gdyż ich treść nie podlega ochronie i nie jest poufna. W związku z tym wiele banków będzie musiało przeanalizować standardowe sposoby potwierdzania transakcji i wprowadzić nowe rozwiązania, na które pozwala dyrektywa PSD2.

Zgodnie z PSD2 w transakcjach zbliżeniowych kod PIN musi być podany albo od kwoty 150 euro, albo co min. 5 transakcji (wybór jednej z tych opcji należy do wydawcy karty)[6]. Transakcje kartą w samoobsługowych automatach parkingowych i transportowych (autostrady, bilety autobusowe, kolejowe etc.) są zwolnione z obowiązku podawania kodu PIN.

2. Bezpieczna komunikacja

PSD2 formułuje ogólne ramy dla nowych usług związanych z rachunkami płatniczymi konsumentów, takimi jak tzw. usługi inicjowania płatności i usługi informacji o rachunkach. W tym kontekście *Regulatory Technical Standards* określają wymagania dotyczące powszechnych i bezpiecznych standardów komunikacji między bankami, podmiotami trzecimi świadczącymi usługi związane z płatnościami i użytkownikami[7].

Konsumenci i firmy będą mogły udzielać dostępu do swoich danych płatniczych *Third Party Providers*, którymi są na przykład dostawcy usług inicjowania płatności (PISP) i dostawcy informacji o kontach (AISP). TPP mogą być firmy z sektora FinTech, a także inne banki czy instytucje płatnicze[8]. Klienci będą musieli wyrazić zgodę na dostęp, wykorzystanie i przetwarzanie swoich danych, a TPP nie będą mieć dostępu do innych danych z rachunku płatniczego niż te, na których przetwarzanie wyrażono zgodę.

RTS reguluje podstawowe zasady korzystania z procedury silnego uwierzytelniania klienta w ramach transakcji płatniczych, dlatego liczba nieudanych prób uwierzytelnienia jest ograniczona do pięciu. Jeśli użytkownik nieskutecznie wykona całą procedurę uwierzytelniania pięć razy, konto powinno zostać tymczasowo lub na stałe zablokowane. Ponadto maksymalny czas bez jakiejkolwiek

[6]Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Tekst mający znaczenia dla EOG).
[7]Raport „Wszystko o PSD2", Deloitte.
[8]https://www.spidersweb.pl/2018/04/psd2-czyli-koniec-z-monopolem-bankow.html.

działalności użytkownika po zalogowaniu na konto internetowe jest ograniczony do pięciu minut liczonych od momentu pomyślnego zakończenia procedury uwierzytelniania.

3. *Screenscraping*

Dyrektywa PSD2 zabrania zewnętrznym dostawcom usług dostępu do jakichkolwiek innych danych z rachunku płatniczego klienta poza tymi, na których przetwarzanie mają jego wyraźną zgodę. Dzięki nowym regułom nie będzie już można uzyskać dostępu do danych klienta za pomocą tzw. *screen scrapingu* – czyli za pośrednictwem interfejsu klienta z wykorzystaniem poświadczeń bezpieczeństwa wykorzystywanych w innych programie użytkownika. Wspomniana technika pozwala dostawcom TPP uzyskać dostęp do danych klienta bez konieczności jego dalszej identyfikacji.

Ta praktyka będzie musiała odejść w zapomnienie, a banki będą zmuszone wdrożyć kanał komunikacyjny, który umożliwi dostawcom usług internetowych dostęp do danych, których potrzebują, zgodnie z PSD2. Kanał będzie wykorzystywany także do umożliwienia bankom i TPP identyfikowania się nawzajem podczas uzyskiwania dostępu do tych danych. Pozwoli również na komunikowanie się przez cały czas za pośrednictwem bezpiecznych wiadomości[9].

4. Zgoda konsumenta

Aby sprawdzić, czy TPP jest zweryfikowanym podmiotem świadczącym usługi płatnicze, dostawca usług płatniczych musi zbadać, czy użytkownik wyraził zgodę na świadczenie tych usług przez każde TPP. Zasadniczo zgoda wyrażona przez użytkownika zachowuje ważność do czasu jej cofnięcia, więc niezależnie od jej warunków w PSD2 i RTS jest ważna i dostawca usług płatniczych ma prawo zezwolić TPP na wykonanie płatności[10].

