BEZPIECZEŃSTWO USŁUG OPARTYCH O OTWARTE INTERFEJSY PROGRAMISTYCZNE (API) W KONTEKŚCIE IMPLEMENTACJI DYREKTYWY PSD2

RAPORT ANALITYCZNY

SYGN. WIB PAB 2020/3

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

PROGRAM ANALITYCZNO BADAWCZY

Warszawa, 10.02.2020

PROGRAM ANALITYCZNO BADAWCZY

O Raporcie

Raport **Bezpieczeństwo usług opartych o otwarte interfejsy programistyczne (API) w kontekście implementacji Dyrektywy PSD 2** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy:

Raport przygotowany przez zespół w składzie:

Maciej Kostro – doradca zarządu Związku Banków Polskich, autor koncepcji badań i raportu
Piotr Sterczała – członek zarządu Obserwatorium.biz sp. z o.o.
dr Miłosz Brakoniecki – członek zarządu Obserwatorium.biz sp. z o.o.
Michał Tabor – członek zarządu Obserwatorium.biz sp. z o.o.
Dominika Rzęsa – analityk Obserwatorium.biz sp. z o.o.
Marcin Żywicki – analityk Obserwatorium.biz sp. z o.o.
Marcin Wolski – ekspert Obserwatorium.biz sp. z o.o.
Konrad Stradowski – ekspert Obserwatorium.biz sp. z o.o.

OBSERWATORIUM . BIZ

Obserwatorium.biz jest niezależną polską firmą doradczą, specjalizującą się w tworzeniu i wdrażaniu strategii cyfrowych w przedsiębiorstwach, głównie z sektora finansowego oraz administracji publicznej. Spółka wspiera klientów w poszczególnych fazach rozwoju strategicznego — od diagnozy sytuacji wewnętrznej, otoczenia rynkowego przez wsparcie w formułowaniu nowych celów i produktów, uwzględniając trendy społeczne i biznesowe aż po wparcie procesów wdrożeniowych i realizacyjnych. Obserwatorium to zespół specjalistów w dziedzinie finansów i technologii posiadających bogate doświadczenie w prowadzeniu projektów w instytucjach finansowych, IT oraz administracji publicznej.

PROGRAM ANALITYCZNO BADAWCZY

O Programie

Program Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce.

Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów – końcowych użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie i cyberbezpieczeństwo**
- **Zdolność banków do finansowania gospodarki**
- **Bankowość spółdzielcza**
- **Rynek nieruchomości**
- **Zielony ład i finansowanie energetyki odnawialnej**
- **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt:

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-394 Warszawa, ul. Solec 38, lok. 104
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl

Spis treści

Słowniczek pojęć i skrótów

Pojęcie	Opis
AIS	Account Information Service – zagregowana informacja o stanie rachunków bankowych (kilku, w różnych bankach), dająca klientom łatwy wgląd online w stan ich finansów
AISP	Account Information Service Provider – dostawca świadczący wyłącznie usługę dostępu do informacji o rachunku
API	Application Programming Interface – Interfejs programowania aplikacji – zestaw procedur, protokołów i narzędzi do budowy aplikacji. Interfejs API określa sposób, w jaki komponenty oprogramowania powinny ze sobą współpracować
ASPSP	Account Servicing Payment Service Provider – dostawca usług płatniczych zapewniający i utrzymujący rachunek płatniczy dla płatnika
CBPII/CISP/PIISP	Card Based Payment Instruments Issuer / Card Issuing Service Provider / Payment Instrument Issuing Service Provider – dostawcy kart i innych instrumentów płatniczych
CSC	Common Secure Communication – wspólna, bezpieczna komunikacja, standard komunikacji TPP z bankami zabezpieczający wiadomości przed „podsłuchaniem", a także zapewniający możliwość dokładnej identyfikacji stron
EBA/EUNB	European Banking Authority – Europejski Urząd Nadzoru Bankowego
EEA/EOG	European Economic Area / Europejski Okręg Gospodarczy – okręg gospodarczy obejmujący kraje UE + Norwegia, Islandia, Liechtenstein
eIDAS	Rozporządzenie Parlamentu Europejskiego i Rady "Electronic Identification, Authentication and Trust Services", weszło w życie 17 września 2014 r., w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym
ESI	Dokument "Electronic Signatures and Infrastructures"
ETSI	European Telecommunications Standards Institute – Europejski Instytut Norm Telekomunikacyjnych
GAFA	Google, Amazon, Facebook, Apple – duże firmy technologiczne dysponujące znaczącymi bazami klientów w skali globalnej
KIP	Krajowa instytucja płatnicza
KNF	Komisja Nadzoru Finansowego
NCA	National Competent Authorities – Organy Właściwe Kraju – krajowi regulatorzy

Open API	Otwarte interfejsy programistyczne
PIS	Payment Initiation Service – realizacja płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu
PISP	Payment Initiation Service Providers – to uregulowane podmioty, które mogą realizować płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu. Po otrzymaniu danych do logowania w bankowości internetowej klienta, PISP będzie inicjować płatność w określonej kwocie do określonego odbiorcy i raportować klientowi o jej realizacji
PolishAPI	Polski standard interfejsu programistycznego
PSD2	Payment Services Directive II – Dyrektywa w sprawie usług płatniczych 2015/2366, w tym związane z nią regulacyjne standardy techniczne opracowane przez EBA i zatwierdzone przez Komisję Europejską oraz wdrożone w ramach sprawozdania okresowego, a także wszelkie formalne wytyczne wydane przez właściwy organ
PSP	Payment Service Provider – Dostawca usług płatniczych jest podmiotem, który wykonuje regulowane usługi płatnicze, w tym AISP, PISP, CBPII i ASPSP
PSU	Payment Service User – końcowy użytkownik usług płatniczych
QSeal	Qualified Certificate for Seals – kwalifikowany certyfikat dla pieczęci elektronicznych
QWAC	Qualified Website Authentication Certificate – kwalifikowany certyfikat cyfrowy w ramach usług zaufania określonych w rozporządzeniu eIDAS
RODO	Rozporządzenie o Ochronie Danych Osobowych
RTS	Regulatory Technical Standards – zestaw szczegółowych kryteriów zgodności ustalonych dla wszystkich stron, które obejmują takie obszary jak bezpieczeństwo danych, odpowiedzialność prawna i inne procesy
SCA	Strong Customer Authentication – silne uwierzytelnienie klienta, to uwierzytelnienie oparte na wykorzystaniu dwóch lub więcej elementów sklasyfikowanych jako „wiem" (coś, co tylko użytkownik zna [na przykład hasło]), „mam" (coś, co tylko użytkownik posiada [na przykład konkretny telefon komórkowy i numer]) i „jestem" (coś, czym użytkownik jest [lub ma, na przykład, odcisk palca lub wzór tęczówki]), które są niezależne – naruszenie jednego nie zagraża innym i jest zaprojektowane w taki sposób, aby chronić poufność danych uwierzytelniających
TOiP	Tabela Opłat i Prowizji
TPP	Third Party Providers – kategoriia usługodawców na rynku usług płatniczych, które będą mogły świadczyć dwa typy nowych usług: dostarczania zagregowanej informacji o stanie rachunków bankowych (AIS) oraz realizacja płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu (PIS)
TSP	Technical Service Provider – Dostawcy usług technicznych to przedsiębiorstwa, które współpracują z dostawcami regulowanymi w celu dostarczania produktów lub usług z zakresu open bankingu
WG-API	EBA Working Group on APIs under PSD2 – grupa robocza do spraw interfejsów programistycznych aplikacji w ramach PSD2

Podsumowanie zarządcze

I. Określone podmioty (ASPSP, TPP, PSP) w wyniku pogłębionej analizy ryzyka powinny zwrócić uwagę na specyficzne wewnętrzne uwarunkowania organizacyjne, które pozwolą na wypracowanie szczegółowej listy ryzyk wraz z oszacowaniem prawdopodobieństwa ich materializacji oraz doborem konkretnych zabezpieczeń. Stworzenie i bieżąca aktualizacja takiej polityki zarządzania ryzykiem na poziomie każdej z instytucji jest niezbędna dla efektywnego i bezpiecznego funkcjonowania ekosystemu finansów cyfrowych w przyszłości.

II. Niezbędna jest współpraca sektorowa, w której środowisko bankowe ściśle współpracuje z podmiotami trzecimi na rzecz rozwoju rynku w zakresie legislacji, zarządzania ryzykiem, w tym cyberbezpieczeństwem oraz komunikacją do klientów.

III. Potrzebne jest wypracowanie i uspójnienie jednego standardu komunikacji z konsumentami na rynku, w tym jednolitego nazewnictwa podmiotów uczestniczących na rynku oraz nowych procesów biznesowych związanych z pobieraniem danych i inicjowaniem transakcji przez podmioty trzecie.

IV. Rekomenduje się również wypracowanie na poziomie lokalnym rejestru i baz wszystkich dokumentów związanych z aspektami rejestracji, autoryzacji, licencjonowania dostawców usług płatniczych, który dodatkowo będzie na bieżąco aktualizowany. Wypracowanie jednego źródła procedur i standardów.

V. Samo wdrożenie dyrektywy PSD2 stanowi jedynie punkt wyjścia dla potencjalnych zmian na rynku szeroko pojętych cyfrowych finansów, zarówno w Polsce, jak i na całym obszarze geograficznym obowiązywania Dyrektywy. Rozwój rynku wynikającego z wdrożenia dyrektywy PSD2 w znacznej mierze będzie wynikał z realnych wdrożeń biznesowych poszczególnych graczy – tak banków, jak i TPP, ergonomii i bezpieczeństwa plasowanych na rynku nowych i rozwijanych aplikacji. Już teraz wiadomo jednak, że Dyrektywa ma szansę spowodować:

a. Zwiększenie konkurencyjności rynku w kontekście wejścia graczy z sektora pozafinansowego oraz zwiększenia puli dostępnych narzędzi w rywalizacji między samymi bankami na bardzo istotnym polu cyfrowych finansów.

b. Koncentrację na walce o rolę finansowej „aplikacji wiodącej" dla klienta końcowego, w której będą mogły dzięki mechanizmom PSD2 uczestniczyć podmioty pozabankowe (FinTechy, Merchanci, stacje paliw, supermarkety itd.).

c. Zwiększenie wagi biznesowych i wizerunkowych konsekwencji kompromitacji danych. Kompromitacja po stronie podmiotów trzecich jak TPP może negatywnie odbić się również na samych bankach.

d. Zmniejszenie przychodów z bieżącej działalności banków – dalsze ograniczenie marży na biznesie płatniczym oraz spadek dochodów np. z kredytów, gdy dzięki wykorzystaniu mechanizmów PSD2 do weryfikacji zdolności kredytowej, część biznesu przejdzie do podmiotów trzecich.

e. Wykorzystanie popularności bankowości elektronicznej do rozwoju innych obszarów gospodarki oraz administracji publicznej, które dzięki mechanizmom PSD2 będą mogły być bardziej wydajnie scyfryzowane.

Cele raportu

Raport „Bezpieczeństwo usług opartych o otwarte interfejsy programistyczne (API) w kontekście implementacji Dyrektywy PSD2" powstał w celu skatalogowania i uporządkowania wiedzy i źródeł informacji dotyczących wdrożenia PSD2. Wpływ Dyrektywy na długoterminowy rozwój rynku płatności nie jest jeszcze jasny, natomiast z założenia ma ona zrewolucjonizować europejski rynek poprzez promowanie konkurencji, innowacyjności i bezpieczeństwa usług płatniczych.

W ramach prac nad raportem przeprowadzono szereg analiz obejmujących dokumentację, najważniejsze ryzyka i aspekty biznesowe. Ponadto przeprowadzone zostały wywiady bezpośrednie z 10 przedstawicielami instytucji finansowych, których wiedza pozwoliła wzbogacić raport o perspektywę bezpośrednich uczestników rynku.

Przeprowadzona analiza pozwoliła na stworzenie bazy wiedzy oraz źródeł informacji, obejmujących najważniejsze aspekty Dyrektywy, tj. prawne, techniczne i organizacyjne. Raport ma na celu wsparcie uczestników rynku w zakresie dostępu do wiedzy oraz informacji dotyczących PSD2 oraz powiązanych dokumentów.

Metodologia pracy nad raportem

Prace nad raportem podzielone były na cztery główne etapy:

1. Analiza dokumentacji i źródeł wiedzy
Analiza otoczenia prawnego prowadzona była od 09.2019 r. do 11.2019 r. W ramach tego etapu stworzony został katalog wszystkich najważniejszych aktów prawnych powiązanych z Dyrektywą PSD2 na poziomie europejskim oraz krajowym, kwestii dyskusyjnych, Właściwych Organów Krajowych, rejestrów krajowych i interesariuszy. Analizie na potrzeby raportu poddane zostały m.in. akty prawne, opracowania przygotowane przez EBA, instytucje odpowiedzialne za standaryzację czy lokalnych regulatorów.

2. Wywiady bezpośrednie
Na potrzeby raportu przeprowadzone zostały wywiady bezpośrednie z przedstawicielami instytucji finansowych, badanie to miało charakter jakościowy. Badanie przeprowadzone zostało w grudniu 2019 roku i obejmowało przeprowadzenie i analizę 10 telefonicznych indywidualnych wywiadów pogłębionych z przedstawicielami podmiotów mających bezpośredni kontakt ze zmianami wywołanymi przez PSD2 w Polsce. Ten sam kwestionariusz, w formie CAWI, został również zastosowany w ankietach rozesłanych do zagranicznych podmiotów. Wykorzystanie formularza w przypadku badania poza granicami polski podyktowane było niższą dostępnością respondentów – użycie techniki CAWI miało pozwolić na zwiększenie response rate. Wywiady pozwoliły pogłębić wiedzę dotyczącą ryzyka w zakresie bezpieczeństwa danych, ryzyk biznesowych oraz tworzenia się nowych bądź rozwoju istniejących strategii rynkowych.

3. Analiza ryzyk
Ocena skutków dla zidentyfikowanych ryzyk została przeprowadzona metodą ekspercką przy uwzględnieniu najlepszych praktyk i standardów rynkowych w zakresie oceny ryzyk i uzupełniona została wiedzą pozyskaną na bazie realizowanych wywiadów bezpośrednich z uczestnikami rynku. Planowanie i przeprowadzenie analizy ryzyka zostało wykonane zgodnie z wytycznymi Normy ISO 31000:2018, w szczególności skupiając się na zdefiniowaniu zakresu i kontekstu analizy ryzyka oraz określeniu kryteriów oceny ryzyka.

4. Analiza biznesowa
Analiza biznesowa przeprowadzona została na bazie pozyskanych w ramach wywiadów opinii respondentów, analizy desk research i wiedzy eksperckiej autorów raportu.

Najważniejsze wnioski z przeprowadzonych wywiadów bezpośrednich

Respondenci zgodnie przyznali, że istnieje zauważalne ryzyko związane z wyciekiem danych, przede wszystkim po stronie TPP. Podkreślają, że banki są objęte bardziej rygorystycznymi regulacjami, których efektem jest zwiększone bezpieczeństwo danych – TPP pod te regulacje nie podchodzą. Może się to również wiązać ze „świeżością" niektórych TPP, którzy mogą nie być gotowi na obsługę dużej ilości zapytań lub nie dysponować odpowiednią infrastrukturą zapewniającą bezpieczeństwo danych. Taka opinia wybrzmiała w niemal każdej wypowiedzi respondentów. TPP jako nowe podmioty, z mniejszym doświadczeniem, stawiane są tu w pewnej opozycji do banków, uważanych za doświadczonych graczy z odpowiednią infrastrukturą. Pojawił się jednak głos, mówiący o ogólnym zwiększeniu bezpieczeństwa danych po wejściu w życie PSD2.

W przypadku ryzyk biznesowych, respondenci zgodnie uważają, że najbardziej narażone są banki. Składają się na to trzy czynniki:

1. Banki jako podmioty o dużej inercji, stosunkowo wolno reagujące na zmiany, będą musiały konkurować z nowymi, zwinnymi graczami. Mają co prawda przewagę doświadczenia i zasobów, ale może zabraknąć im zwinności potrzebnej do szybkiego reagowania na potrzeby klientów.

2.Do tej pory banki były jedynymi instytucjami zarządzającymi danymi finansowymi PSU. W rzeczywistości po PSD2 do tych danych dostęp będą miały podmioty trzecie, co wytrąci z rąk banków swoisty monopol na istotny rodzaj danych, co więcej TPP będą mogły za zgodą klientów wykorzystać te dane do tworzenia nowych usług, których banki dotąd nie mogły oferować.

3. Banki bez wątpienia stracą część bezpośredniego kontaktu z klientem. Będzie to efektem przejęcia przez TPP części „codziennych" interakcji, takich jak sprawdzenie salda rachunku czy wykonanie przelewu. Jest to ryzyko szczególnie istotne dla banków, które prezentują niższy poziom swoich aplikacji czy serwisów transakcyjnych. Ryzyko to zwiększy się w momencie, w którym na rynek wejdą duże firmy technologiczne (GAFA) dysponujące najczęstszym kontaktem z klientami.

TPP również są narażone na pewne biznesowe ryzyka, respondenci wyróżniają tutaj przede wszystkim ich brak rozpoznawalności i wyrobionej marki, co może utrudnić przyciąganie nowych klientów.

Rzeczywistość po PSD2 ma też według respondentów wywołać zmiany strategii różnych graczy. Przewidywany rozwój rynku będzie powolny, ale nieuniknione. Zauważalne są już nowe modele, między innymi u firm oferujących pożyczki i innych podmiotów, np. Alior Banku, prawdopodobne jest pojawienie się alternatyw do pay-by-linków.

Co również uznawane jest za istotne, niektóre banki będą musiały zacząć więcej inwestować w rozwój, aby uniknąć stania się jedynie dostawcą infrastruktury, bez rzeczywistego kontaktu z klientem.

Respondenci spodziewają się, że rynek raczej rozwinie się w kierunku współpracy fintechów z bankami, co uważają też za rozwiązanie najbardziej korzystne dla klientów. Za mniej prawdopodobną uważają przyszłość, w które fintechy, czy duże firmy technologiczne same, bez współpracy banków, zaczną oferować rozwiązania wynikające z PSD2.

Respondenci zgodnie twierdzą, że Dyrektywa jest bodźcem do rozwoju i innowacji. Dodaje ona dodatkowego pędu fintechom, co może skłaniać banki do tego samego. Pojawiły się jednak głosy mówiące o fakcie istnienia wielu mechanizmów open bankingu już wcześniej, według tych respondentów PSD2 stanie się jedynie dodatkowym motywem i ułatwieniem dla różnych podmiotów, wpływając pozytywnie na popularyzację usług typu AIS i PIS.

Respondentom ciężko było powiedzieć, jakie nowe usługi mogą pojawić się na rynku. Poza istniejącymi już modelami oferującymi scoring kredytowy na bazie AIS, przewidywane jest powstanie alternatyw dla pay-by-linków, całkiem prawdopodobne, że będą za nimi stały fintechy, które obecnie są integratorami płatności. Oznaczać to może swoistą kanibalizację przez nich ich własnych produktów.

Przewidywana jest wyraźna współpraca pomiędzy różnymi graczami – bankami i fintechami – w zakresie tworzenia nowych rozwiązań. Respondenci zauważają, że wyniknie to z przedstawionych powyżej ryzyk – banki będą potrzebowały zwinności fintechów, a fintechy – marki i infrastruktury banków.

Analiza otoczenia prawnego

1.1. Wprowadzenie

PSD2, czyli Payment Services Directive II to unijna Dyrektywa w sprawie usług płatniczych. W pełni działająca od 14 września 2019 roku powstała jako odpowiedź na propozycję stworzenia bardziej innowacyjnych i bezpieczniejszych płatności na terenie EOG. Nowe zasady nie tylko miały rozwijać, otwierać bankowość i wprowadzać na szeroki rynek nowe podmioty – TPP (Third Party Provider), ale też umożliwiać klientom banków lepszą kontrolę, nad swoimi danymi. Wprowadzenie Dyrektywy było krokiem w stronę bardziej jednolitego rynku cyfrowego.

Dzięki Dyrektywie podmioty, które uzyskały licencję na działanie jako TPP mogą oferować swoim klientom dwie usługi: AIS (Account Information Service) i PIS (Payment Initiation Service), które pozwalają odpowiednio na prezentację informacji o rachunkach z różnych banków w jednym miejscu, np. w aplikacji oraz na inicjowanie płatności w imieniu klienta bezpośrednio z jego rachunku. TPP mogą znajdować się w jednej lub w dwóch kategoriach dostawców usług.

Aby jednak móc świadczyć klientom którąkolwiek z tych usług, podmiot musi być zarejestrowany jako ich dostawca. Aby tego dokonać należy po pierwsze wypełnić formularz znajdujący się najczęściej na stronie internetowej narodowego organu zajmującego się wydawaniem licencji instytucjom płatniczym. W Polsce tę rolę pełni Komisja Nadzoru Finansowego. Szczegółowe informacje dotyczące formularza wraz z instrukcją wypełniania znajdują się w serwisie KNF (https://www.knf.gov.pl/dla_rynku/procesy_licencyjne/platniczy). Z wytycznymi dotyczącymi informacji niezbędnych podczas rejestracji można się również zapoznać w dokumencie „Wytyczne dotyczące informacji, które należy przedstawić w celu uzyskania zezwolenia przez instytucje płatnicze i instytucje pieniądza elektronicznego oraz zarejestrowania dostawców świadczących usługi dostępu do informacji o rachunku zgodnie z art. 5 ust. 5 dyrektywy (UE) 2015/2366" opublikowanym przez Europejski Urząd Nadzoru Bankowego. Aby skutecznie działać jako TPP, wymagane jest również posiadanie certyfikatów QWAC i QSeal. Pierwszy z nich stanowi odpowiednik TLS/SSL i służy zabezpieczeniu komunikacji TPP – bank, QSeal z kolei może być wymagany jako forma zabezpieczenia przesyłanych informacji.

Zaangażowanych w proces udostępniania usług z wykorzystaniem otwartych interfejsów programistycznych jest więcej. Charakterystyka wszystkich aktorów zawarta została w poniższej tabeli.

> “
>
> Przed wejściem w życie Dyrektywy dużo mówiło się o nowych rozwiązaniach, z którymi miałyby wejść na rynek np. duże firmy technologiczne – niewiele z tego się wydarzyło. W wyniku wprowadzenia PSD2 upatrywałbym raczej ewolucji, niż rewolucji na rynku.

Aktor	Opis
ASPSP (Account Servicing Payment Service Provider)	Dostawca usług płatniczych zapewniający i utrzymujący rachunek płatniczy dla płatnika
PISP (Payment Initiation Service Providers)	Uregulowane podmioty, które za zgodą klienta mogą realizować płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu
AISP (Account Information Service Providers)	Podmiot dostarczający zagregowaną informację o stanie rachunków bankowych – kilku, w różnych bankach – dając łatwy wgląd online w stan wszystkich finansów
TTP (Third Party Providers)	Realizuje płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu (PIS) oraz dostarcza zagregowanej informacji o stanie rachunków bankowych (AIS)
PSU (Payment Services Users)	Konsument, klient, płatnik. Odbiorca usług, aktor posiadający dostęp do konta, inicjujący elektroniczne transakcje płatności zdalnych lub wykonujący wszelkie inne działania za pośrednictwem kanałów zdalnych
CISP (Card Issuing Service Provider)/ PIISP – Payment Instrument Issuing Service Provider	Dostawcy usług kartowych, wydający instrumenty płatnicze (np. karty) Informuje o dostępności środków na transakcjach płatniczych PSD2 opartych na kartach płatniczych. Dostarczone usługi powiązane można określić jako FCS (potwierdzenie dostępności usługi funduszy)
EBA (European Banking Authority)	Niezależny organ regulacyjny i nadzorujący Europejski Urząd Nadzoru Bankowego (EUNB) Organ zapewniający spójność regulacji i nadzór w europejskim sektorze bankowym
API (Application Programming Interface)	Interfejs programistyczny aplikacji Zestaw reguł, który opisuje, w jaki sposób aplikacje i systemy mogą się ze sobą komunikować. Dzięki temu jedna aplikacja może wykorzystywać inną do pozyskiwania informacji lub wykonywania zadań

1.2. Zestawienie wszystkich regulacji i aktów prawych związanych z PSD2 na poziomie UE i PL

Poniższy rozdział zawiera wykaz najważniejszych aktów prawnych i innych przepisów regulujących funkcjonowanie usług płatniczych opartych o dostęp do otwartych interfejsów programistycznych, w tym standardów rynkowych i norm opracowywanych przez międzynarodowe instytucje standaryzacyjne. Spisy wraz z odpowiednim podziałem zostały zaprezentowane w tabelach.

Otwarta bankowość to szeroki termin, pod który możemy zakwalifikować ogół technologii i usług, ścisłych regulacji, procesów i produktów będących częścią sektora finansowego. Dyrektywa wprowadza szereg zmian w regulacjach i przepisach, a co za tym idzie – zmienia funkcjonowanie usług płatniczych w całej Europie. Wprowadza również mechanizmy, dzięki którym rynek poddany będzie zwiększonej kontroli i standaryzacji.

Obok zaprezentowana została tabela przedstawiająca europejskie regulacje prawne (w tym poprzedzające) związane z PSD2.

Sygnatura	Nazwa	Data implementacji
(UE) 2015/2366	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.	29.11.2018
(UE) 910/2014	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.	29.11.2018
(UE) 2019/411	Rozporządzenie Delegowane Komisji (UE) 2019/411 z dnia 29 listopada 2018 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych określających techniczne wymogi w zakresie opracowania, obsługi i prowadzenia elektronicznego centralnego rejestru w dziedzinie usług płatniczych i w zakresie dostępu do informacji w nim zawartych.	27.11.2017
(UE) 2019/410	Rozporządzenie Delegowane Komisji (UE) 2019/410 z dnia 29 listopada 2018 r. ustanawiające wykonawcze standardy techniczne w odniesieniu do szczegółów i struktury informacji przekazywanych w dziedzinie usług płatniczych przez właściwe organy Europejskiemu Urzędowi Nadzoru Bankowego zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366.	14.11.2017
	Plan działania w sprawie detalicznych usług finansowych.	23.06.2017
	Zielona księga w sprawie detalicznych usług finansowych.	22.11.2016
(UE) 2018/389	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 oraz bezpiecznych standardów komunikacji.	25.11.2015
(UE) 2017/2055	Rozporządzenie Delegowane Komisji (UE) 2017/2055 z dnia 23 czerwca 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących współpracy i wymiany informacji między właściwymi organami w związku z korzystaniem ze swobody przedsiębiorczości i swobody świadczenia usług przez instytucje płatnicze.	23.07.2014
(UE) 2015/751	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę.	9.06.2016

Obok rozporządzeń opracowano też Regulacyjne Standardy Techniczne (RTS), a także wytyczne (Guidelines), które muszą spełnić kraje członkowskie EOG w ramach PSD2. Dokumenty mają również odzwierciedlenie w aktach prawnych, które zostały już przedstawione.
Lista wszystkich RTS-ów wraz z opisem została umieszczona w tabeli poniżej.

Sygnatura	Nazwa	Opis
EBA/RTS/2017/10 EBA/ITS/2017/07	Techniczne Standardy odnoszące się do Rejestru prowadzonego przez European Banking Authority (EBA) na mocy PSD2	Dokument zawiera opis standardów technicznych oraz wykonawczych, jakie należy spełnić przy prowadzeniu centralnego Rejestru EBA. Zostały tam określone zarówno wymogi dotyczące opracowania, prowadzenia i utrzymania rejestru oraz informacji, jak i same informacje, które mają być w nim zawarte
EBA/RTS/2018/03	Regulacyjne Standardy Techniczne odnoszące się do współpracy państw na mocy PSD2	Dokument określa ramy współpracy i wymiany informacji między właściwymi organami państwa państw członkowskich i państw przyjmujących, precyzuje rodzaj informacji i szablony, które instytucje płatnicze mają stosować przy zgłaszaniu właściwym organom przyjmującego państwa członkowskiego sprawozdań z działalności gospodarczej w zakresie płatności prowadzonej na ich terytoriach.
EBA/RTS/2017/09	Regulacyjne Standardy Techniczne dotyczące centralnych punktów kontaktowych na mocy PSD2	Dokument określa kryteria pozwalające wskazać, kiedy właściwe jest wyznaczenie centralnego punktu kontaktowego na mocy PSD2 oraz jakie funkcje powinny pełnić te punkty kontaktowe.
EBA/RTS/2016/05	Regulacyjne Standardy Techniczne odnoszące się do systemów kart płatniczych i podmiotów przetwarzających płatności zgodnych z rozporządzeniem w sprawie opłat interchange	Dokument wprowadza szczególne wymogi związane z niezależnością systemów kart płatniczych i podmiotów przetwarzających płatności. Dokument został opracowany zgodnie z art. 7 ust. 6 rozporządzenia w sprawie opłat interchange (IFR).
EBA/RTS/2017/02	Regulacyjne standardy techniczne dotyczące silnego uwierzytelniania klienta i bezpiecznej komunikacji w ramach PSD2	Dokument zawiera regulacyjne standardy techniczne dotyczące silnego uwierzytelniania klientów i bezpiecznej komunikacji. Dokument ma szczególne znaczenie, ponieważ stanowi klucz do osiągnięcia założeń PSD2, czyli: zwiększenie ochrony konsumentów, promowanie innowacji i poprawa bezpieczeństwa usług płatniczych w całej Unii Europejskiej.

Lista wszystkich Wytycznych wraz z opisem zostały umieszczone w tabeli poniżej.

Sygnatura	Nazwa	Opis
EBA/GL/2017/08	Wytyczne dotyczące kryteriów określania wysokości minimalnej kwoty pieniężnej ubezpieczenia odpowiedzialności z tytułu prowadzenia działalności zawodowej lub innej porównywalnej gwarancji zgodnie z art. 5 ust. 4 dyrektywy (UE) 2015/2366	Dokument zawiera wytyczne, które określają kryteriów ustalania warunków minimalnej kwoty pieniężnej ubezpieczenia od odpowiedzialności zawodowej (PII) lub innej porównywalnej gwarancji na usługi inicjowania płatności (PIS) i usługi informacji o rachunku (AIS). Właściwe organy opisane w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk, również jeżeli wytyczne są skierowane przede wszystkim do instytucji.
EBA/GL/2017/09	Wytyczne dotyczące informacji, które należy przedstawić w celu uzyskania zezwolenia przez instytucje płatnicze i instytucje pieniądza elektronicznego oraz zarejestrowania dostawców świadczących usługi dostępu do informacji o rachunku zgodnie z art. 5 ust. 5 dyrektywy (UE) 2015/2366	Dokument zawiera wytyczne pokazujące stanowisko EBA w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo europejskie w konkretnym obszarze. Właściwe organy opisane w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk, również jeżeli wytyczne są skierowane przede wszystkim do instytucji.
EBA/GL/2017/10	Wytyczne dotyczące zgłaszania poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2)	Wytyczne określają kryteria, progi i metodykę stosowane przez dostawców usług płatniczych w celu ustalenia czy zdarzenie operacyjne lub związane z bezpieczeństwem należy uznać za poważne. Ponadto określa również czy owe zdarzenie należy zgłosić właściwemu organowi w rodzimym państwie członkowskim.
EBA/GL/2017/13	Wytyczne dotyczące procedur składania skarg w związku z możliwymi naruszeniami przepisów drugiej dyrektywy w sprawie usług płatniczych	Dokument określa wytyczne dotyczące procedur składania skarg w związku z możliwymi naruszeniami przepisów PSD2. W dokumencie zawarto informacje określające: sposób składania skarg, treść, jaka powinna być zawarta, wytyczne dotyczące odpowiedzi oraz wytyczne dotyczące analizy.
EBA/GL/2017/17	Wytyczne w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych na mocy dyrektywy (UE) 2015/2366 (druga dyrektywa w sprawie usług płatniczych)	Dokument określa wytyczne dotyczące środków bezpieczeństwa określonych ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych w ramach PSD2.
EBA/GL/2018/05	Wytyczne w sprawie wymogów zgłaszania nadużyć finansowych na podstawie art. 96 ust. 6 drugiej dyrektywy w sprawie usług płatniczych (PSD2)	Dokument określa wytyczne wymagane od dostawców usług płatniczych w 28 państwach członkowskich UE gromadzenia i zgłaszania danych o transakcjach płatniczych i fraudach przy użyciu jednolitego języka (określonej metodologii, definicji i podziału danych).
EBA/GL/2018/07	Wytyczne w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389 (w sprawie regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji)	Dokument zawiera wytycznych w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389. Dokument określa, w jakich przypadkach można skorzystać z funkcji tzw. fallback-u.

Dyrektywa PSD2 ma również znaczący wpływ na kształt i rozwój polskiego rynku usług płatniczych i bankowych.

Poniższa tabela przedstawia spis ustaw wprowadzających zmiany w polskim prawie, które dotykają zagadnień związanych z otwartą bankowością, w tym usług płatniczych i ochrony danych osobowych.

Sygnatura	Nazwa	Data ogłoszenia	Data wejścia w życie
Dz.U. 2011 nr 199 poz. 1175	Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych	23.09.2011	24.10.2011
Dz.U. 2018 poz. 864	Ustawa z dnia 22 marca 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw	10.05.2018	11.08.2018
Dz. U. 2018 poz. 1000	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych	24.05.2018	25.05.2018
Dz.U. 2018 poz. 1075	Ustawa z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw	5.06.2018	20.06.2018
Dz.U. 2018 poz. 1110	Rozporządzenie Ministra Finansów z dnia 6 czerwca 2018 r. w sprawie metody obliczania kwoty, o której mowa w art. 76 ust. 4 pkt 2 ustawy o usługach płatniczych	8.06.2018	23.06.2018

Ponad powyższe przygotowany został także dokument „Podpisy elektroniczne i infrastruktury elektroniczne (ESI); Wymagania specyficzne dla danego sektora; Profile certyfikatów kwalifikowanych i wymagania dotyczące polityki TSP na mocy dyrektywy w sprawie usług płatniczych (UE) 2015/2366", przedstawia standardy kwalifikowanych usług, zgodnych z PSD2.

Dokument ten dostępny jest do pobrania na stronie ETSI pod adresem:

https://www.etsi.org/standards-search#page=1&search=TS119495&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2019-12-19-&harmonized0=&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1.

1.3. Skrócony opis aktów prawnych

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**

Dyrektywa PSD2 (Payment Services Directive II) wprowadziła szereg zmian w zakresie usług płatniczych, ale nie był to pierwszy tego typu dokument. Znana również pod nazwą Dyrektywa (UE) 2015/2366 jest drugą dyrektywą w sprawie usług płatniczych i ma na celu spowodowanie szeregu zmian na rynku płatności elektronicznych w ramach Unii Europejskiej i Europejskiego Obszaru Gospodarczego. Głównym celem Dyrektywy jest zapewnienie podstawy prawnej, która wpłynie na rozwój lepiej zintegrowanego rynku wewnętrznego płatności elektronicznych w Unii Europejskiej, i poprawa oraz ujednolicenie dotychczasowych przepisów. PSD2 wymaga, aby przepisy dotyczące usług płatniczych w poszczególnych krajach członkowskich były tak samo proste, bezpieczne i efektywne w całej Unii Europejskiej. Kolejnym celem przyświecającym Dyrektywie jest otwarcie rynków płatności na nowych graczy, a w konsekwencji zwiększenie konkurencyjności, możliwości wyboru i innowacyjności dostępnych produktów i usług. Dyrektywa wprowadza szczegółowe przepisy w obszarach wymogów bezpieczeństwa płatności elektronicznych i ochrony danych finansowych konsumentów, praw i obowiązków zarówno użytkowników, jak i dostawców oraz przejrzystości warunków korzystania z poszczególnych usług.

Warto zaznaczyć, że dyrektywa ma moc również poza granicami Unii. Państwa, które dodatkowo przyjmują te regulacje to: Islandia, Norwegia i Liechtenstein, więc kraje, które należą do Europejskiego Obszaru Gospodarczego (European Economic Area – EEA).

Dyrektywa została uzupełniona o wiele rozporządzeń, które zostały opisane poniżej.

Dyrektywa PSD2 zarówno w oryginalnej, jak i w polskiej wersji dostępna jest w bazie aktów prawnych Unii Europejskiej – EUR-Lex, pod adresem: https://eur-lex.europa.eu/homepage.html?locale=pl. Rozporządzenie obowiązuje w okręgu EOG.

2. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Rozporządzenie Parlamentu Europejskiego i Rady UE nr 910/2014 jest równie ważnym dokumentem co sama Dyrektywa PSD2. Odnosi się do usług zaufania oraz identyfikacji elektronicznej, które są niezwykle istotne w kontekście usług płatniczych. Głównym celem rozporządzenia jest zwiększenie zaufania do płatności elektronicznych na rynku wewnętrznym. Zwiększenie efektywności usług online (prywatnych i publicznych), e-handlu i e-biznesu na terenie całej Unii będzie możliwe dzięki zapewnieniu bezpiecznej interakcji elektronicznej między użytkownikami (obywatelami, przedsiębiorcami i instytucjami publicznymi).

Rozporządzenie zarówno w oryginalnej, jak i w polskiej wersji dostępne jest w bazie aktów prawnych Unii Europejskiej – EUR-Lex, pod adresem: https://eur-lex.europa.eu/homepage.html?locale=pl. Rozporządzenie obowiązuje w obszarze EOG.

3. ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2019/411 z dnia 29 listopada 2018 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych określających techniczne wymogi w zakresie opracowania, obsługi i prowadzenia elektronicznego centralnego rejestru w dziedzinie usług płatniczych i w zakresie dostępu do informacji w nim zawartych

Dokument powiązany z Dyrektywą PSD2, stanowi jego uzupełnienie w zakresie standardów technicznych. Rozporządzenie zawiera informacje co do sposobu przekazywania, udostępniania, aktualizowania informacji, które powinny być zawarte w rejestrze centralnym. Ponadto ściśle określa rodzaj informacji, które mają się w nim znajdować. Dodatkowo dokument zawiera szereg wymogów dotyczących bezpieczeństwa, dostępności i wydajności rejestru, jego obsługi i wparcia oraz przedstawia zakres dostępu do informacji.

Rozporządzenie zarówno w oryginalnej, jak i w polskiej wersji dostępne jest w bazie aktów prawnych Unii Europejskiej – EUR-Lex, pod adresem: https://eur-lex.europa.eu/homepage.html?locale=pl. Rozporządzenie obowiązuje w obszarze EOG.

4. ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2019/410 z dnia 29 listopada 2018 r. ustanawiające wykonawcze standardy techniczne w odniesieniu do szczegółów i struktury informacji przekazywanych w dziedzinie usług płatniczych przez właściwe organy Europejskiemu Urzędowi Nadzoru Bankowego zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366

Dokument powiązany z Dyrektywą PSD2, obejmuje jego uzupełnienie w zakresie standardów technicznych. Główną część dokumentu stanowi Załącznik, który przedstawia szczegóły i format przekazywanych informacji w zakresie usług płatniczych (zgodnie z art. 15 ust. 1 dyrektywy (UE) 2015/2366). Jest on czymś w rodzaju szablonu dla podmiotów, które wskazują posiadane zezwolenia lub dostępy.
Rozporządzenie zarówno w oryginalnej, jak i w polskiej wersji dostępne jest w bazie aktów prawnych Unii Europejskiej – EUR-Lex, pod adresem: https://eur-lex.europa.eu/homepage.html?locale=pl. Rozporządzenie obowiązuje w obszarze EOG.

5. 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

Jedno z najważniejszych rozporządzeń uzupełniających Dyrektywę PSD2. Rozporządzenie ustanawia wymogi, które dostawcy usług płatniczych muszą spełniać w celu wdrożenia środków bezpieczeństwa. W całości odnosi się do regulacyjnych standardów technicznych (RTS) głównie w kontekście silnego uwierzytelniania.

W dokumencie określone zostały więc ogólne wymogi dotyczące uwierzytelniania, a także został zawarty przegląd środków bezpieczeństwa oraz dokładny opis zasad stosowanych przy konkretnych rozwiązaniach, które mają zostać wdrożone przez wszystkich dostawców usług płatniczych (PSP). Mocno zaakcentowane jest silne uwierzytelnianie – zostało szczegółowo opisane zagadnienie bezpieczeństwa, wyłączenia, poufności i integralności danych. Wprowadzono zasadę podwójnej weryfikacji, tzn. uwierzytelnianie musi być dokonane w oparciu o 2 z 3 elementów. Do elementów należą: wiedza (coś co wie tylko użytkow-

nik), posiadanie (coś co ma tylko użytkownik) oraz cechy (coś czym jest tylko użytkownik). W końcowej części rozporządzenia ujęto wspólne i bezpieczne otwarte standardy komunikacji.

Standardy zabezpieczeń opisane w RTS mają na celu zapewnienie ochrony konsumenta i wzmocnienie konkurencyjności. Ochrona konsumentów zostanie osiągnięta poprzez zwiększenie poziomu bezpieczeństwa płatności elektronicznych. RTS wprowadza standardy bezpieczeństwa, których dostawcy usług płatniczych muszą przestrzegać podczas przetwarzania płatności lub świadczenia usług związanych z płatnościami. Standardy wyznaczające wymagania dotyczące silnego uwierzytelniania dotyczą klientów oraz przypadków, w których dostawcy usług płatniczych mogą być zwolnieni z takiego uwierzytelniania. W kontekście drugiego celu (zwiększenie innowacyjności i konkurencji) standardy określają dwa nowe rodzaje usług płatniczych: usługi inicjowania płatności (PIS) i usługi informacji o rachunkach (AIS).

Rozporządzenie zarówno w oryginalnej, jak i w polskiej wersji dostępne jest w bazie aktów prawnych Unii Europejskiej – EUR-Lex, pod adresem: https://eur-lex.europa.eu/homepage.html?locale=pl. Rozporządzenie obowiązuje w obszarze EOG.

6. **ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2017/2055 z dnia 23 czerwca 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących współpracy i wymiany informacji między właściwymi organami w związku z korzystaniem ze swobody przedsiębiorczości i swobody świadczenia usług przez instytucje płatnicze**

Rozporządzenie uzupełnia Dyrektywę PSD2.

Ustanawia ono przepisy dotyczące współpracy i wymiany informacji między właściwymi organami państw członkowskich w odniesieniu do zgłoszeń dotyczących korzystania ze swobody przedsiębiorczości lub swobody świadczenia usług przez instytucje płatnicze oraz przekazywania zgłoszeń między wyżej wymienionymi instytucjami (w tym, gdy prowadzą one dystrybucję pieniądza elektronicznego za pośrednictwem osoby fizycznej lub prawnej). Całość zgodna jest z dyrektywą (UE) 2015/2366. Dokument zawiera sześć załączników, które stanowią podstawę informacji („Format odpowiedniego niepowtarzalnego numeru identyfikacyjnego w każdym państwie członkowskim") oraz wzory powiadamiania.

Rozporządzenie zarówno w oryginalnej, jak i w polskiej wersji dostępne jest w bazie aktów prawnych Unii Europejskiej – EUR-Lex, pod adresem: https://eur-lex.europa.eu/homepage.html?locale=pl
Rozporządzenie obowiązuje w obszarze EOG.

7. **ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę**

Wraz z Dyrektywą PSD2, jako dokument uzupełniający, wydano również Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751. Dokument określa jednolite wymogi techniczne i handlowe w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę na terytorium Unii. Zapisy dotyczą sytuacji, w której dostawca usług płatniczych płatnika oraz dostawca usług płatniczych odbiorcy znajdują się w UE. Ponadto zapisany ustalały zakres stosowania rozporządzenia, zasady realizowania transakcji oraz zasady opłat interchange. Głównym celem rozporządzenia w połączeniu z Dyrektywą jest ograniczenie opłat za transakcje oparte na kartach debetowych i kredytowych oraz nałożenie na sprzedawców detalicznych zakazu nakładania dodatkowych opłat na klientów za korzystanie z tego rodzaju kart. Rozporządzenie wprowadza pułapy opłat interchange pomiędzy bankami z tytułu płatności dokonywanych kartą. Ma to zmniejszyć koszty sprzedawców przyjmujących karty debetowe i kredytowe od konsumentów.

Rozporządzenie zarówno w oryginalnej, jak i w polskiej wersji dostępne jest w bazie aktów prawnych Unii Europejskiej – EUR-Lex, pod adresem: https://eur-lex.europa.eu/homepage.html?locale=pl
Rozporządzenie obowiązuje w ramach EOG.

1.4. Wykaz rejestrów i innych źródeł danych

Zadaniem European Banking Authority (Europejskiego Urzędu Nadzoru Bankowego) było utworzenie centralnego rejestru na potrzeby PSD2. Opracowany został dedykowany RTS, którego zadaniem było wyznaczenie wymogów dotyczących opracowania, działania i utrzymania elektronicznego rejestru oraz określono informacje, które mają być w nim zawarte.

European Bank Authority utrzymuje dwa rejestry: Payment Institutions Register i Credit Institutions Register. Pierwszy z nich zawiera informacje zawarte w rejestrze instytucji płatniczych i instytucji pieniądza elektronicznego EBA, drugi odnosi się do instytucji kredytowych. Rejestry są regularnie aktualizowane.

Payment Institutions Register został stworzony wyłącznie na podstawie informacji dostarczonych przez właściwe organy krajowe państw członkowskich EOG. W związku z tym, w przeciwieństwie do rejestrów krajowych (w ramach PSD2), rejestr ten nie ma mocy prawnej i stanowi jedynie agregat rejestrów krajowych. Oznacza to, że jeśli nieuprawniona instytucja zostaje przypadkowo wpisana do rejestru, jej status prawny nie ulega zmianie; podobnie, jeżeli instytucja została przypadkowo pominięta w rejestrze, ważność jej zezwolenia nie ulegnie zmianie. Podsumowując, European Banking Authority odpowiada jedynie za dokładne odtworzenie informacji otrzymanych przez właściwe organy w odniesieniu do każdej osoby fizycznej lub prawnej wpisanej do rejestru. Właściwe organy na szczeblu krajowym odpowiadają za dokładność tych informacji[1].

Wyszukiwarka odpowiednich podmiotów w ramach rejestru składa się z 4 części. Pierwsza z nich zawiera podstawowe informacje, które dają możliwość wybrania m.in. typu instytucji, nazwy instytucji, miasta, kraju. Druga część dotyczy właściwego organu krajowego. Pod „Payment and electronic money services" wybieramy interesujące z dostępnych pozycji oraz kraj. Ostania część odnosi się do typu i rodzaju statusu. Wskazanie opcji jest dobrowolne, ponieważ cały rejestr można otworzyć bez dokonywania wyborów, jednak utrudni to odszukanie najcelniejszych wyników.

Rejestr jest dostępny pod adresem: https://euclid.eba.europa.eu/register/pir/search .

Drugi z rejestrów – Credit Institutions Register, podobnie do Payment Institutions Register, został utworzony na podstawie informacji udostępnionych przez właściwe rejestry krajowe dla EBA. Wszelkie zasady dotyczące np. znaczenia prawnego zostały powtórzone z pierwszego wymienionego rejestru.

Credit Institutions Register poprzedzony jest wyszukiwarką, która ma pomóc we wskazaniu najtrafniejszych informacji. W tym przypadku możliwościami jest wybór m.in. typu instytucji, nazwy instytucji, kodu, kraju, miasta. Wybranie opcji jest dobrowolne.

Rejestr dostępny jest pod adresem: https://euclid.eba.europa.eu/register/cir/search .

Poniższa tabela zawiera listę Właściwych Organów Krajowych. Właściwe Organy Krajowe, czyli National Competent Authorities (NCA), są krajowymi regulatorami. Każdy kraj posiada tylko jeden taki organ.

Aktualna lista podmiotów dostępna jest również publicznie na stronie https://eba.europa.eu/

[1] Źródło: https://eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2

Kraj	Nazwa (ang.)	Nazwa krajowa
Austria	Austrian Financial Market Authority	Finanzmarktaufsicht
Belgia	National Bank of Belgium	National Bank van Belgie / Banque Nationale de Belgique
Bułgaria	Bulgarian National Bank	Българска народна банка
Chorwacja	Croatian National Bank	Hrvatska Narodna Banka
Cypr	Central Bank of Cyprus	Κεντρική Τράπεζα της Κύπρου
Czechy	Czech National Bank	Česká národní banka
Dania	Danish Financial Supervisory Authority	Finanstilsynet
Estonia	Estonian Financial Supervision Authority	Finantsinspektsioon
Finlandia	Finnish Financial Supervisory Authority	Finanssivalvonta / Finansinspektionen
Francja	Prudential Supervisory and Resolution Authority	Autorité de Contrôle Prudentiel et de Résolution
Grecja	Bank of Greece	Η Τράπεζα της Ελλάδος
Hiszpania	Bank of Spain	Banco de España
Holandia	The Netherlands Bank	De Nederlandsche Bank
Irlandia	Central Bank of Ireland	
Islandia	Financial Supervisory Authority	Fjarmalaeftirlitid
Liechtenstein	Financial Market Authority Liechtenstein	Finanzmarktaufsicht Liechtenstein
Litwa	Bank of Lithuania	Lietuvos Bankas
Luksemburg	Commission for the Supervision of Financial Sector	Commission de Surveillance du Secteur Financier
Łotwa	Financial and Capital Market Commission	Finanšu un kapitāla tirgus komisija
Malta	Malta Financial Services Authority	
Niemcy	Federal Financial Supervisory Authority	Bundesanstalt für Finanzdienstleistungsaufsicht
Norwegia	The Financial Authority of Norway	Finanstilsynet
Polska	Polish Financial Supervision Authority	Komisji Nadzoru Finansowego

Portugalia	Bank of Portugal	Banco de Portugal
Rumunia	National Bank of Romania	Banca Naţională a României
Słowacja	National Bank of Slovakia	Národná banka Slovenska
Słowenia	Bank of Slovenia	Banka Slovenije
Szwecja	Swedish Financial Supervisory Authority	Finansinspektionen
Węgry	Central Bank of Hungary	Magyar Nemzeti Bank
Wielka Brytania	Financial Conduct Authority (FCA)	
Włochy	Bank of Italy	Banca d'Italia

Europejski Urząd Nadzoru Bankowego prowadzi szereg rejestrów na podstawie wymogu określonego w art. 15 ust. 1 dyrektywy (UE) 2015/2366 w sprawie usług płatniczych w ramach rynku wewnętrznego (PSD2), jak również uzupełniającego rozporządzenia wykonawczego Komisji (UE) 2019/410 oraz rozporządzenia delegowanego Komisji (UE) 2019/411 z dnia 29 listopada 2018 r., które są oparte na RTS i ITS na mocy PSD2 opublikowanym przez EUNB w grudniu 2017 r. Scentralizowane rejestry zasilane są danymi dostarczanymi bezpośrednio przez NCAs. Istnieje centralny rejestr (EBA Register on Payment and Electronic Money Institutions), który agreguje informacje o osobach fizycznych lub prawnych, które mogą świadczyć usługi płatnicze i/lub usługi związane z pieniądzem elektronicznym. W skład rejestru wchodzą:

- Instytucje płatnicze – zgodnie z definicją prawną zawartą w art. 4 ust. 4 dyrektywy w sprawie usług płatniczych 2
- Zwolnione instytucje płatnicze – na mocy art. 32 dyrektywy PSD2
- Podmioty świadczące usługi w zakresie informacji o rachunkach – na mocy art. 33 dyrektywy PSD2
- Instytucje pieniądza elektronicznego – zgodnie z definicją prawną zawartą w art. 2 ust. 1 dyrektywy w sprawie pieniądza elektronicznego 2
- Instytucje pieniądza elektronicznego objęte wyłączeniem – na mocy art. 9 dyrektywy w sprawie pieniądza elektronicznego
- Agenci – zgodnie z definicją prawną zawartą w art. 4 ust. 38 dyrektywy PSD2
- Oddziały w EOG – zgodnie z definicją prawną zawartą w art. 4 ust. 39 dyrektywy PSD2
- Instytucje uprawnione na mocy prawa krajowego do świadczenia usług płatniczych – zgodnie z art. 2 ust. 5 dyrektywy PSD2
- Dostawcy usług wyłączeni z zakresu dyrektywy PSD2 – zgodnie z art. 3 lit. k) ppkt (i) i (ii) oraz lit. l) dyrektywy PSD2.

Dane z rejestru dostępne są do pobrania w formacie JSON i SHA256.

Wszystkie rejestry można odnaleźć na stronie EBA, pod adresem: https://euclid.eba.europa.eu/register/ .

Rejestr EBA stanowi odtworzenie informacji podanych przez NCAs, co oznacza, że mogą wystąpić pewne uchybienia lub rozbieżności pomiędzy rejestrami lokalnymi a głównym rejestrem.

Poniżej znajduje się wykaz NCA wraz z odnośnikami do odpowiednich Rejestrów Krajowych.

Kraj	Nazwa właściwego organu w języku narodowym
AUSTRIA	Financial Market Authority (FMA)
BELGIA	National Bank of Belgium (NBB)
BUŁGARIA	Financial Supervision Commission (FSC)
CHORWACJA	Hrvatska Narodna Banka (HNB)
CYPR	Central Bank of Cyprus (CBC)
CZECHY	Czech National Bank (CNB)
DANIA	finanstilsynet (FSA)
ESTONIA	FINANTSINSPEKTSIOON (FSA)
FINLANDIA	Finanssivalvonta (FIN-FSA)
FRANCJA	Autorité de Controle Prudentiel (ACPR) „Regafi”
GRECJA	Bank Of Greece
HISZPANIA	Banco de Espana (BDE)
HOLANDIA	De Nederlandsche Bank (DNB)
IRLANDIA	Central Bank of Ireland (CBI)
ISLANDIA	Narodna Banka Slovenska (NBS)
LIECHTENSTEIN	Finanzmarktaufsicht Liechtenstein (FMA)
LITWA	Bank of Lithuania (LB)
LUKSEMBURG	Commission de Surveillance du Secteur Financier (CSSF)
ŁOTWA	Finansu un Kapital Tirgus Komisija (FKTK)
MALTA	Malta Financial Services Authority (MFSA)
NIEMCY	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
NORWEGIA	Finanstilsynet (FSA)

POLSKA	Komisja Nadzoru Finansowego (KNF)
PORTUGALIA	Banco De Portugal
RUMUNIA	Banca Nationala a Romaniei (BNR)
SŁOWACJA	Narodna Banka Slovenska (NBS)
SŁOWENIA	Banka Slovenije (BSI)
SZWECJA	Finansinspektionen (FI)
WĘGRY	Magyar Nemzeti Bank (MNB)
WIELKA BRYTANIA	Financial Conduct Authority (FCA)
WŁOCHY	Banca d'Italia

1.5. Najważniejsze zmiany i wnioski dla uczestników rynku

Dyrektywa PSD2 ma za zadanie ujednolicenie rynku usług płatniczych w całym Europejskim Obszarze Gospodarczym, zwiększenie bezpieczeństwa transakcji, rozwój konkurencyjności oraz ulepszenie doświadczenia konsumentów. Wokół tych zagadnień (korzyści ekonomiczne, prawa konsumenta, bezpieczeństwo transakcji, nowe podmioty, jednolity rynek) skupia się najwięcej zmian wprowadzonych przez Dyrektywę.

> "Wchodzący na rynek TPP mogą nie zdawać sobie sprawy ze skali, z jaką będą musieli się zmierzyć – muszą zapewnić infrastrukturę, która obsłuży bardzo dużą ilość zapytań na odpowiednim poziomie.

Zmiany na rynku zapewne zachodzić będą dość powoli, lecz docelowo najbardziej skorzystać na Dyrektywie mają sami konsumenci. Najważniejszą zmianą dla nich jest pobudzenie konkurencyjności, co oznacza szerszą gamę produktów, lepszy wybór oraz niższe ceny. Będą mogli swobodnie żonglować pomiędzy rodzajami usług płatniczych, a także samymi dostawcami. Pozytywne, z perspektywy konsumentów, zmiany dotyczą także ich praw oraz możliwości składania reklamacji.

E-Commerce cieszy się od lat rosnącym zainteresowaniem, co w konsekwencji spowodowało pojawienie się na rynku podmiotów, które zaoferowały lub umożliwiły wraz z bankami realizację niemal natychmiastowych płatności online także bez konieczności posiadania karty.

PSD2 obejmuje dostawców usług inicjowania płatności i usług dostępu do informacji o rachunku, w zakresie poufności, odpowiedzialności, bezpieczeństwa transakcji i procesu rejestracji.

Ponadto zniesione zostały dodatkowe opłaty za korzystanie z kart debetowych i kredytowych, nastąpiło więc zmniejszenie kosztów dla konsumenta. Konsumenci zostali również objęci lepszą ochroną przed fraudami, czyli nadużyciami oraz incydentami związanymi z nieautoryzowanymi płatnościami. Maksymalna kwota, jaką płatnik mógłby zapłacić w przypadku nieautoryzowanej transakcji płatniczej, została obniżona z kwoty 150 EUR do 50 EUR. Oprócz powyższych korzyści konsumenci zyskali także więcej praw, m.in. bezwarunkowe prawo do otrzymania zwrotu pieniędzy przez okres 8 tygodni w odniesieniu do poleceń zapłaty (w ramach SEPA), możliwość blokady środków na koncie przez płatnika tylko w przypadku, gdy znana jest konkretna kwota transakcji (np. przy rezerwacji hotelu, samochodu). Dodatkowo Dyrektywa PSD2 zwiększa prawa konsumentów w przypadku tzw. transakcji jednostronnych, czyli poza UE lub w walucie państw spoza UE. PSD2 obejmuje „unijną część" transakcji, zapewniając większą przejrzystość na rynku.

Skutkiem posiadania większych praw przez konsumenta jest wyznaczenie przez państwa członkowskie właściwych organów do rozpatrywania skarg. Natomiast dostawcy usług płatniczych zobowiązani są do wprowadzenia odpowiednich procedur składania reklamacji przez klientów spełniających wymogi ustawy dotyczące kwoty odpowiedzialności i terminu odniesienia się do złożonej reklamacji.