Zgodnie z art. 40 UUP transakcja płatnicza może być autoryzowana za pomocą wyraźnej zgody użytkownika wyrażonej zgodnie z umową między użytkownikiem a dostawcą usług płatniczych. Paragraf 2 tego artykułu stanowi, że zgoda powinna być wyrażona przed transakcją, chyba że użytkownik i dostawca usług płatniczych zgodzili się, że można ją wyrazić również po niej.

Zgoda może być udzielona TPP w celu świadczenia usług inicjowania płatności, w tym cyklicznego transferu lub przesłania pytania dotyczącego bieżącej transakcji po zainicjowaniu. Zgodnie z art. 64 ust. 3 PSD2 zgoda może zostać cofnięta przez płatnika w dowolnym momencie, ale nie później niż w chwili nieodwołalności zgodnie z art. 80 UUP (ustawa o usługach płatniczych), czyli po udzieleniu dostawcy usługi inicjowania płatności zgody na rozpoczęcie transakcji płatniczej lub po udzieleniu zgody na wykonanie transakcji płatniczej. Ponadto warto wspomnieć, że wszystkie podmioty trzecie prowadzące działalność gospodarczą w Polsce muszą być zarejestrowane w rejestrze KNF. Z tego powodu, w celu zweryfikowania firmy przed udzieleniem

[9]https://www.bbva.com/en/everything-need-know-psd2/.
[10]Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC.

zgody, warto sprawdzić, czy TPP, której chcemy udzielić zgody na przetwarzanie danych dotyczących rachunku bankowego, znajduje się w odpowiednim rejestrze.

5. Rozszerzenie uprawnień konsumentów

Zasadnicza zmiana nastąpiła w przypadku reklamowania konkretnej płatności, która w odczuciu konsumenta nie miała miejsca lub nie została autoryzowana przez właściciela rachunku. W takich przypadkach reklamowana kwota będzie musiała wrócić na konto płatnika najpóźniej w dniu roboczym następującym po rozpatrzeniu reklamacji, o ile nie ma wyraźnych oznak, że jest to próba wyłudzenia czy oszustwa. Co więcej, to po stronie usługodawcy (czyli najczęściej banku) będzie leżało udowodnienie, że reklamacja jest bezzasadna. Termin rozpatrywania reklamacji skróci się z 30 do 15 dni. W szczególnych przypadkach termin na udzielenie ostatecznej odpowiedzi będzie mógł być wydłużony do 35 dni, ale przy należytym uzasadnieniu opóźnienia.[11]

Zmianie ulega również maksymalna kwota, do której użytkownik ponosi odpowiedzialność, jeżeli ktoś ukradnie mu kartę i wykona nią transakcje. Dotychczas odpowiedzialność klienta ustawiona była w wysokości 150 euro, teraz zostanie zmniejszona do 50 euro – ta granica była już wprowadzona w niektórych bankach (Alior Bank, mBank) przed grudniem 2018 r. Natomiast jeżeli konsument nie mógł mieć świadomości, że został okradziony, to nie powinien w ogóle ponosić odpowiedzialności (jeśli jednak jego zamiary były nieuczciwe lub dopuścił się rażącego niedbalstwa, może nie być chroniony dopuszczalnym limitem). Dyrektywa sankcjonuje również od dawna stosowane w Polsce i innych krajach UE rozwiązanie polegające na tym, że od momentu zgłoszenia utraty karty bankowi klient nie ponosi odpowiedzialności za wykonane nią transakcje[12].

Unia Europejska stwarza ponadto warunki, aby konsumenci banków byli bardziej mobilni i mogli łatwiej zmienić bank – ma temu służyć zagwarantowanie bezpłatnego wypowiedzenia umowy ramowej z bankiem. Jedynym wyjątkiem jest pierwsze półrocze – przed upływem sześciu miesięcy bank może nałożyć na klienta opłaty odpowiadające kosztom poniesionym w związku z wypowiedzeniem umowy. Maksymalny okres wypowiedzenia umowy ramowej dla konsumenta będzie wynosił jeden miesiąc, a dla banku – nie mniej niż dwa miesiące. Twórcy projektu uznali, że to klient jest stroną słabszą i to jego interesy trzeba chronić mocniej[13].