Kluczową zmianą PSD2 było zdefiniowanie i wprowadzenie nowego typu podmiotu – TPP (Third Party Providers), czyli nowej, w rozumieniu Dyrektywy, kategorii usługodawców na rynku usług płatniczych. Usługami obsługiwanymi przez ten typ podmiotu są inicjacja płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu (PIS – Payment Initiation Services) i dostarczenie zagregowanej informacji o stanie rachunków bankowych (AIS – Account Information Services).

Instytucje płatnicze, oferując usługi inicjowania płatności lub usługi dostępu do informacji o rachunku, będą zobowiązane uzyskać ubezpieczenie odpowiedzialności z tytułu prowadzenia działalności zawodowej. Będzie to jeden z warunków, które należy spełnić podczas wnioskowania o zezwolenie lub dokonanie rejestracji. Ponadto w Dyrektywie określono również przepisy dotyczące nadzoru nad posiadającymi zezwolenie instytucjami płatniczymi. PSD2 wprowadza także procedurę postępowania w przypadku nieprzestrzegania przepisów przez wybrane podmioty.

Europejski Urząd Nadzoru Bankowego zyskał większą rolę w zakresie opracowania regulacyjnych standardów technicznych, wsparcia podczas rozwiązywania sporów oraz tworzenia ogólnodostępnego centralnego rejestru.

1.6. SCA, czyli silne uwierzytelnianie klienta i funkcja fallback

PSD2 wprowadza rygorystyczne wymogi bezpieczeństwa dotyczące inicjowania i przetwarzania płatności elektronicznych, które mają zastosowanie do wszystkich dostawców usług płatniczych. Jedną z największych zmian, jakie niesie za sobą Dyrektywa, jest procedura silnego uwierzytelniania. Silne uwierzytelnianie klienta (SCA) to inaczej autentykacja tożsamości klienta, który korzysta z elektronicznych usług płatniczych. SCA wymaga zastosowania w procesie dwóch z trzech wymienionych elementów, tj.:

- Wiedzy (coś, co wie wyłącznie użytkownik),
- Posiadania (coś, co posiada wyłącznie użytkownik),
- Cechy klienta (coś, czym jest wyłącznie użytkownik).

Wymagane cechy muszą być od siebie niezależne. Oznacza to, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych.

Każdy bank wprowadził własne sposoby weryfikacji klientów podczas logowania.

Ponadto, zostały określone przypadki, kiedy silne uwierzytelnianie ma miejsce, są to: uzyskanie dostęp do swojego rachunku płatniczego w trybie online, inicjacja elektronicznej transakcji płatniczej oraz przeprowadzenie czynności za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć. Bardziej rygorystyczne podejście do bezpieczeństwa powinno przyczynić się do zmniejszenia ryzyka oszustwa w przypadku wszystkich nowych i obecnych wcześniej na rynku metod płatności (zwłaszcza płatności internetowych) oraz do ochrony poufności danych finansowych użytkownika – m.in. danych osobowych.

Innym bardzo ważnym wymaganiem nałożonym na ASPSP jest konieczność utrzymania odpowiednich standardów oferowanych interfejsów dostępowych oraz utworzenie oraz utrzymywanie opcji zapasowej na wypadek awarii lub czasowej niedostępności. Zgodnie z art. 33 ust. 4 RTS, odnoszącym się do mechanizmów awaryjnych mających zastosowanie w sytuacji, gdy API nie działa zgodnie z wymogami RTS lub gdy wystąpi nieplanowana niedostępność interfejsu czy awaria systemu, ASPSP ma obowiązek umożliwić TPP – do momentu przywrócenia poziomu dostępności i efektywności API – korzystanie z interfejsów udostępnionych użytkownikom usług płatniczych na potrzeby uwierzytelniania i komunikacji z ASPSP. Mówimy tutaj o tzw. opcji „fallback". Zgodnie z art. 33 ust. 6 RTS odpowiedni NCAs z każdego kraju może zwolnić ASPSP z obowiązku posiadania opcji fallback przy spełnieniu wszystkich niżej wymienionych warunków:

1) stosowane API spełnia wszystkie określone w art. 32 RTS obowiązki dotyczące specjalnych interfejsów;

2) API został opracowany i przetestowany, zgodnie z art. 30 ust. 5 RTS, w sposób zadowalający TPP;

3) od co najmniej trzech miesięcy API jest powszechnie stosowany w celu świadczenia usług płatniczych przez TPP;

4) wszelkie problemy związane z API rozwiązano bez zbędnej zwłoki.

1.7. Kwestie sporne i dyskusyjne

EBA Working Group on APIs under PSD2 (WG-API) jest grupą roboczą do spraw interfejsów programistycznych aplikacji w ramach PSD2. Zwierzchnictwo nad grupą ma EBA. WG-API składa się z przedstawicieli ASPSP – dostawców usług płatniczych (9 przedstawicieli), przedstawicieli TPP (9 przedstawicieli) i przedstawicieli inicjatyw API (również 9) oraz trzech innych osób – przedstawicieli dostawców usług technicznych organów normalizacyjnych i użytkowników usług płatniczych.

Zadaniem grupy jest konsultacja i zaopiniowanie kwestii dyskusyjnych z EBA, właściwymi organami krajowymi, Komisją Europejską i Europejskim Bankiem Centralnym. Celem konsultacji jest rozwiązanie kwestii spornych lub dyskusyjnych, które pojawiły się w czasie przygotowań do wejścia w życie regulacyjnej normy technicznej (RTS) w zakresie silnego uwierzytelniania klientów oraz wspólnej i bezpiecznej komunikacji w ramach PSD2 (RTS w sprawie SCA&CSC).

W załączniku numer 1 do raportu przedstawiono podsumowanie kwestii spornych, które były lub wciąż są konsultowane w ramach spotkań grupy roboczej EBA WG-API.

Analiza ryzyka

Celem niniejszego rozdziału jest zapewnienie zainteresowanym podmiotom materiału pomocniczego przy wykonywaniu własnych analiz ryzyka w kontekście usług wprowadzonych Dyrektywą PSD2. Rozdział stanowi ogólną analizę ryzyka skupiającą się na opisaniu i klasyfikacji potencjalnych skutków wystąpienia poszczególnych ryzyk. Ocena prawdopodobieństwa wystąpienia poszczególnych ryzyk nie mogła zostać rzetelnie zrealizowana ze względu na bardzo dużą liczbę interesariuszy, poziomu i różnorodności stosowanych przez nich systemów, modeli biznesowych czy polityk bezpieczeństwa.

Ocena prawdopodobieństwa materializacji ryzyk powinna być realizowana na poziomie poszczególnych interesariuszy, w szczególności ze względu na dużą liczbę indywidualnych czynników wpływających na ocenę – np. przyjęte zabezpieczenia techniczno-organizacyjne, polityki bezpieczeństwa, potencjał organizacyjny czy otoczenie zewnętrzne.

Przeprowadzona analiza ma charakter oceny potencjalnych skutków w kontekście:

- Ryzyk związanych z bezpieczeństwem chronionych danych;
- Ryzyk operacyjnych i regulacyjnych;
- Ryzyk biznesowych.

2.1. Metodyka realizacji prac związanych z oceną i kategoryzacją ryzyk

W pierwszym etapie prac nad analizą ryzyka zaplanowano podejścia do sposobu przeprowadzenia analizy ryzyka w obszarze komunikacji opartej na otwartych interfejsach programistycznych (API). Planowanie prac podzielono na następujące aspekty:

- Określenie zakresu i kontekstu analizy ryzyka
- Określenie kryteriów oceny ryzyka.

Planowanie i przeprowadzenie analizy ryzyka zostało wykonane zgodnie z wytycznymi Normy ISO 31000:2018.

Zakres analizy ryzyka obejmuje trzy usługi wprowadzone Dyrektywą PSD2:

- Usługi dostępu do informacji o rachunku
- Usługi inicjowania płatności
- Usługi potwierdzania dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej.

Na zakres analizy wpływ ma zidentyfikowany kontekst otoczenia, na który składają się następujące artefakty:

Podstawowy cel biznesowy w kontekście bezpieczeństwa dla procesu udostępnienia usług z wykorzystaniem otwartych API dotyczy zabezpieczenia danych chronionych, obejmujących:

- dane uwierzytelniające klientów,
- dane transakcyjne (informacje o transakcjach finansowych wykonanych w ramach interfejsu PolishAPI: kwoty, opisy oraz nazwy stron transakcji),
- dane bankowe (informacje o rachunkach bankowych i ich saldach),
- dane osobowe (dane identyfikujące osoby zgodnie z ustawą o ochronie danych osobowych),
- klucze kryptograficzne (np. wszelkie klucze prywatne występujące w środowisku oraz klucz publiczny do certyfikatu TLS w przypadku użycia obustronnego uwierzytelnienia w tym protokole – w zakresie jego integralności)
- informacje o wewnętrznej strukturze systemu (architektura wewnętrznych baz danych po stronie serwerowej, format komunikatów przesyłanych pomiędzy systemami wewnętrznymi oraz nazwy obiektów wewnętrznych),
- dowody z przeprowadzonych transakcji.

Interesariusze:

- EBA (European Banking Authority) – Europejski Urząd Nadzoru Bankowego
- NCA (National Competent Authorities) – Organy Właściwe Kraju – krajowi regulatorzy
- ASPSP (Account Servicing Payment Service Provider) – podmioty prowadzące rachunki płatnicze
- TPP (Third Party Providers) – Podmioty trzecie, które będą mogły świadczyć dwa typy nowych usług: dostarczania zagregowanej informacji o stanie rachunków bankowych (AIS) oraz inicjacja płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu (PIS)

- PSU (Payment Services Users) – użytkownicy rachunku płatniczego, którego dotyczą transakcje realizowane za pośrednictwem PolishAPI

- Personel – pracownicy występujący w różnych rolach w TPP, ASPSP, EBA, NCA.

Wymagania prawne:

- Ustawa o usługach płatniczych wprowadzająca Dyrektywę PSD2 – ustawa wprowadzająca do polskiego porządku prawnego trzy usługi, które stanowią przedmiotowy zakres niniejszej analizy

- RODO – przepisy dotyczące ochrony danych osobowych, w kontekście niniejszej analizy dotyczy danych osobowych klientów (PSU)

- Ustawa Prawo bankowe – przepisy regulujące funkcjonowanie instytucji bankowych

- Ustawa o świadczeniu usług drogą elektroniczną – reguluje obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną

- Rekomendacja D KNF dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach

- 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 – przepisy wprowadzające mechanizmy silnego uwierzytelniania klienta

- Rozporządzenie delegowane Komisji (UE) 2019/411 z dnia 29 listopada 2018 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych określających techniczne wymogi w zakresie opracowania, obsługi i prowadzenia elektronicznego centralnego rejestru w dziedzinie usług płatniczych i w zakresie dostępu do informacji w nim zawartych

- Rozporządzenie wykonawcze Komisji (UE) 2019/410 z dnia 29 listopada 2018 r. ustanawiające wykonawcze standardy techniczne w odniesieniu do szczegółów i struktury informacji przekazywanych w dziedzinie usług płatniczych przez właściwe organy Europejskiemu Urzędowi Nadzoru Bankowego zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366

- Rozporządzenie delegowane Komisji (UE) 2017/2055 z dnia 23 czerwca 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących współpracy i wymiany informacji między właściwymi organami w związku z korzystaniem ze swobody przedsiębiorczości i swobody świadczenia usług przez instytucje płatnicze.

Komponenty i usługi techniczne:

- Sprzęt
- Oprogramowanie
- Interfejsy
- Protokoły sieciowe.

W kolejnym etapie prac wypracowano kryteria oceny skutków:

Krytyczność skutków	Opis
Niska	Wystąpienie ryzyka może spowodować wystąpienie skutków o niskim wpływie na bieżącą pracę i stabilność podmiotu odpowiedzialnego za dane zdarzenie. Potencjalne reperkusje wystąpienia ryzyka nie przekroczą poniższych kryteriów: • Dotkną niewielkiej liczby klientów. • Dotyczyć będą danych lub informacji, które nie są krytyczne z perspektywy bezpieczeństwa. • Nie wpłyną na długoterminowe obniżenie lub utratę reputacji. • Nie spowodują wystąpienia znacznego ani trwałego uszczerbku na zdolność podmiotu do realizowania celów biznesowych. • Nie będą miały dużego wpływu finansowego w postaci kar czy obniżenia przychodowości podmiotu.
Średnia	Wystąpienie opisywanego ryzyka może doprowadzić do umiarkowanych konsekwencji względem winnego podmiotu. Ryzyka z tej kategorii mogą spowodować realne straty w zakresie bieżącego biznesu. Ryzyka określone w tej kategorii mogą: • Dotknąć umiarkowanej liczby klientów. • Dotyczyć niewielkich ilości danych krytycznych z perspektywy bezpieczeństwa. • Mogą krótko i/lub długoterminowo wpłynąć na utratę reputacji podmiotu np. poprzez nagłośnienie incydentu w mediach specjalistycznych. • Negatywnie wpłynąć na realizację bieżących działań biznesowych podmiotu. • Wymagać zmian regulaminowych, operacyjnych lub technicznych u podmiotu odpowiedzialnego za incydent. • Mieć reperkusje finansowe związane z reklamacjami, odejściem klientów, zmniejszenia zdolności do realizacji oferowanych usług czy nałożeniem kar przez regulatora.
Wysoka	Ryzyka zakwalifikowane do tej kategorii mogą spowodować wysokie lub krytyczne konsekwencje i bardzo negatywnie wpłynąć nie tylko na działalność odpowiedzialnego podmiotu, ale także na całą branżę finansową. Kompleksowe zaadresowanie ryzyk w tej kategorii powinno być dla wszystkich uczestników rynku kluczowym elementem strategii rozwoju i prowadzenia biznesu. Potencjalne konsekwencje wystąpienia wybranego ryzyka mogą: • Wpłynąć na długoterminowe szkody wizerunkowe i reputacyjne odpowiedzialnego podmiotu, ale także na obniżenie zaufania klientów do rynku finansowego. • Spowodować masowe odejścia klientów. • Mieć konsekwencje prawne ze strony klientów i/lub organów regulacyjnych. • Spowodować wysokie straty finansowe związane z odejściem klientów, odszkodowaniami i karami finansowymi.

Ocena skutków dla zidentyfikowanych ryzyk została przeprowadzona metodą ekspercką przy uwzględnieniu najlepszych praktyk i standardów rynkowych w zakresie oceny ryzyk i uzupełniona została wiedzą pozyskaną na bazie realizowanych wywiadów bezpośrednich z uczestnikami rynku.

2.2. Identyfikacja i ocena ryzyka

W kontekście wymienionych w punkcie 2.1 trzech usług w obszarze komunikacji opartej na standardzie PolishAPI, identyfikacja i ocena ryzyka została zawężona do trzech kategorii:

- Ryzyka związane z bezpieczeństwem informacji danych chronionych
- Ryzyka biznesowe
- Ryzyka operacyjne i regulacyjne.

> “
>
> Ryzykiem z jednej strony dla bezpieczeństwa, z drugiej biznesowym jest wyciek czy miks danych po stronie TPP. To co banki dopracowywały przez lata, czyli bezpieczeństwo w obszarze prezentowania danych, to dziś stoi przed TPP. A nie każdego TPP stać na to, aby utrzymać wysoki poziom zabezpieczeń.

2.2.1. Ryzyka związane z bezpieczeństwem danych chronionych

W kontekście zapewnienia bezpieczeństwa informacji danych chronionych autorzy zidentyfikowali i skatalogowali poniższy zbiór ryzyk. Opisane ryzyka mają charakter wysokopoziomowy i nie wskazują na dobór konkretnych rozwiązań technologicznych, a raczej na obszary zabezpieczeń, które należy wziąć pod uwagę ze względu na specyfikę danego ryzyka. Określone podmioty (ASPSP, TPP, PSP) w wyniku pogłębionej analizy ryzyka powinny zwrócić uwagę na specyficzne wewnętrzne uwarunkowania organizacyjne, które pozwolą na wypracowanie szczegółowej listy ryzyk wraz z oszacowaniem prawdopodobieństwa ich materializacji oraz doborem konkretnych zabezpieczeń.

> “
>
> Na dzień dzisiejszy nie wiemy, jak będą wyglądały zabezpieczenia po stronie TPP, które nie są objęte tak restrykcyjnymi regulacjami jak banki, a to może oznaczać, że te dane niekoniecznie muszą być tak bezpieczne jak w bankach. Dla klienta końcowego również niekoniecznie musi być jasne, w którym momencie te dane przekazywane są i zarządzane przez podmioty trzecie, dlatego spodziewam się tutaj przerzucenia odpowiedzialności na banki. To mogą być sytuacje zapalne.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek danych uwierzytelniających pojedynczego klienta**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa (m.in. bezpieczeństwa sesji) w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Wyciek danych uwierzytelniających może być uwarunkowany niskimi wymaganiami w stosunku do polityki względem jakości haseł. Nieskomplikowane jakościowo hasła mogą zostać łatwo złamane. Ryzyko może również zaistnieć w przypadku skutecznie przeprowadzonego ataku phishingowego, mającego na celu uzyskanie danych uwierzytelniających za pomocą podstawionego serwisu internetowego. Problemy ze skutecznym szyfrowaniem sesji na etapie uwierzytelniania się klienta do usługi danego usługodawcy mogą wpłynąć na możliwość przechwycenia danych uwierzytelniających.
Opis skutków	Skutki wycieku danych uwierzytelniających dla pojedynczego klienta mogą eskalować wiele ryzyk. W szczególności może to obejmować: • Nieautoryzowany dostęp do danych: osobowych, transakcyjnych czy danych bankowych • Utrata zaufania klienta do usług bankowych • Roszczenia klienta • Kary administracyjne w wyniku naruszenia ochrony danych osobowych dla dostawcy usługi
Krytyczność skutków	Średnia
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotnym jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Rekomenduje się wykorzystanie/promowanie zaleceń standardu NIST Special Publication 800-63B w stosunku do polityki jakościowej haseł. • Realizacja skoordynowanej kampanii edukacyjnej dopasowanej do poszczególnych profili klientów oraz uwzględniająca różne kanały komunikacji w tym zakresie. • Realizacja szkoleń/kampanii informacyjnej wewnątrz poszczególnych organizacji dla personelu celem podnoszenia świadomości z zakresu bezpieczeństwa informacji. • W ramach systemów każdego z usługodawców należy zapewnić mechanizm szyfrujący sesję zapobiegający możliwość przechwycenia danych uwierzytelniających.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek danych uwierzytelniających grupy klientów**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa (m.in. bezpieczeństwa sesji) w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Wyciek danych uwierzytelniających może być uwarunkowany niskimi wymaganiami w stosunku do polityki względem jakości haseł. Nieskomplikowane jakościowo hasła mogą zostać łatwo złamane. Ryzyko może również zaistnieć w przypadku skutecznie przeprowadzonego ataku phishingowego, mającego na celu uzyskanie danych uwierzytelniających za pomocą podstawionego serwisu internetowego. Problemy ze skutecznym szyfrowaniem sesji na etapie uwierzytelniania się klienta do usługi danego usługodawcy mogą wpłynąć na możliwość przechwycenia danych uwierzytelniających.
Opis skutków	Skutki wycieku danych uwierzytelniających dla grupy klientów mogą eskalować wiele ryzyk. W szczególności może to obejmować: • Nieautoryzowany dostęp do danych: osobowych, transakcyjnych czy danych bankowych • Niekontrolowaną sprzedaż danych klientów • Utratę zaufania klientów do usług bankowych • Utratę reputacji banku • Kary administracyjne w wyniku naruszenia ochrony danych osobowych dla dostawcy usługi • Roszczenia klientów
Krytyczność skutków	Wysoka
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotnym jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Rekomenduje się wykorzystanie/promowanie zaleceń standardu NIST Special Publication 800-63B w stosunku do polityki jakościowej haseł. • Realizacja skoordynowanej kampanii edukacyjnej dopasowanej do poszczególnych profili klientów oraz uwzględniająca różne kanały komunikacji w tym zakresie. • Realizacja szkoleń/kampanii informacyjnych wewnątrz poszczególnych organizacji dla personelu celem podnoszenia świadomości z zakresu wiedzy na temat bezpieczeństwa informacji oraz najnowszych wektorów ataków. • W ramach systemów każdego z usługodawców należy zapewnić mechanizm szyfrujący sesję zapobiegający możliwość przechwycenia danych uwierzytelniających.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek danych transakcyjnych pojedynczego klienta**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Ryzyko może również zaistnieć w przypadku skutecznie przeprowadzonych działań o charakterze phishingowym.
Opis skutków	Skutki wycieku danych transakcyjnych dla pojedynczego klienta mogą eskalować wiele ryzyk. W szczególności może to obejmować: • Możliwość wykorzystania utraconych danych transakcyjnych klienta na potrzeby zbudowania wiarygodnego ataku phishingowego ukierunkowanego na konkretną osobę. • Utratę zaufania klienta do usług bankowych • Roszczenia klienta
Krytyczność skutków	Średnia
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotnym jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Realizacja skoordynowanej kampanii edukacyjnej dopasowanej do poszczególnych profili klientów oraz uwzględniająca różne kanały komunikacji w tym zakresie.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek danych transakcyjnych grupy klientów**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Ryzyko może również zaistnieć w przypadku skutecznie przeprowadzonych działań o charakterze phishingowym.
Opis skutków	Skutki wycieku danych transakcyjnych grupy klientów mogą eskalować wiele ryzyk. W szczególności może to obejmować: • Sprzedaż danych transakcyjnych podmiotom trzecim • Możliwość wykorzystania utraconych danych transakcyjnych grupy klientów na potrzeby zbudowania zmasowanego ataku phishingowego • Utratę reputacji banku • Masowe pozwy osób, których dane były przedmiotem wycieku
Krytyczność skutków	Wysoka
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotnym jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Realizacja skoordynowanej kampanii edukacyjnej dopasowanej do poszczególnych profili klientów oraz uwzględniająca różne kanały komunikacji w tym zakresie. • W ramach systemów poszczególnych podmiotów należy rozważyć zastosowanie systemu DLP (Data Loss Prevention), który minimalizuje ryzyko przypadkowych wycieków, wynikających z nieostrożności pracowników, jak i wycieków celowych.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek danych bankowych pojedynczego klienta**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych oraz organizacyjnych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka.
Opis skutków	• Utrata zaufania klienta do usług bankowych • Pozew sądowy osoby, której dane były przedmiotem wycieku
Krytyczność skutków	Średnia
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotnym jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Realizacja szkoleń/kampanii informacyjnych wewnątrz poszczególnych organizacji dla personelu celem podnoszenia świadomości z zakresu wiedzy na temat bezpieczeństwa informacji oraz najnowszych wektorów ataków.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek danych bankowych grupy klientów**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych oraz organizacyjnych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka.
Opis skutków	Skutki wycieku danych bankowych grupy klientów mogą eskalować wiele ryzyk. W szczególności może to obejmować: • Utratę zaufania społecznego (w tym klientów) do usług bankowych • Sprzedaż danych bankowych podmiotom trzecim • Utratę reputacji banku • Masowe pozwy osób, których dane były przedmiotem wycieku
Krytyczność skutków	Wysoka
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotnym jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Realizacja szkoleń/kampanii informacyjnych wewnątrz poszczególnych organizacji dla personelu celem podnoszenia świadomości z zakresu wiedzy na temat bezpieczeństwa informacji oraz najnowszych wektorów ataków. • W ramach systemów poszczególnych podmiotów należy rozważyć zastosowanie systemu DLP (Data Loss Prevention), który minimalizuje ryzyko przypadkowych wycieków, wynikających z nieostrożności pracowników, jak i wycieków celowych.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek danych osobowych pojedynczego klienta**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do wyników przeprowadzonej analizy ryzyka zabezpieczeń technicznych, tudzież organizacyjnych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Istotnym aspektem, który może również wpłynąć na zaistnienie powyższego ryzyka, mogą być niewłaściwie zaprojektowane procesy: monitorowania zdarzeń, zgłaszania incydentów oraz reakcji na incydenty.
Opis skutków	Skutki wycieku danych osobowych dla pojedynczego klienta mogą eskalować wiele ryzyk. W szczególności może to obejmować: • Sprzedaż danych osobowych podmiotom trzecim • Utratę zaufania klienta do usług bankowych • Roszczenia klienta • Pozew sądowy osoby, której dane były przedmiotem wycieku
Krytyczność skutków	Średnia
Mityganty	• Konieczność przebudowania systemu (na który składają się rozwiązania techniczne oraz organizacyjne) ochrony danych osobowych, ze szczególnym uwzględnieniem procesów: monitorowania zdarzeń, zgłaszania incydentów oraz reakcji na incydenty. Edukacja personelu w zakresie zewnętrznych oraz wewnętrznych zagrożeń socjotechnicznych/phishingowych wpływających na prawdopodobieństwo materializacji powyższego ryzyka. • W ramach systemów poszczególnych podmiotów należy rozważyć zastosowanie systemu DLP (Data Loss Prevention), który minimalizuje ryzyko przypadkowych wycieków, wynikających z nieostrożności pracowników, jak i wycieków celowych.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Masowy wyciek danych osobowych grupy klientów**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych tudzież organizacyjnych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Istotnym aspektem, który może również wpłynąć na zaistnienie powyższego ryzyka mogą być niewłaściwie zaprojektowane procesy: monitorowania zdarzeń, zgłaszania incydentów oraz reakcji na incydenty. Wyciek może mieć miejsce również w przypadku braku mechanizmów rozliczalności dla działań personelu mającego dostęp do danych osobowych. Wówczas zarówno przypadki celowego wynoszenia danych osobowych, jak również wycieki wynikające z błędu ludzkiego mogą pozostać niewykryte i spowodować powtarzające się sekwencje wycieków.
Opis skutków	Skutki masowego wycieku danych osobowych klientów mogą eskalować wiele ryzyk. W szczególności może to obejmować: • Utratę zaufania społecznego (w tym klientów) do usług bankowych • Karę administracyjną nałożoną przez organ ds. ochrony danych osobowych: Urząd Ochrony Danych Osobowych w wyniku poważnego naruszenia • Sprzedaż danych osobowych podmiotom trzecim na szeroką skalę • Masowe pozwy osób, których dane były przedmiotem wycieku.
Krytyczność skutków	Wysoka
Mityganty	• Konieczność zbudowania efektywnego systemu (na który składają się rozwiązania techniczne oraz organizacyjne) ochrony danych osobowych ze szczególnym uwzględnieniem procesów: monitorowania zdarzeń, zgłaszania incydentów/naruszeń oraz reakcji na incydenty/naruszenia. Edukacja personelu w zakresie zewnętrznych oraz wewnętrznych zagrożeń socjotechnicznych/phishingowych wpływających na prawdopodobieństwo materializacji powyższego ryzyka. • W ramach systemów poszczególnych podmiotów należy rozważyć zastosowanie systemu DLP (Data Loss Prevention), który minimalizuje ryzyko przypadkowych wycieków, wynikających z nieostrożności pracowników, jak i wycieków celowych.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Nieautoryzowany dostęp do kluczy kryptograficznych służących do uwierzytelnienia**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Nieautoryzowany dostęp może również wynikać z niewłaściwie zorganizowanego procesu zarządzania uprawnieniami wewnątrz danego podmiotu, w którym dostęp do dokumentacji stanowiącej przedmiot niniejszego ryzyka ma osoba nieuprawniona.
Opis skutków	• Możliwość podszywania się atakującego pod usługę płatniczą (pozyskiwanie danych klienta czy zlecanie płatności). • Utrata zaufania klientów banku do mechanizmów bezpieczeństwa bankowości elektronicznej • Duże straty finansowe wynikające z potencjalnych szkód powodowanych działaniem osób nieuprawnionych
Krytyczność skutków	Wysoka
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotne jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Należy rozważyć wdrożenie/dokonanie przeglądu procesu zarządzania uprawnień opartego na roli wewnątrz organizacji danego dostawcy usług (RBAC ang. role-based access control), który pozwoli zminimalizować ryzyko nieautoryzowanego dostępu z wewnątrz organizacji.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wyciek dokumentacji architektury systemowej IT dostawcy usługi**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Niniejsze ryzyko może być efektem wdrożenia nieadekwatnych do przeprowadzonej analizy ryzyka zabezpieczeń technicznych oraz organizacyjnych. W przypadku wykorzystywania nieskutecznych lub niepoprawnie dobranych mechanizmów mających na celu zapewnienie bezpieczeństwa w ramach systemów IT – możemy mówić o dużym prawdopodobieństwie materializacji ryzyka. Ponadto nienależyte zabezpieczenie dokumentacji architektury systemowej IT wewnątrz organizacji również rodzi ryzyko wycieku. Ten rodzaj wycieku może również wynikać z niewłaściwie zorganizowanego procesu zarządzania uprawnieniami wewnątrz organizacji danego dostawcy usług, w którym dostęp do dokumentacji stanowiącej przedmiot niniejszego ryzyka ma osoba nieuprawniona.
Opis skutków	• W przypadku zidentyfikowanego wycieku dokumentacji stanowiącej przedmiot niniejszego ryzyka, skutek wiąże się z koniecznością przebudowy architektury systemowej IT. Na czas powyższej przebudowy, część funkcjonalności związanych z podstawowymi usługami bankowości byłaby niedostępna co mogłoby narazić bank na utratę reputacji. Do czasu wykrycia wycieku, osoby nieuprawnione posiadające informacje o wewnętrznej strukturze systemu mogą dokonać kradzieży wszystkich rodzajów danych w ramach całego systemu IT. • W sytuacji, w której wyciek nie zostałby wykryty: skompromitowana architektura systemu IT może stanowić cel ataków hakerskich. Wówczas może to skutkować wyciekiem danych: osobowych, transakcyjnych oraz danych bankowych. • Poważne konsekwencje finansowe (związane z działalnością hakerów na skompromitowanym systemie IT oraz koniecznością przebudowy jego architektury).
Krytyczność skutków	Wysoka
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotne jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Należy rozważyć wdrożenie/dokonanie przeglądu procesu zarządzania uprawnieniami opartego na roli wewnątrz organizacji danego dostawcy usług (RBAC, ang. role-based access control), który pozwoli zminimalizować ryzyko nieautoryzowanego dostępu z wewnątrz. • Dokumentacja architektury systemowej IT powinna uwzględniać różne poziomy (warstwy) jej odzwierciedlenia adekwatne dla poszczególnych ról w ramach organizacji danego podmiotu. • W ramach systemów poszczególnych podmiotów należy rozważyć zastosowanie systemu DLP (Data Loss Prevention), który minimalizuje ryzyko przypadkowych wycieków, wynikających z nieostrożności pracowników, jak i wycieków celowych.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Utrata danych dowodowych**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Ryzyko może zmaterializować się w wyniku awarii systemów dostawcy usługi bądź ataku hakerskiego. Niewłaściwie zaprojektowana architektura rozwiązania, zarówno pod kątem wydajności, jak i bezpieczeństwa, która stanowi fundament systemu IT danego podmiotu może wpłynąć na utratę danych dowodowych. Ponadto nieprawidłowo zdefiniowane reguły pozyskiwania logów transakcyjnych również powodować mogą ograniczony zakres zbieranych danych dowodowych. Utrata danych dowodowych może zaistnieć również w przypadku celowego lub przypadkowego działania personelu danego podmiotu polegającego na wymazaniu określonego zakresu danych dowodowych.
Opis skutków	Potencjalny skutek może być oddalony w czasie, natomiast może to implikować utrudnione postępowanie w przypadku reklamacji, obrony przed roszczeniami. Bank wówczas narażony jest na straty finansowe oraz utratę reputacji.
Krytyczność skutków	Wysoka
Mityganty	• Cyklicznie realizowana analiza ryzyka, uwzględniająca nowe obszary zagrożeń wraz z doborem adekwatnych zabezpieczeń. Istotne jest również monitorowanie aktualności oraz skuteczności zabezpieczeń. • Istotne jest zdefiniowanie reguł zbierania logów transakcyjnych, które zapewnią zgodność z regulacjami jak również uchronią dostawcę usługi przed stratami finansowymi z tytułu braku możliwości wykazania określonych działań w ramach systemu IT. • Należy rozważyć wdrożenie/dokonanie przeglądu procesu zarządzania uprawnieniami opartego na roli wewnątrz organizacji danego dostawcy usług (RBAC ang. role-based access control), który pozwoli zminimalizować ryzyko nieautoryzowanego dostępu z wewnątrz.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Wzrost liczby fraudów**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Materializacja ryzyka może nastąpić w przypadku braku precyzyjnych zasad dotyczących zarządzania uprawnieniami. Nadmierne uprawnienia systemowe/ organizacyjne powinny zawsze posiadać uzasadnienie biznesowe (odpowiednio umocowane i zabezpieczone mechanizmami kontrolnymi). Natomiast w przypadku braku takowego: można spodziewać się fraudu ze strony pracownika bądź wykorzystania (np. poprzez socjotechnikę) jego uprawnień do realizacji fraudu. Ponadto niektóre czynności o charakterze transferów finansowych realizowane przez pojedynczą osobę również mogą powodować zmaterializowanie się niniejszego ryzyka. W związku ze stosunkowo krótkim okresem funkcjonowania PSD2 w Polsce należy wziąć pod uwagę, iż wiedza klientów w stosunku do zmian, jakie za sobą niesie Dyrektywa, jest jeszcze niewielka bądź nieprecyzyjna. W wyniku powyższego oraz w kontekście rosnącej liczby usług jest to szczególnie newralgiczny moment na coraz częstszą materializację ryzyka pojawienia się fraudów. Mechanizm 2FA, do którego wraz z wejściem w życie PSD2 każdy użytkownik bankowości internetowej musiał się przyzwyczaić, może skutkować sytuacją, w której wpisywany SMS staje się rutyną, podczas której nie zwraca się uwagi na charakter operacji, której jest potwierdzeniem. W połączeniu z nowymi metodami phishingu/ malware powoduje to zwiększenie prawdopodobieństwa zaistnienia niniejszego ryzyka.
Opis skutków	Skutkiem może być upadłość finansowa danego podmiotu, roszczenia klientów oraz wynikające z nich postępowania sądowe, utrata reputacji.
Krytyczność skutków	Wysoka
Mityganty	• Należy rozważyć wdrożenie mechanizmów kontrolnych, które pozwolą zapewnić rozliczalność każdego działania w obrębie systemu IT. Mechanizmy te powinny uwzględniać zaprojektowane oraz wdrożone logi systemowe, pozwalające na uzyskanie pełnego zestawu informacji na temat wszelkich operacji pracowników/ administratorów danego podmiotu. Informacja na temat zbieranych logów powinna być zakomunikowana pracownikom celem wywarcia prewencyjnego działania o charakterze odstraszającym. • Ponadto najważniejsze operacje (zdefiniowane przez właściciela biznesowego, często o charakterze strategicznym) dokonywane przez personel w ramach systemu IT powinny być realizowane po zatwierdzeniu przez dwóch uprawnionych użytkowników. • W celu zmitygowania ryzyka fraudów należy rozważyć wdrożenie/dokonanie przeglądu procesu zarządzania uprawnień opartego na roli wewnątrz organizacji danego dostawcy usług (RBAC, ang. role-based access control). W ramach powyższego niezbędne jest wypracowanie wyraźnej separacji ról opartych na realizowanych przez dany personel czynności • Warto dokonać analizy w zakresie wykorzystania rozwiązań typu Fraud Detection/ Prevention Systems (FDS) pozwalających na wykrywanie transakcji posiadających znamiona nielegalnych.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Ataki na API/Aplikacje**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Ryzyko dotyczy zarówno API, jak i aplikacji poszczególnych podmiotów. Jego materializacja nastąpić może z powodu niezidentyfikowanych bądź niezałatanych luk/podatności, które mogą być wykorzystane do przeprowadzenia ataków o zróżnicowanym charakterze. Niezałatane podatności z kolei mogą wynikać z niewłaściwie dobranych zabezpieczeń technicznych, zaś w ogólnym rozrachunku: z niepoprawnie przeprowadzonej analizy ryzyka.
Opis skutków	Skutki powyższego ryzyka mogą dotykać bardzo wielu rozmaitych obszarów: od wycieku różnego rodzaju danych aż po całkowity paraliż API/Aplikacji. Ataki mogą skutkować: • Niedostępnością danej usługi (API/Aplikacji) • Wyciekiem danych (każdej kategorii) klientów • Stratami finansowymi • Utratą zaufania klientów do bankowości elektronicznej
Krytyczność skutków	Wysoka
Mityganty	• Na podstawie cyklicznie realizowanej analizie ryzyka oraz zidentyfikowanych, potencjalnych zagrożeniach dla bezpieczeństwa i przeprowadzanych zmianach zarówno w obszarach organizacyjnych, jak i technicznych (infrastrukturalnych/ systemowych) należy przeprowadzić testy w celu uwzględnienia scenariuszy zidentyfikowanych i znanych potencjalnych ataków. • Należy wdrożyć mechanizmy monitorujące ruch sieciowy oraz wszelkie anomalie systemowe pozwalające na przedwczesne wykrycie ataku wraz z możliwością na adekwatną reakcję mającą na celu: minimalizację skutków ataku/jego przerwanie/ zapobiegnięcie atakowi. • Niezbędny jest przegląd procedur związanych z zarządzaniem zmianą, ciągłością działania oraz odtwarzaniem awaryjnym.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Większa powierzchnia ataku ze względu na zwiększenie liczby aktorów**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Posiłkowanie się HUB-ami API oraz idący za tym, znaczący przyrost ilości aktorów może stanowić ryzyko w postaci nadmiernie rozproszonych punktów dostępu, które mogą zaistnieć jako potencjalne podmioty do wykorzystania w charakterze backdoor'a (luki zarówno w obszarach technologicznych, jak i organizacyjnych).
Opis skutków	W przypadku materializacji niniejszego ryzyka zwiększa się pole manewru dla potencjalnych atakujących określone usługi. Może to w skutkach prowadzić nie tylko do zainfekowanych, pojedynczych punktów dostępowych, ale również innych aktorów komunikujących się z zaatakowanym podmiotem pośrednio lub bezpośrednio. Wykorzystywanie HUB API może skutkować atakami nie tylko na bank czy TPP, ale także na pośredników, co w skrajnych przypadkach może zwiększać powierzchnię ataków w znaczącym stopniu.
Krytyczność skutków	Średnie
Mityganty	• Należy rozważyć doszczegółowienie/rozszerzenie warunków brzegowych w zakresie konieczności spełnienia określonych wymagań/standardów (bezpieczeństwa) dla nowych podmiotów. • Przeprowadzanie okresowych audytów bezpieczeństwa i testów podatności • Należy rozważyć rozszerzenie dokumentacji związanej z bezpieczeństwem informacji o opis scenariuszy krytycznych oraz politykę ich wykonywania.