Dyrektywa wprowadza też restrykcje w stosunku do transakcji, w których ostateczna kwota nie jest znana w momencie płatności kartą. Od 14 września 2019 r. środki potrzebne do opłacenia transakcji zgodnie z ceną naliczoną przez sprzedającego będą mogły zostać ściągnięte z konta konsumenta dopiero w momencie, w którym klient zgodzi się na zablokowanie na jego koncie wskazanej konkretnie kwoty.

---

[11]Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Tekst mający znaczenia dla EOG).
[12]Raport „Wszystko o PSD2", Deloitte.
[13]https://www.forbes.pl/gospodarka/dyrektywa-psd2-co-zmieni-w-bankowosci-nowe-zasady-dla-sklepow/omvd4fw.

6. Transakcje międzywalutowe

Przepisem umieszczonym w zasadzie tylko dla formalności jest obowiązek wykonywania przez banki i instytucje płatnicze maksymalnie w ciągu jednego dnia roboczego przelewów i przekazów pieniężnych wyrażonych w euro lub w pozostałych walutach państw członkowskich UE, innych niż obowiązująca w państwie siedziby banku. Konsument ma być dokładnie informowany o kursie walutowym oraz o wszystkich rzeczywistych kosztach i opłatach związanych z transakcją bezpośrednio przed jej autoryzacją. Powyższa zasada dotyczy także bankomatów – zabroniona będzie praktyka przewalutowania środków konsumenta według niekorzystnej dla klienta waluty, tak jak to miało miejsce w przypadku wypłacania środków z bankomatu w innym państwie UE, gdy niektóre banki dokonywały podwójnego przewalutowania, podwyższając koszt transakcji dla konsumenta. Dodatkowo na terenie Europejskiego Obszaru Gospodarczego (EOG) przy realizowaniu transakcji będzie dostępny tylko jeden sposób pokrycia kosztów przelewu – opcja SHA (od *sharing*), polegająca na podziale kosztów między obie strony stosownie do kosztów wskazanych w bankach stron transakcji, tzn. nadawca płaci w swoim banku za koszty związane z nadaniem przelewu, a odbiorca opłaca koszty związane z jego odebraniem (jeśli się pojawiają).[14]

W ustawie o usługach płatniczych z 11 sierpnia 2018 r. w ramach implementacji dyrektywy PSD2 został dodany dział IIA „Bezpieczeństwo świadczenia usług płatniczych", w którym zawarto przepisy nakazujące wszystkim uczestnikom transakcji (TPP, bankom, instytucjom płatniczym, dostawcom usług płatniczych) udowodnienie, że stosują właściwe środki bezpieczeństwa, w celu zapewnienia odpowiedniego zabezpieczenia płatności oraz corocznego przekazywania KNF kompleksowej oceny bezpieczeństwa usług płatniczych.

WNIOSKI

Tzw. *Open Banking*, który został wprowadzony przez dyrektywę PSD2 w szerokim zakresie, umożliwia firmom technologicznym przeprowadzenie bezpośredniej płatności z konta bankowego klienta. Dziś przykładowo firma PayU, która chce przeprowadzić płatność za zakupy w Internecie, na zlecenie użytkownika oferuje płatności *pay-by-link*, czyli przekierowuje go do banku, żeby tam się zalogował i zapłacił. Pod rządami PSD2 nie będzie trzeba przekierowywać klienta do banku, bo pośrednik będzie mógł sam się podłączyć do jego konta i po autentykacji klienta przeprowadzić płatność.[15]

Ta część PSD2 otwiera wielkie pole firmom technologicznym, takim jak Facebook czy Google. Facebook uruchomił już w Wielkiej Brytanii usługę Pay by Messenger (czyli płatności przez komunikator), zaś Google umożliwia płacenie przez Google Wallet, czyli usługę pozwalającą

[14]https://www.forbes.pl/gospodarka/dyrektywa-psd2-co-zmieni-w-bankowosci-nowe-zasady-dla-sklepow/omvd4fw.
[15]https://biznes.gazetaprawna.pl/artykuly/1115714,fintechy-kontra-banki-wdrozenie-dyrektywy-psd2.html.

wysyłać płatności za pośrednictwem poczty elektronicznej. Facebook zamierza też uruchomić płatności przez WhatsApp.

Zamiast logowań, przekierowań do banku, podpinania kart do e-portmonetek etc. będzie można po prostu wpisać „+20 zł" na czacie i pieniądze zostaną wysłane do wskazanej osoby. Facebook połączy się z bankami nadawcy i odbiorcy i przeprowadzi płatność. Będzie można więc płacić bez wchodzenia do banku. Takie strony jak Allegro, AliExpress czy Amazon nie będą potrzebowały pośredników do przeprowadzania płatności – teoretycznie będą mogły same pobierać pieniądze z kont klientów. Nie wiemy jeszcze, jak dokładnie będzie wyglądać ta funkcja, ale z uwagi na zmieniające się przepisy dyrektywy oraz rozporządzenia RTS jej powstanie jest nieuchronne.

Tymczasem Komisja Europejska jest zobowiązana do tego, żeby 13 stycznia 2021 r. przedstawić raport z przeglądu dyrektywy PSD2 i zaproponować PSD3, jeśli ujawni on nieadekwatność rozwiązań PSD2 do zmian na rynku. Oznacza to, że pod koniec 2019 roku rozpoczną się prace w tym kierunku. Jeśli aktualne światowe trendy regulacyjne się utrzymają, niewątpliwie w ramach przeglądu rozważone zostanie umożliwienie dostawcom niebankowym przyjmowania depozytów w ograniczonym zakresie (tak między innymi zrobiła ostatnio Szwajcaria) oraz otwarcie systemów płatności na uczestnictwo tych podmiotów (Wielka Brytania i Litwa). Otworzy to drogę do pełnoprawnego konkurowania innowacyjnych podmiotów z sektora płatniczego z bankami o *daily banking*, czyli obsługę codziennych wydatków, pozostawiając bankom monopol na *life-long banking* (depozyty wysokokwotowe, hipoteki).

WYKAZ SKRÓTÓW:

AISP (*Account Information Service Provider)* – dostawca usług informacji o rachunkach

API (*AccountPayment Interface)* – system zdalnej obsługi rachunku bankowego za pomocą urządzeń elektronicznych.

EBA (*European Bank Authority*) – unijny bankowy organ nadzorczy

EOG – Europejski Obszar Gospodarczy

KNF – Komisja Nadzoru Finansowego

PISP (*PaymentInitiation Service Provider)*– dostawca usług inicjowania płatności

PSD1 – Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (tekst mający znaczenie dla EOG)

PSD2 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (tekst mający znaczenie dla EOG)

RTS *(Regulatory Technical Standards)*– rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (tekst mający znaczenie dla EOG)

SCA (*Strong Client Authentication*) – procedura służąca precyzyjnej i wiarygodnej weryfikacji użytkownika rachunku płatniczego

TPP (*Third Party Provider*) – podmiot trzeci niebędący bankiem, który prowadzi działalność gospodarczą związaną z usługami płatniczymi

UUP – ustawa o usługach płatniczych z dnia 19 sierpnia 2011 r. (Dz. U. z 2019 poz. 639)

ŹRÓDŁA:

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG).
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2007/64/EC z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Tekst mający znaczenie dla EOG).
3. Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Tekst mający znaczenia dla EOG).
4. Ustawa o usługach płatniczych z dnia 19 sierpnia 2011 (Dz. U. z 2019 poz. 639).
5. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC.
6. https://www.karierawfinansach.pl/artykul/wiadomosci/dyrektywa-psd-2-wszystko-co-powinniscie-o-niej-wiedziec.
7. https://www.spidersweb.pl/2018/04/psd2-czyli-koniec-z-monopolem-bankow.html.
8. https://www.bbva.com/en/everything-need-know-psd2/.
9. https://www.forbes.pl/gospodarka/dyrektywa-psd2-co-zmieni-w-bankowosci-nowe-zasady-dla-sklepow/omvd4fw.
10. https://biznes.gazetaprawna.pl/artykuly/1115714,fintechy-kontra-banki-wdrozenie-dyrektywy-psd2.html.
11. Raport „Wszystko o PSD2", Deloitte.

[Artykuł został przygotowany w ramach działalności w Komitecie Prawnym ELSA Poland]