Cel biznesowy	Zabezpieczenie danych chronionych
Ryzyko	**Uwierzytelnianie TPP oparte wyłącznie na certyfikatach eIDAS**
Właściciel ryzyka	ASPSP, QTSP
Opis ryzyka	Certyfikaty eIDAS dostarczają wiedzy o instytucji, która uzyskała licencję w zakresie usług określonych w certyfikacie. Certyfikat daje jednoznaczne potwierdzenie, że podmiot taką licencję posiadł, natomiast nie zawierają dodatkowych informacji np. o paszportyzacji, co może narazić bank na wykonanie usługi na rzecz nieuprawnionego TPP. Dodatkowo, weryfikacja certyfikatu powinna, poza jego prawidłowością kryptograficzną, także zapewnić weryfikację ważności certyfikatu.
Opis skutków	Skutkiem może być realizacja usługi dostępu do informacji o koncie lub inicjacji płatności w wyniku zapytania podmiotu nieuprawnionego. Odpowiedzialność za niezgodne z licencją skorzystanie z certyfikatu ponosi TPP, natomiast bank ponosi odpowiedzialność za weryfikację ważności certyfikatu. W przypadku gdy QTSP nieprawidłowo zweryfikuje instytucję płatniczą, która składa wniosek o certyfikat, ponosi wyłączną odpowiedzialność prawną oraz finansową. Mimo to ASPSP może ponieść straty wizerunkowe w przypadku zaistnienia sytuacji kryzysowej.
Krytyczność skutków	Średnia
Mityganty	• Wdrożenie procedur ex-post weryfikujących użycie certyfikatu zgodnie z przyznaną paszportyzacją oraz procedury informowania nadzoru w przypadku złamania zakresu licencji przez TPP. • Weryfikowanie ważności każdego certyfikatu w momencie jego użycia. • Ręczne weryfikowanie podmiotów w odpowiednich rejestrach ponad certyfikat.

2.2.2. Ryzyka operacyjne i regulacyjne

Cel biznesowy	Zapewnienie zgodności regulacji wewnętrznych do wymagań regulatora
Ryzyko	**Niedostosowanie regulacji wewnętrznych do wymagań regulatora**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Brak przeprowadzonej analizy prawnej aktów prawnych/regulacji związanych bezpośrednio z przedmiotem działalności określonego podmiotu (w szczególności opisanych w rozdziale: Zestawienie wszystkich regulacji i aktów prawych związanych z PSD2 na poziomie UE i PL) może powodować brak spójności w stosunku do wewnętrznych regulaminów określonych produktów/usług.
Opis skutków	Brak zgodności w zakresie niniejszego ryzyka może skutkować: • Karami finansowymi • Utratą reputacji
Krytyczność skutków	Średnia
Mityganty	Stałe monitorowanie uwarunkowań regulacyjnego i prawnego wraz z cykliczną analizą ich wpływu na bieżące i planowane produkty oraz usługi.

Cel biznesowy	Zapewnienie zgodności regulacji wewnętrznych do wymagań regulatora
Ryzyko	**Niespełnienie wymagań narzuconych przez PSD2 związanych z obsługą reklamacji**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Dyrektywa PSD2 wprowadziła zmiany w zasadach rozstrzygania reklamacji dotyczących transakcji finansowych. Czas na udzielenie odpowiedzi skrócony został co do zasady do 15 dni roboczych od dnia wpłynięcia reklamacji klienta. W przypadku spraw bardziej skomplikowanych termin rozpatrzenia i odpowiedzi wydłuża się do 35 dni. W związku z powyższymi zmianami instytucje oferujące usługi płatnicze będą miały realnie mniej czasu na udzielanie odpowiedzi niż miało to miejsce przed wejściem w życie powyższej zmiany w przepisach.
Opis skutków	Przekroczenie ustawowego terminu odpowiedzi oznaczało będzie automatyczne uznanie wniosku klienta na jego korzyść. Ponadto nagminne niezastosowanie się do wytycznych narzucanych przez dyrektywę może skutkować obniżeniem reputacji.
Krytyczność skutków	Niska
Mityganty	• Najważniejszym mitygantem adresującym powyższe ryzyko jest przygotowanie adekwatnych procedur i dostosowanie systemów reklamacyjnych do szybkiej analizy zgłaszanych incydentów i odpowiedzi na wnioski klientów. Kluczowe jest także odpowiednie klasyfikowanie poszczególnych zgłoszeń jako związanych z usługami płatniczymi.

Cel biznesowy	Zapewnienie zgodności regulacji wewnętrznych do wymagań regulatora
Ryzyko	**Niespełnienie wymagań i standardów związanych z dostępnością i czasem reakcji API**
Właściciel ryzyka	ASPSP
Opis ryzyka	Zgonie z wytycznymi Rozporządzenia Delegowanego Komisji (UE) 2018/389 „każdy dostawca usług płatniczych prowadzący rachunek, który obsługuje rachunki płatnicze dostępne za pośrednictwem internetu, powinien zapewnić co najmniej jeden interfejs dostępu umożliwiający bezpieczną komunikację z dostawcami świadczącymi usługę dostępu do informacji o rachunku, dostawcami świadczącymi usługę inicjowania płatności i dostawcami usług płatniczych wydającymi instrumenty płatnicze oparte na karcie.” Ponadto dostawcy usług płatniczych prowadzący rachunek odpowiedzialni są także za wyznaczenie KPI dla udostępnionego interfejsu, które będą sformułowane równie rygorystycznie co w przypadku interfejsu stosowanego przez ich klientów. W praktyce oznacza to, że dostawcy usług płatniczych prowadzący rachunek oferujący dedykowane API do wykorzystania przez TPP w celu świadczenia usług inicjowania płatności, dostępu do informacji o rachunku czy potwierdzenie dostępności środków na rachunku będą musieli jasno opisać standardy dostępności.
Opis skutków	W przypadku wystąpienia problemów z dostępem do odpowiednich informacji za pomocą dedykowanego interfejsu dostawcom usług płatniczych powinno być umożliwione korzystanie z interfejsów udostępnionych użytkownikom usług płatniczych w celu uwierzytelnienia i komunikacji z ASPSP (tzw. opcja fallback).
Krytyczność skutków	Wysoka
Mityganty	• Bieżąca analiza dostępności i realizacja okresowych audytów związanych z dostępnością i jakością oferowanego interfejsu. • Zgodnie z art. 33 ust. 6 RTS KNF może zwolnić ASPS z konieczności udostępniania mechanizmu zastępczego przy spełnieniu odpowiednich kryteriów. Skorzystanie z tej opcji, poprzez udowodnienie odpowiedniego poziomu jakości usług pozwoli na ograniczenie kosztów wdrożeniowych po stronie banków.

Cel biznesowy	Utworzenie standardu pracy dostosowanych do wymagań NCA
Ryzyko	**Trudności realizacji zadań na linii ASPSP i TPP a NCA**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Zgodnie z Dyrektywą PSD2 dla każdego kraju wyznaczony jest tylko jeden NCA. Dzięki temu nie ma wątpliwości co do tego, który organ reprezentuje system finansowy każdego kraju, a co za tym idzie – czy dostawca usług płatniczych (PSP) jest autoryzowany, czy nie. Na NCA nałożone jest szereg obowiązków, m.in.: • Przetwarzanie wniosków o rejestrację i podejmowanie decyzji dla wszystkich dostawców usług płatniczych, udzielanie zezwolenia, paszportowanie oraz zmienianie statusu w kraju • Prowadzenie wniosków i rejestrów wszystkich PSP odnośnie rejestracji, autoryzacji, paszportowania, zmiany statusu w kraju • Zarządzanie sporami • Zarządzanie incydentami • Prowadzenie krajowego rejestru oraz komunikacji z organami europejskimi • Komunikacja transgraniczna innymi NCA w przypadku wniosków, takich jak paszporty, spory lub cofnięcie statusu W związku z tym ASPSP i TPP powinny ściśle przestrzegać oraz dostosowywać się do standardów, tak aby NCA sprawnie wykonywali nałożone na nich obowiązki oraz aby komunikacja pomiędzy tymi organami przebiegała bez niepotrzebnych barier i utrudnień.
Opis skutków	• Tak duża ilość obowiązków może skutkować ich niedopełnieniem, trudnościami komunikacyjnymi i przedłużeniem procesów realizowanych na styku NCA i uczestników rynku finansowego. • Brak spójnego modelu pracy wszystkich ASPSP i TPP z NCA może skutkować powstawaniem rozbieżności między poszczególnymi krajami.
Krytyczność skutków	Średnia
Mityganty	• Opracowanie szczegółowych standardów procesowych związanych z realizacją procesów związanych z wymogami Dyrektywy. • Bieżąca realizacja analiz prawnych w zakresie prowadzonej działalności i zgodności z wymogami stawianymi przez regulatorów.

Cel biznesowy	Zapewnienie zgodności regulacji wewnętrznych do wymagań regulatora
Ryzyko	**Wzrost liczby reklamacji**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Wraz z wejściem w życie Dyrektywy PSD2 zmianie uległy elementy postępowania związane z obsługą i rozpatrywaniem nieautoryzowanych transakcji. Najważniejsze aspekty związane z obowiązkami dostawców usług płatniczych: • Zasady odpowiedzialności za nieautoryzowane transakcje • Wysokość kwoty odpowiedzialności płatnika za nieautoryzowane transakcje • Termin rozpatrywania reklamacji związanych z korzystaniem z usług płatniczych PSD2 nakłada na dostawców usług płatniczych odpowiedzialność za nieautoryzowane transakcje płatnicze. Wraz z rozszerzeniem zakresu i poziomu odpowiedzialności dostawców rośnie ryzyko związane z nadużyciami klientów i ze zwiększoną aktywnością przestępców wykorzystujących nowe realia PSD2, w których przeciętni klienci mogą się zagubić, jeżeli nie otrzymają odpowiedniego wsparcia informacyjnego i edukacyjnego.
Opis skutków	W przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca zobowiązany jest do zwrócenia kwoty konsumentowi bez zwłoki, co w praktyce oznacza konieczność realizacji zwrotu do końca następnego dnia roboczego od momentu wykrycia takiego zdarzenia. Dopiero po dopełnieniu tego obowiązku dostawca może oceniać czy realizacja danego zwrotu była uzasadniona. Ponadto w przypadku niezastosowania procedury silnego uwierzytelniania klient nie ponosi żadnej odpowiedzialności za nieautoryzowane transakcje, chyba że dopuścił się oszustwa lub działał w złej wierze. Dostawcy usług płatniczych w przypadku dużego wzrostu liczby fraudów narażeni będą zarówno na konsekwencje finansowe, jak i reputacyjne.
Krytyczność skutków	Średnia
Mityganty	• Należy zapewnić funkcjonujące mechanizmy SCA (Strong Customer Authentication), polegające na dwuskładnikowym uwierzytelnieniu np. logowaniu do systemu określonego usługodawcy przy wykorzystaniu jednorazowego kodu SMS. Dzięki temu zapewniony zostaje wyższy poziom wiarygodności klienta dokonującego określone operacje systemowe/transakcyjne. ASPSP oraz TPP zapewniając mechanizmy silnego uwierzytelnienia zapobiega potencjalnym roszczeniom klientów spowodowanych nieautoryzowanych transakcji/operacji. • Warto dokonać analizy w zakresie możliwości oraz zasadności wykorzystania rozwiązań typu Fraud Detection/Prevention Systems (FDS) pozwalających na wykrywanie transakcji posiadających znamiona nielegalnych. • Edukacja klientów w zakresie zmian, jakie niesie za sobą PSD2. Należy dokonać analizy w zakresie skutecznego przekazu trafiającego do jak największego grona klientów.

2.2.3. Ryzyka biznesowe

Cel biznesowy	Utrzymanie przychodowości
Ryzyko	**Utrata klientów na rzecz konkurencji**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Dyrektywa PSD2 u swoich podstaw ma na celu zapewnienie większej konkurencyjności i ułatwienie klientom dostępu do informacji i środków na rachunkach. W praktyce oznaczać to może, że walka o klienta rozgrywać się będzie nie tylko między bankami, ale także pomiędzy innymi uczestnikami rynku. Jest to efekt zamierzony w zamyśle D,yrektywy, natomiast z perspektywy uczestników rynku stanowi on wyzwanie, któremu będą musieli stawić czoła. Migracja klientów pomiędzy instytucjami jest zjawiskiem naturalnym, jednak PSD2 może w znaczącym stopniu zwiększyć skalę i tempo w jakim będzie się ona odbywać.
Opis skutków	Konsekwencją aktywizacji banków i TPP w zakresie działań związanych z Open Bankingiem pojawią się podmioty, które nie dostosują swojej strategii, działań komunikacyjnych i operacyjnych do nowych realiów, czego skutkiem może być odejście znacznej liczby klientów, a co za tym idzie – obniżenie przychodowości. Zmiany związane z PSD2 mogą się odbić na wybranych instytucjach w negatywny sposób, jeżeli nie będą w stanie utrzymać pozytywnego wyniku netto migracji klientów, tj., jeżeli liczba klientów odchodzących będzie większa niż tych przychodzących. Skutki migracji klientów mogą być najbardziej odczuwalne zwłaszcza w przypadku małych banków i TPP których strategia dotąd nie przewidywała pełnego wykorzystania szans związanych z otwarciem rynku i możliwością rozwijania usług i produktów. Bardzo ważnym elementem mogącym mieć wpływ na rozwój sytuacji mogą być duże międzynarodowe podmioty, które będą chciały rozszerzyć swoje dotychczasowe usługi o płatności czy dostarczanie informacji o kontach bankowych klientom (przykładami mogą być Facebook czy Google, które już dziś posiadają bardzo silną relację z klientami).
Krytyczność skutków	Średnia
Mityganty	• Strategia rozwoju usług i produktów • Komunikacja, budowanie i utrzymywanie silnej relacji z klientem • Dostosowanie oferty cenowej, zaproponowanie wartości dodatkowych • Badania rynku • Badania potrzeb klientów

Cel biznesowy	Utrzymanie przychodowości Zapewnienie zgodności regulacji wewnętrznych do wymagań regulatora
Ryzyko	**Utrata lub znaczące ograniczenie bieżącej relacji z klientem i obniżenie przychodowości**
Właściciel ryzyka	ASPSP, TPP
Opis ryzyka	Wraz ze wzrostem popularności rozwiązań oferowanych przez TPP istnieje ryzyko, że dostawcy usług płatniczych prowadzący rachunek mogą stanąć przed problemem związanym z efektywnym dotarciem do bazy swoich klientów, którzy z usług finansowych korzystać będą za pośrednictwem rozwiązań zewnętrznych opartych na API. Wraz z utrudnieniem w utrzymaniu bieżącej relacji z klientami ASPSP będą musiały stawić czoła problemowi związanemu z obniżeniem przychodowości na kliencie poprzez zmniejszenie wolumenu transakcji, utratę potencjału do cross i up-sell'u.
Opis skutków	Ryzyko to ma dwa potencjalne skutki w zakresie komunikacji z klientem: 1. Utrudnienie komunikacji marketingowej i działań sprzedażowych. Ryzyko to może docelowo przełożyć się na obniżenie wyników biznesowych związanych z brakiem wzrostu uproduktowienia klientów. Utrata relacji z konsumentami może długoterminowo mieć negatywny wpływ na możliwości rozwoju instytucji. 2. Utrata możliwości dostarczenia informacji dotyczących zmian regulaminów czy zmian w TOiP.
Krytyczność skutków	Średnia
Mityganty	1. Komunikacja marketingowa i sprzedażowa: • Wsparcie strategii sprzedażowej rozwojem funkcjonalnym, aby jak najlepiej konkurować z pojawiającymi się na rynku konkurencyjnymi rozwiązaniami. • Proaktywne wykorzystanie możliwości, jakie daje PSD2 i uzupełnienie strategii pozyskiwania klienta i sprzedaży o dane pozyskiwane za pomocą API z innych ASPSP. • Regularne badania potrzeb klientów w ramach poszczególnych segmentów. Badania takie powinny uzupełniać wiedzę ASPSP o informacje, z jakich funkcjonalności klienci chcieliby korzystać, jakie rozwiązania dostępne na rynku są z ich perspektywy interesujące i dlaczego. • Praca nad stałym rozwojem kanałów zdalnych, metod płatności i proponowanie wartości dodanych klientom w celu stworzenia środowiska, które spełnia potrzeby klientów wykraczające poza realizację płatności i sprawdzanie informacji o rachunkach. 2. Komunikacja związana z regulaminami: • ASPSP powinny dążyć do tego, aby komunikacja związana ze zmianami regulaminowymi dostarczana była więcej niż w jednym kanale. Uzyskanie zgód klientów na dostarczenie komunikacji drogą e-mail zdaje się być docelowym rozwiązaniem pozwalającym na zmitygowanie ryzyka dotyczącego niedostępności informacji ze względu na niekorzystanie przez klienta z kanałów zdalnych. • Regularne pozyskiwanie i aktualizacja danych kontaktowych klientów, w tym numerów telefonów i adresów e-mail.

Poniższa tabela zawiera zagregowany wykaz przeanalizowanych ryzyk w podziale na ich kategorie oraz oszacowaną krytyczność skutków.

	Ryzyka związane z bezpieczeństwem informacji danych chronionych	Ryzyka operacyjne i regulacyjne	Ryzyka biznesowe
Wysokie	• Wyciek danych uwierzytelniających grupy klientów • Wyciek danych transakcyjnych grupy klientów • Wyciek danych bankowych grupy klientów • Wyciek danych osobowych grupy klientów • Nieautoryzowany dostęp do kluczy kryptograficznych służących do uwierzytelniania • Wyciek dokumentacji architektury systemowej IT dostawcy usługi • Utrata danych dowodowych • Wzrost liczby fraudów • Ataki na API/Aplikacje	• Niespełnienie wymagań i standardów związanych z dostępnością i czasem reakcji API	
Średnie	• Wyciek danych uwierzytelniających pojedynczego klienta • Wyciek danych transakcyjnych pojedynczego klienta • Wyciek danych bankowych pojedynczego klienta • Wyciek danych osobowych pojedynczego klienta • Większa powierzchnia ataku ze względu na zwiększenie liczby aktorów • Uwierzytelnianie TPP oparte wyłącznie na certyfikatach eIDAS	• Niedostosowanie regulacji wewnętrznych do wymagań regulatora • Trudności realizacji zadań na linii ASPSP/TPP a NCA • Wzrost liczby reklamacji	• Utrata klientów na rzecz konkurencji • Utrata lub znaczące ograniczenie bieżącej relacji z klientem i obniżenie przychodowości
Niskie		• Niespełnienie wymagań narzuconych przez PSD2 związanych z obsługą reklamacji	

Rynek po PSD2 – aspekty biznesowe

3.1. Strategie banków

Dyrektywa PSD2 otworzyła zupełnie nowe perspektywy przed rynkiem finansowym w całej Europie. Z jednej strony stanowi ona zagrożenie dla ustanowionego dotąd ładu, z drugiej pozwala na zwiększenie konkurencyjności i stworzenie nowych usług oraz modeli biznesowych. Dyrektywa wraz ze swoim wejściem w życie nie zrewolucjonizowała rynku, a zaledwie wprowadziła w ruch powolny proces zmian, które stopniowo zmieniać będą oblicze bankowości i usług finansowych. Pomimo że powstało już kilka usług związanych z PSD2 to wciąż nie jest jasne w jakim kierunku pójdzie cały rynek. Związane jest to z wieloma czynnikami począwszy od tempa, w jakim powstawać będą TPP, przez zmieniającą się percepcję i oczekiwania klientów aż po strategie, jakie przyjmą banki.

Rynek bankowy w Polsce był przez ostatnie lata bardzo innowacyjny w zakresie rozwiązań płatniczych i szerzej – finansów cyfrowych. Bardzo wiele usług oferowanych klientom budowanych było na współpracy banków zarówno z dostawcami zewnętrznymi, jak i pomiędzy samymi bankami. Do tego typu usług należały między innymi BLIK, płatności pay-by-link czy usługi dodatkowe jak doładowania telefonów prepaid, płatności za parkowanie czy bilety komunikacji miejskiej. Uważamy, że te doświadczenia powinny przełożyć się na otwartość banków do wyjścia naprzeciw nowym realiom.

> “
>
> Zauważamy, że rozwój rynku dotkniętego przez PSD2 jest powolny, ale nieunikniony.
>
> Michał Bonczysty, Credit Agricole

Aktualnie, ze względu na to, że proces rejestracji i licencjonowania TPP jest stosunkowo trudny i czasochłonny, banki są w uprzywilejowanej pozycji i mają potencjał do stania się liderami rynku w zakresie wykorzystania nowych możliwości biznesowych, jakie niesie ze sobą PSD2. Z jednej strony wymagania związane z wdrożeniem API pozwoliły im na zdobycie cennych doświadczeń, także w ramach współpracy z fintechami, w zakresie budowania rozwiązań technologicznych i biznesowych, a z drugiej strony wciąż cieszą się dużym zaufaniem klientów w zakresie dostarczania bezpiecznych usług finansowych i mają z nimi bezpośrednią relację i możliwość efektywnej, bieżącej komunikacji. Czynniki te są bardzo cennym kapitałem, który może zostać wykorzystany do utrzymania banków w roli liderów rynkowych w zmieniającym się krajobrazie usług i produktów finansowych. W innym przypadku banki zależne będą, przynajmniej w pewnym zakresie, od działań pojawiających się dostawców zewnętrznych. W takim wypadku bardzo realnym zagrożeniem dla banków będzie utrata bieżącej relacji z klientami i zepchnięcie do pasywnej roli dostawców rachunków bankowych, a co za tym idzie – utratę przychodowości i potencjału sprzedażowego.

> “
>
> Kluczem do sukcesu w rzeczywistości po PSD2 jest współpraca.

Po spełnieniu wymagań ustawowych banki będą musiały zdecydować, jakie podejmą dalsze kroki w ramach zmian związanych z PSD2. Ich potencjalne strategie w podejściu do zmian związanych z dyrektywą można podzielić na dwie grupy. Z jednej strony są banki, które będą próbowały bardzo aktywnie wykorzystać szanse związane z Dyrektywą, z drugiej natomiast będą te, które potraktują PSD2 głównie jako zagrożenie i będą pasywnie starały się chronić przed zmianami i ograniczą się do spełnienia zgodności z wymogami Dyrektywy. W każdej z grup podejście poszczególnych banków do strategii produktowej i komunikacyjnej oraz do pojawiających się możliwości współpracy z TPP może być inne.

Banki decydujące się na strategię aktywnego wykorzystania możliwości jakie niesie ze sobą PSD2 będą mogły to uczynić na kilka sposobów. Pierwszym, który przychodzi na myśl jest samodzielne budowanie rozwiązań oferujących nowe metody płatności i agregacji danych klientów. Takie podejście wiązać się będzie najprawdopodobniej z zaangażowaniem dość dużego kapitału na rozwój i działania komunikacyjne, natomiast w zamian banki nie będą musiały dzielić się zyskami ze swojego przedsięwzięcia z podmiotami zewnętrznymi. Drugim możliwym podejściem będzie budowanie usług z partnerami zewnętrznymi, zarówno w ramach współpracy, jak i poprzez przejmowanie wybranych Fin-Techów. Trzecim, najmniej agresywnym podejściem, byłoby rozszerzanie usług udostępnianych przez API lub budowanie nowych form współpracy z TPP, ograniczając przynajmniej częściowo rolę banku do roli dostawcy technologii w zamian za udział w zyskach i utrzymanie bieżącej relacji z klientem.

Kluczowym elementem w przypadku aktywnego podejścia do zmian będzie budowanie rozwiązań, któ-

re spełnią oczekiwania i potrzeby klientów, zapewnią wartość dodaną i spełniać będą najwyższe standardy w zakresie User Experience. Wykorzystanie narzędzi takich jak badania z użytkownikami, realizacja testów użyteczności czy włączanie użytkowników końcowych do procesu projektowania rozwiązań, pozwoli na najlepsze dopasowanie nowych produktów i usług do potrzeb rynku. Już dzisiaj duża część polskich banków realizuje działania związane z badaniem użytkowników, więc wykorzystanie wcześniej uzyskanej wiedzy i dalsze rozszerzanie projektów badawczych może sprawić, że rynek bankowy skutecznie będzie mógł rywalizować z TPP, które na przestrzeni kilku przyszłych lat na pewno będą się pojawiały w Polsce.

> “
>
> Nie mam wątpliwości co do tego, że banki pracują nad innymi, dużo bardziej oryginalnymi produktami, o których teraz jeszcze pewnie nikt mówić nie chce, bo stanowi to obszar bezpośredniej konkurencji.

Innym podejściem będzie ograniczenie się jedynie do spełnienia wymagań regulacyjnych przez wybrane banki. Strategia taka w krótkim i średnim terminie oznaczać będzie ograniczenie kosztów związanych z tworzeniem i udostępnianiem nowych usług, jednak długoterminowo może wiązać się ze spadkiem konkurencyjności, a co za tym idzie przychodowości. Z jednej strony banki zrezygnują z budowania nowych strumieni przychodów, z drugiej natomiast może okazać się, że także dotychczasowe źródła ulegną pomniejszeniu. Najbardziej oczywistym zagrożeniem ze strony podmiotów trzecich będzie przejęcie bieżącej relacji z klientami co za sobą pociągnie ograniczenie możliwości sprzedażowych, spadek zaangażowania klientów w banku i przejście jedynie do roli dostawcy pieniądza. Kolejnym elementem może być odejście klientów od tradycyjnych metod płatności jak karty czy pay-by-link na rzecz usług PIS, co spowoduje dalsze obniżanie przychodowości z obecnych modeli biznesowych. Mimo że przyjęcie powyższej, defensywnej strategii wydaje się mniej ryzykowne, to docelowo jest ona raczej sposobem na chwilowe ignorowanie zagrożenia i długoterminową utratę pozycji rynkowej.

Niezależnie od wybranych strategii, kluczowym elementem długoterminowego sukcesu banków będzie dostarczanie najwyższej jakości produktów i usług odpowiadających oczekiwaniom klientów.

3.2. Kierunki rozwoju i wyzwania dla rynku

Samo wdrożenie Dyrektywy PSD2 stanowi jedynie punkt wyjścia dla potencjalnych zmian na rynku szeroko pojętych cyfrowych finansów, zarówno w Polsce, jak i na całym obszarze geograficznym obowiązywania Dyrektywy. Aktualnie można jedynie zarysować potencjalne wyznaczniki rozwoju rynku, które stworzą przestrzeń dla urealnienia się konkretnych scenariuszy biznesowych.

Konkurencyjność rynku

Rozszerzenie szeroko rozumianego rynku płatności elektronicznych o graczy spoza sektora bankowego – a jest to jedno z założeń, leżących generalnie u podstaw wdrożenia Dyrektywy, bezwzględnie wpłynie na poziom konkurencyjności rynku. Z jednej strony banki, które na rynku polskim okazały się być pierwszymi podmiotami, które aktywnie wykorzystują PSD2, wdrażając nowe mechanizmy takie jak AIS czy CAF, będą je wykorzystywać do wzmocnienia swojej pozycji na rynku. Może to skutkować zwiększeniem się dystansu banków – liderów bankowości cyfrowej – w stosunku do banków małych lub nie rozwijających wystarczająco dynamicznie tych kanałów dystrybucji. Rynek podmiotów pozabankowych – TPP może przejść klasyczną ścieżkę rynkową – poprzez różnorodność i wielość graczy w początkowym etapie po naturalną „oligopolizację” – przejście w rynek 2-3 podmiotów, które z kolei uzyskają potencjał do realnej konkurencji z bankami krajowymi w obszarze płatności oraz budowania relacji z klientem czy nawet ekspansji międzynarodowej. Generalnie już teraz takie podmioty jak PayU czy Dialcom24/PayPro są częścią większych pan-europejskich czy wręcz globalnych podmiotów. Kolejnym czynnikiem zwiększającym konkurencyjność analizowanego rynku o podmioty pozabankowe, może być wykorzystanie narzędzi PSD2 przez przedstawicieli grupy GAFA (Google, Amazon, Facebook, Apple). Jakkolwiek podmioty te starają się budować swoje rozwiązania w zakresie płatności (np. Google Pay, Apple Pay), to zastosowanie narzędzi PSD2 może ich na trwałe wpisać w krajobraz tego rynku, realnie zwiększyć wartość dodaną dla ich szerokich baz klienckich oraz może

> “
>
> Nie widzę jeszcze aktywności GAFA, podejrzewam, że czekają na popularyzację systemu, żeby nie wchodzić do takiego, który się jeszcze buduje, a do takiego, który działa.
>
> Michał Pierzgalski

pozwolić wejść na nowe obszary produktowe, oprócz samych płatności, np. związane z potwierdzaniem tożsamości (usługa CAF) czy zarządzaniem finansami osobistymi (usługa AIS).

Problem „aplikacji wiodącej"

Aktualnie, użytkownik rozwiązań z zakresu finansów cyfrowych dąży do uproszczenia i „ekonomizacji". Eksperymentuje z kilkoma rozwiązaniami i usługami, ale docelowo jedna lub dwie aplikacje finansowe gromadzą gros jego aktywności. Dyrektywa PSD2 daje narzędzia innym podmiotom, aby zabrały rozwiązaniom bankowym tytuł do pełnienia roli finansowej „aplikacji wiodącej" dla klienta. Przykład sukcesów rynkowych (również w Polsce) rozwiązań typu aplikacja Revolut oraz potencjał rozwoju bardzo popularnych aplikacji sklepowych (Rossmann, Żabka) o funkcje płatnicze wskazuje, że istnieje ryzyko sprowadzenia banków do roli źródła pieniądza i ograniczenia ich wpływu na bieżące zarządzanie relacjami z klientami. Banki, które nie wypracują aktywnej strategii w tym zakresie, mogą rzeczywiście w dłuższej perspektywie być skazane na taką rolę, na rzecz innych, dających lepszą ergonomię użytkowania i funkcjonalność aplikacji pozabankowych, ale i bankowych – wykorzystujących efektywnie narzędzia takiej jak PIS, AIS i inne.

> "
>
> Mamy sytuację, w której banki mogą, ale nie muszą, stracić swoją pozycję pierwszego wyboru, jeśli chodzi o zarządzanie danymi finansowymi.

Problem biznesowych i wizerunkowych konsekwencji kompromitacji danych

Szereg badań wskazuje, że klienci oczekują od banków zapewnienia bezpieczeństwa w kanale elektronicznym, stąd też potencjalne fraudy, incydenty związane z ujawnieniem tajemnicy bankowej, jakkolwiek mające swe źródła w nieodpowiednim działaniu systemów TPP będą z dużym prawdopodobieństwem negatywnie wpływać na wizerunek banków, do których to klienci zwrócą się z reklamacjami i protestami. Odpowiednie zarządzanie ryzykiem operacyjnym, ale również właściwe zarządzanie incydentami oraz samą polityką informacyjną i PR będzie kluczowe dla mitygacji przez banki tego typu ryzyk w nowym środowisku regulacyjno-technicznym wynikającym z PSD2.

> "
>
> Open banking, czyli możliwość pozyskiwania informacji o kliencie, czy o rachunku klienta, danych dotyczących jego transakcji, czy nawet możliwość inicjowania płatności, to tak naprawdę nie są nowe usługi, tylko usługi, które na rynku już były stosowane od wielu lat. Co ta Dyrektywa zmieni, to przede wszystkim upowszechni je i sprawi, że stają się one bezpłatne dla graczy, którzy chcą z nich korzystać.
>
> Michał Bonczysty, Credit Agricole

Problem zmniejszenia przychodów z bieżącej działalności banków

Wejście TPP w obszary produktowe zarezerwowane do tej pory dla banków wiąże się z ryzykiem zmniejszenia przychodów z bieżącej działalności oraz braku wykorzystania potencjału biznesowego nowych usług. Na rynku krajowym w pierwszym rzędzie istotny jest wątek przychodów z tzw. pay-by-linków, cały czas najbardziej popularnego narzędzia płatności elektronicznych, z których banki czerpią dochód pochodzący od integratorów płatności, a pośrednio od merchantów – przy wykorzystaniu narzędzia inicjacji płatności bazującego na PSD2, dochód ten będzie zmniejszony lub w ogóle zniwelowany. Mechanizmy PSD2 będą mogły służyć również jako narzędzia pomocnicze do weryfikacji historii rachunku i docelowo zdolności kredytowej w bankach, co również może przyczynić się do ograniczenia przychodów w sprzedaży i obsłudze produktów kredytowych. Innym obszarem jest weryfikacja tożsamości, niezbędna w wielu procesach on-line, rozwiązania typu CAF mogą spowodować obejście wypracowywanego modelu biznesowego użycia tożsamości bankowej, gwarantującego instytucjom finansowym możliwość zarabiania na udostępnianiu danych służących do takiej zdalnej identyfikacji.

> "
>
> Ryzyko dla banków, posiadających do tej pory bezpośredni kontakt może polegać na tym, że PSU nie będzie już odczuwał potrzeby takiego kontaktu, ponieważ większość operacji będzie mógł wykonać za pośrednictwem podmiotów trzecich.

PSD2 – narzędzie przyspieszonej transformacji cyfrowej

Sektor finansowy – przynajmniej w Polsce – jest jednym z najbardziej „ucyfrowionych" rynków – świadczą o tym chociażby liczby aktywnych użytkowników bankowości mobilnej (ok. 13 mln – dane PRNEWS za 3 kw. 2019) oraz internetowej (ok. 18 mln – dane ZBP za 2 kw. 2019). Te szerokie rzesze klientów detalicznych (ale co za tym idzie firmowych i korporacyjnych), staną się docelowymi grupami usług, które będą mogły powstawać na bazie mechanizmów wynikających z PSD2. Dotyczy to również usług, w których dostawcami będą podmioty, do tej pory działające poza sektorem finansowym, tak jak na przykład wskazane wcześniej podmioty z rynku handlu detalicznego. Przyczyni się to do cyfryzacji „transakcyjnej" pozafinansowych domen życia gospodarczego, ponieważ klienci będą mogli stosować znane narzędzia bazujące na dostępie do bankowości elektronicznej do takich usług jak dostęp do e-paragonu, dostęp do usług ubezpieczeniowych w kanale on-line, dostęp do usług medycznych w formule zdalnej i inne. Wspomniana wyżej popularność bankowości cyfrowej zostanie więc „zlewarowana" na rzecz innych branż i obszarów aktywności konsumenckiej i biznesowej.

> "
>
> Bezwzględnie będzie to katalizatorem innowacji. Z drugiej strony banki, które do tej pory nie były zbyt innowacyjne będą musiały zrobić krok do przodu, aby uniknąć stania się tym bankiem, który jest tylko dostawcą infrastruktury i bezpośredniej relacji do klienta nie przejęła konkurencja.
>
> Krzysztof Pulkiewicz, BanqUP

Doświadczenie i przekonania użytkowników a popularyzacja rozwiązań bazujących na PSD2

Rozwój rynku wynikającego z wdrożenia Dyrektywy PSD2 w znacznej mierze będzie wynikał z realnych wdrożeń biznesowych poszczególnych graczy – tak banków, jak i TPP, ergonomii i bezpieczeństwa plasowanych na rynku nowych i rozwijanych aplikacji. Dopiero to rynkowe „rozpoznanie bojem" pozwoli skonfrontować wskazane powyżej hipotezy dotyczące kierunków rozwoju rynków z doświadczeniami końcowych użytkowników i ich realnymi zachowaniami, a na koniec przełoży się na to, w jaki sposób będzie się kształtował rynek cyfrowych finansów po wdrożeniu analizowanej Dyrektywy.

3.3. Case Studies

Wejście w życie dyrektywy PSD2 otworzyło nowy rozdział rozwoju usług finansowych. Rynek nowych usług jest jeszcze stosunkowo młody i w ciągu kilku najbliższych lat liczba i kompleksowość oferowanych usług zapewne będzie stale wzrastała. Obecnie oferowane usługi wciąż można uznawać za pierwsze kroki w kierunku wykorzystania potencjału, jaki niesie ze sobą PSD2, jednak można już zauważyć, że na rynku są podmioty ambitnie i aktywnie podchodzące do wykorzystania nowych szans. Poniżej przedstawiamy trzy wybrane przypadki użycia nowych modeli w zakresie oferowania nowych usług zarówno w modelu B2C, jak i B2B.

banqUP – APIHub

banqUP jest czwartym podmiotem w Polsce, po Blue Media, PayU i Kontomatiku, który znalazł się w rejestrze licencjonowanych dostawców świadczących usługi AIS, prowadzonym przez KNF.

banqUP rozwija platformę technologiczną, APIHub, która pozwala firmie i jej partnerom sprawniej integrować się z systemami banków i pozyskiwać na tej drodze informacje o rachunkach, co jest konieczne w przypadku takich usług jak integracja kont bankowych, ocena zdolności kredytowej, potwierdzanie tożsamości czy też finance managing.

banqUP swoją działalność opiera na udostępnianiu innym podmiotom jednej platformy, już podłączonej do interfejsów europejskich banków, co pozwala klientom banqUP na połączenie się z jednym dostawcą, w efekcie upraszczając cały proces. Obecnie firma świadczy tylko usługę AIS, w planach jest rozbudowa o PIS i stworzenie pełnego „TPP-as-a-Service", co ułatwiłoby fintechom wejście na rynek związany z usługami pod PSD2. Firma sama nie świadczy usług dla użytkownika końcowego, swoją działalność opierając na odpłatnym dostępie do huba. Płatność odbywa się na zasadzie pay-as-you-go. Klienci mają z nią jednak kontakt, jako że do poprawnego działania usługi niezbędna jest rejestracja PSU w serwisie banqUP, wybranie ASPSP i wyrażenie zgód.

Rozwiązanie banqUP pozwala połączyć się z bankami korzystającymi ze standardów:

- Berlin Group Standard
- PolishAPI (PL)
- Open Banking UK
- SBA (SK)
- Borica (BG)
- STET
- Wordlin

Możliwe jest również połączenie z wybranymi bankami, niekorzystającymi z żadnego w wyżej wymienionych standardów.

PSD2Hub pozwala odczytywać dane z konta klienta, za pośrednictwem usługi AIS, co w efekcie pozwala analizować źródła przychodów PSU, historię transakcji transakcje itp. BanqUP może również wykonać analizy za swojego klienta, co może przynieść efekty podobne do wykorzystania danych z mediów społecznościowych czy Big Data.

Firma udostępnia także sandbox, pozwalający na testowanie rozwiązań przed udostępnieniem ich na rynku.

Do połączenia z platformą APIHub nie jest potrzebna licencja TPP, co dla wielu podmiotów może oznaczać znaczne ułatwienie rozpoczęcia świadczenia usług – skorzystać z tej możliwości można po pomyślnym przejściu weryfikacji przez banqUP i jedynie w modelu TPP-as-a-Service – elementy rozwiązania nie mogą być implementowane w infrastrukturze klienta. Korzystanie z APIHub nie wymaga implementacji silnego uwierzytelnienia ani samodzielnego onboardingu do ASPSP – PSD2Hub jest już po procesie onboardingu, który nie musi być powtarzany, a silne uwierzytelnianie jest już jego elementem.

Alior Bank – Sprzedaż produktów kredytowych w oparciu o AIS

Alior Bank oferuje klientom wybranych banków (PKO BP, Pekao S.A., Santandera i ING Banku Śląskiego) możliwość ubiegania się o kredyt w Alior Banku bez wcześniejszego przedstawienia zaświadczenia o zarobkach. Aby skorzystać z tej usługi, nie trzeba być klientem Alior Banku.

Działanie Alior Banku opiera się na usłudze AIS – za zgodą klienta bank pobiera informacje o jego rachunkach w innych bankach i wykorzystuje uzyskane informacje do oceny zdolności kredytowej. Proces udzielenia zgody przebiega on-line, Alior Bank przesyła SMS-em link do regulaminu i formularza, który klient wypełnia, a następnie zostaje przeniesiony na stronę swojego banku, w którym zatwierdza żądanie dostępu do danych o swoich rachunkach. Potwierdzenie tej dyspozycji odbywa się za pomocą mechanizmu SCA.

Obecnie taki mechanizm wnioskowania o kredyt dostępny jest tylko w wybranych placówkach banku i w call center, z końcem stycznia Alior Bank chce wprowadzić taką możliwość w każdym oddziale, a także w bankowości elektronicznej. W drugiej połowie 2020 roku bank chce także umożliwić klientom przeniesienie swoich depozytów z innych banków do Alior Banku.

W przypadku call center proces wygląda w następujący sposób:

1. Klient zainteresowany kredytem łączy się z konsultantem, który wytłumaczy, jak działa procedura i udziela wszystkich niezbędnych informacji.
2. Po wyrażeniu przez klienta chęci kontynuowania konsultant przesyła klientowi wiadomość SMS zawierającą odnośnik do formularza, w którym kredytobiorca może wyrazić zgodę na usługę AIS.
3. Następnie, w banku, do którego trafiają jego regularne przychody lub innym, wybranym przez siebie, potwierdza zgodę na udostępnienie danych.
4. Procedura nie jest natychmiastowa, proces trwa „do jednego dnia roboczego". Po przeprocesowaniu wniosku klient otrzymuje decyzję czy kredyt na kwotę, o którą wnioskował może być mu udzielony.
5. Proces może zostać zakończony w oddziale – gdzie klient udaje się w celu podpisania umowy bądź zdalnie, za pośrednictwem kuriera.

Według przedstawicieli Alior Banku takie rozwiązanie przyspiesza proces wnioskowania, nie tylko po stronie klienta, ale także ułatwia pracę zaangażowanemu doradcy, który nie musi już weryfikować dostarczonego przez klienta dokumentu. Usprawnienie procesu kredytowego może przełożyć się na zmniejszenie kosztów po stronie banku i zwiększenie sprzedaży produktów kredytowych.

Alior Bank odnotował już sprzedaż kredytów za pomocą tego mechanizmu, jednak nie komentuje jeszcze wyników sprzedaży.

ING Bank Śląski – Usługa podglądu rachunków innych banków

Jednym z pierwszych banków oferujących usługę AIS był ING Bank Śląski, udostępniający swoim klientom możliwość podglądu salda rachunków prowadzonych przez inne banki: PKO BP, mBank, Pekao S.A., Millennium i BNP Paribas. Wyświetlanie stanu innego konta można włączyć w serwisie bankowości elektronicznej ING, nie jest to jednak rozwiązanie intuicyjne i może być stosunkowo trudne do odszukania przez część klientów. Funkcjonalność ta została wprowadzona stosunkowo niedługo po wejściu w życie Dyrektywy, jednak początkowo korzystanie z niej przysparzało problemów – próby uzyskania dostępu do innego konta skutkowały błędami.

Obecnie podłączenie kont jest możliwe i w pełni funkcjonalne. Klient zleca jego realizację w serwisie

transakcyjnym ING, a następnie autoryzuje operację w serwisie drugiego banku. Po krótkiej konfiguracji i niedługim czasie oczekiwania informacje o stanie konta dostępne są w serwisie banku ING, a klient może w dowolnym momencie wyłączyć i włączyć ich prezentację. Dostęp do danych z innego banku przydzielany jest na rok i musi być potwierdzany co 90 dni.

Bank ING informuje, że klienci mają również możliwość użycia danych z innego banku podczas wnioskowania o pożyczkę – zamiast dostarczać wyciągi z konta w formie papierowej, czy jako pdf, klient może wykorzystać usługę AIS i tak jak w przypadku Alior Banku – bank ING będzie w stanie sam pobrać wymagane informacje.

Baza wiedzy

Przepisy, regulacje

Sygnatura	Nazwa	Link	Data	Treść/tytuł
(UE) 2015/2366	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366		29.11.2018	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)
(UE) 910/2014	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014		29.11.2018	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
Dz. U. 2018 poz. 1075	Ustawa z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw	link	10.05.2018	USTAWA z dnia 10 maja 2018 r.o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającą dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającą dyrektywę 2007/64/WE (Dz. Urz. UE L 337 z 23.12.2015, str. 35) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawę z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ustawę z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami, ustawę z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, ustawę z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, ustawę z dnia 12 maja 2011 r. o kredycie konsumenckim, ustawę z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym, ustawę z dnia 15 grudnia 2017 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw oraz ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 208 z 02.08.2013, str. 68, Dz. Urz. UE L 321 z 30.11.2013, str. 6, Dz. Urz. UE L 165 z 04.06.2014, str. 31, Dz. Urz. UE L 11 z 17.01.2015, str. 37, Dz. Urz. UE L 143 z 09.06.2015, str. 7, Dz. Urz. UE L 328 z 12.12.2015, str. 108, Dz. Urz. UE L 151 z 08.06.2016, str. 4, Dz. Urz. UE L 171 z 29.06.2016, str. 153, Dz. Urz. UE L 336 z 10.12.2016, str. 36, Dz. Urz. UE L 20 z 25.01.2017, str. 4, Dz. Urz. UE L 144 z 07.06.2017, str. 14, Dz. Urz. UE L 310 z 25.11.2017, str. 1, Dz. Urz. UE L 322 z 07.12.2017, str. 27 oraz Dz. Urz. UE L 345 z 27.12.2017, str. 27

(UE) 2019/411	Rozporządzenie Delegowane Komisji (UE) 2019/411	link	27.11.2017	ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2019/411 z dnia 29 listopada 2018 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych określających techniczne wymogi w zakresie opracowania, obsługi i prowadzenia elektronicznego centralnego rejestru w dziedzinie usług płatniczych i w zakresie dostępu do informacji w nim zawartych (Tekst mający znaczenie dla EOG)
(UE) 2019/410	Rozporządzenie Wykonawcze Komisji (UE) 2019/410	link	14.11.2017	ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2019/410 z dnia 29 listopada 2018 r. ustanawiające wykonawcze standardy techniczne w odniesieniu do szczegółów i struktury informacji przekazywanych w dziedzinie usług płatniczych przez właściwe organy Europejskiemu Urzędowi Nadzoru Bankowego zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366 (Tekst mający znaczenie dla EOG)
	Plan działania w sprawie detalicznych usług finansowych	link	23.06.2017	P8_TA(2017)0428 Plan działania w sprawie detalicznych usług finansowych Rezolucja Parlamentu Europejskiego z dnia 14 listopada 2017 r. w sprawie planu działania w sprawie detalicznych usług finansowych (2017/2066(INI)) (2018/C 356/03)
	Zielona księga w sprawie detalicznych usług finansowych	link	22.11.2016	P8_TA(2016)0434 Zielona księga w sprawie detalicznych usług finansowych Rezolucja Parlamentu Europejskiego z dnia 22 listopada 2016 r. w sprawie zielonej księgi w sprawie detalicznych usług finansowych (2016/2056(INI)) (2018/C 224/02)
(UE) 2018/389	Rozporządzenie Delegowane Komisji (UE) 2018/389	link	25.11.2015	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)
(UE) 2017/2055	Rozporządzenie Delegowane Komisji (UE) 2017/2055	link	23.07.2014	(Akty o charakterze nieustawodawczym) ROZPORZĄDZENIA ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2017/2055 z dnia 23 czerwca 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących współpracy i wymiany informacji między właściwymi organami w związku z korzystaniem ze swobody przedsiębiorczości i swobody świadczenia usług przez instytucje płatnicze (Tekst mający znaczenie dla EOG)
(UE) 2015/751	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751		29.04.2015	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę (Dz.U. L 123 z 19.5.2015, s. 1–15)

Przepisy – kraje

Kraj	Termin transpozycji	Rozporządzenie
Belgia	13.01.2018	FEDERALE OVERHEIDSDIENST FINANCIEN 11 MAART 2018. – Wet betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen Oficjalna publikacja: Belgisch Staatsblad; Data publikacji: 2018-03-26; Strona: 29444-29514
Belgia	13.01.2018	Wet houdende wijziging en invoering van bepalingen inzake betalingsdiensten in verschillende boeken van het Wetboek van economisch recht. Oficjalna publikacja: Belgisch Staatsblad; Data publikacji: 2018-07-30; Strona: 59823-59849
Bułgaria	13.01.2018	Закон за платежните услуги и платежните системи Oficjalna publikacja: Държавен вестник; Numer: 20; Data publikacji: 2018-03-06; Strona: 00003-00069
Bułgaria	13.01.2018	НАРЕДБА № 16 на БНБ за издаване на лицензи и одобрения, за вписване в регистъра по чл. 19 от Закона за платежните услуги и платежните системи и за изискванията към дейността на операторите на платежни системи с окончателност на сетълмента Oficjalna publikacja: Държавен вестник; Numer: 32; Data publikacji: 2018-04-13; Strona: 00080-00113
Bułgaria	13.01.2018	Наредба № 3 от 18 април 2018 г. за условията и реда за откриване на платежни сметки, за изпълнение на платежни операции и за използване на платежни инструменти Oficjalna publikacja: Държавен вестник; Numer: 37; Data publikacji: 2018-05-04; Strona: 00071-00088
Czechy	13.01.2018	Zákon č. 99/1963 Sb., občanský soudní řád Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 1963-12-04
Czechy	13.01.2018	Zákon č. 563/1991 Sb., o účetnictví Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 1991-12-31
Czechy	13.01.2018	Zákon č. 21/1992 Sb., o bankách Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 1992-01-20
Czechy	13.01.2018	Zákon České národní rady č. 6/1993 Sb., o České národní bance Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 1992-12-31
Czechy	13.01.2018	Zákon č.143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže) Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2001-04-27

Czechy	13.01.2018	Zákon č. 150/2002 Sb., soudní řád správní Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2002-04-17
Czechy	13.01.2018	Zákon č. 229/2002 Sb., o finančním arbitrovi Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2002-06-04
Czechy	13.01.2018	Vyhláška č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2002-12-05
Czechy	13.01.2018	Vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2002-12-05
Czechy	13.01.2018	Vyhláška č. 473/2003 Sb., kterou se mění vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2003-12-31
Czechy	13.01.2018	Zákon č. 340/2004 Sb., kterým se mění zákon č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), a některé další zákony Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2004-06-02
Czechy	13.01.2018	Zákon č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2004-07-26
Czechy	13.01.2018	Zákon č. 500/2004 Sb., správní řád Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2004-09-24
Czechy	13.01.2018	Zákon č. 57/2006 Sb., o změně zákonů v souvislosti se sjednocením dohledu nad finančním trhem Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2006-03-08
Czechy	13.01.2018	Vyhláška č. 349/2007 Sb., kterou se mění vyhláška č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2007-12-21
Czechy	13.01.2018	Vyhláška č. 350/2007 Sb., kterou se mění vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2007-12-21
Czechy	13.01.2018	Zákon č. 93/2009 Sb., o auditorech a o změně některých zákonů (zákon o auditorech) Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2009-04-14
Czechy	13.01.2018	Zákon č. 155/2009 Sb., kterým se mění zákon č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2009-06-04

Czechy	13.01.2018	Zákon č. 285/2009 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o platebním styku Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2009-09-04
Czechy	13.01.2018	Vyhláška č. 419/2010 Sb., kterou se mění vyhláška č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2010-12-29
Czechy	13.01.2018	Vyhláška č. 420/2010 Sb., kterou se mění vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2010-12-29
Czechy	13.01.2018	Vyhláška č. 413/2011 Sb., kterou se mění vyhláška č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2011-12-22
Czechy	13.01.2018	Zákon č. 360/2012 Sb., kterým se mění zákon č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů, a zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2012-10-29
Czechy	13.01.2018	Vyhláška č. 408/2012 Sb., kterou se mění vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2012-11-30
Czechy	13.01.2018	Zákon č. 227/2013 Sb., kterým se mění zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů, a další související zákony Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2013-08-02
Czechy	13.01.2018	Vyhláška č. 467/2013 Sb., kterou se mění vyhláška č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2013-12-31
Czechy	13.01.2018	Vyhláška č. 468/2013 Sb., kterou se mění vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2013-12-31
Czechy	13.01.2018	Zákon č. 135/2014 Sb., kterým se mění některé zákony v souvislosti se stanovením přístupu k činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry a dohledu nad nimi Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2014-07-22
Czechy	13.01.2018	Vyhláška č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2014-08-07

Czechy	13.01.2018	Zákon č. 334/2014 Sb., kterým se mění zákon č. 93/2009 Sb., o auditorech a o změně některých zákonů (zákon o auditorech), ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2014-12-29
Czechy	13.01.2018	Zákon č. 334/2014 Sb., kterým se mění zákon č. 93/2009 Sb., o auditorech a o změně některých zákonů (zákon o auditorech), ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2014-12-29
Czechy	13.01.2018	Vyhláška č. 250/2015 Sb., kterou se mění vyhláška č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2015-10-02
Czechy	13.01.2018	Vyhláška č. 251/2015 Sb., kterou se mění vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2015-10-02
Czechy	13.01.2018	Zákon č. 375/2015 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o ozdravných postupech a řešení krize na finančním trhu a v souvislosti s úpravou systému pojištění vkladů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2015-12-28
Czechy	13.01.2018	Zákon č. 378/2015 Sb., kterým se mění zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů, a některé další zákony Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2015-12-28
Czechy	13.01.2018	Zákon č. 257/2016 Sb., o spotřebitelském úvěru Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2016-08-05
Czechy	13.01.2018	Zákon č. 293/2016 Sb., kterým se mění zákon č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů, a zákon č. 135/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zadávání veřejných zakázek Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2016-09-19
Czechy	13.01.2018	Zákon č. 299/2016 Sb., kterým se mění zákon č. 93/2009 Sb., o auditorech a o změně některých zákonů (zákon o auditorech), ve znění pozdějších předpisů, a další související zákony Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2016-09-21
Czechy	13.01.2018	Zákon č. 452/2016 Sb., kterým se mění zákon č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů, a další související zákony Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2016-12-29
Czechy	13.01.2018	Zákon č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2017-06-28
Czechy	13.01.2018	Zákon č. 370/2017 Sb., o platebním styku Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2017-11-13
Czechy	13.01.2018	Vyhláška č. 442/2017 Sb., kterou se mění vyhláška č. 501/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi, ve znění pozdějších předpisů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2017-12-15

Czechy	13.01.2018	Vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2018-01-11
Czechy	13.01.2018	Zákon č. 94/2018 Sb., kterým se mění zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů, a další související zákony Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2018-06-05
Czechy	13.01.2018	Zákon č. 111/2018 Sb., kterým se mění zákon č. 159/1999 Sb., o některých podmínkách podnikání a o výkonu některých činností v oblasti cestovního ruchu, ve znění pozdějších předpisů, a další související zákony Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2018-06-15
Czechy	13.01.2018	Zákon č. 171/2018 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o distribuci pojištění a zajištění Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2018-08-16
Czechy	13.01.2018	Zákon č. 5/2019 Sb., kterým se mění zákon č. 277/2013 Sb., o směnárenské činnosti, ve znění zákona č. 183/2017 Sb., a zákon č. 370/2017 Sb., o platebním styku Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2019-01-10
Czechy	13.01.2018	Zákon č. 110/2019 Sb., o zpracování osobních údajů Oficjalna publikacja: Sbirka Zakonu CR; Data publikacji: 2019-04-24
Czechy	13.01.2018	Explanatory document Data publikacji: 1001-01-01
Dania	13.01.2018	Forvaltningsloven – Lovbekendtgørelse nr. 433 af 22. april 2014 Oficjalna publikacja: Lovtidende A ; Numer: 433; Data publikacji: 2014-05-03
Dania	13.01.2018	Forslag til lov om betalinger Oficjalna publikacja: Lovtidende A ; Numer: 157; Data publikacji: 2017-03-15
Dania	13.01.2018	Lov om betalinger Oficjalna publikacja: Lovtidende A ; Numer: 652; Data publikacji: 2017-06-08
Dania	13.01.2018	Finanstilsynets forretningsgang for efterlevelse af myndighedsrettede bestemmelser i direktiver Oficjalna publikacja: Obsolete; Numer: N/A ; Data publikacji: 1001-01-01
Niemcy	13.01.2018	Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie Oficjalna publikacja: Bundesgesetzblatt Teil 1 (BGB 1); Numer: 48; Data publikacji: 2017-07-21; Strona: 02446-02494
Estonia	13.01.2018	Haldusmenetluse seadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 25.10.2016, 5; Data publikacji: 2016-10-26
Estonia	13.01.2018	Tarbijakaitseseadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 21.06.2017, 7; Data publikacji: 2017-07-04
Estonia	13.01.2018	Elektroonilise side seadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 01.07.2017, 2; Data publikacji: 2017-09-01
Estonia	13.01.2018	Makseasutuste ja e-raha asutuste seadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 17.11.2017, 34; Data publikacji: 2017-11-27
Estonia	13.01.2018	Võlaõigusseadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 17.11.2017, 40; Data publikacji: 2017-11-27

Estonia	13.01.2018	Äriseadustik Oficjalna publikacja: Riigi Teataja; Numer: RT I, 17.11.2017, 21; Data publikacji: 2017-11-27
Estonia	13.01.2018	Krediidiasutuste seadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 17.11.2017, 30; Data publikacji: 2017-11-27
Estonia	13.01.2018	Makseasutuste ja e-raha asutuste seadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 07.12.2017, 2; Data publikacji: 2018-01-13
Estonia	13.01.2018	Võlaõigusseadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 07.12.2017, 5; Data publikacji: 2018-01-13
Estonia	13.01.2018	Finantsinspektsiooni seadus Oficjalna publikacja: Riigi Teataja; Numer: RT I, 07.12.2017, 7; Data publikacji: 2018-01-13
Irlandia	13.01.2018	DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC Oficjalna publikacja: Iris Oifigiúl; Data publikacji: 2018-01-12
Irlandia	13.01.2018	European Union (payment Services) (Amendment) Regulations 2019 Oficjalna publikacja: Iris Oifigiúl; Numer: 2015/2366; Data publikacji: 2019-06-14; Strona: 00002-00002
Grecja	13.01.2018	Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2015/2366/ΕΕ για τις υπηρεσίες πληρωμών και άλλες διατάξεις. Oficjalna publikacja: Εφημερίς της Κυβερνήσεως (ΦΕΚ) (Τεύχος Α); Numer: 84; Data publikacji: 2018-05-15; Strona: 07905-07960
Grecja	13.01.2018	Υιοθέτηση των κατευθυντηρίων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών για την αναφορά μειζόνων συμβάντων δυνάμει της Οδηγίας 2015/2366/ΕΕ. Oficjalna publikacja: Εφημερίς της Κυβερνήσεως (ΦΕΚ) (Τεύχος Β); Numer: 1597; Data publikacji: 2019-05-10; Strona: 18731-18746
Hiszpania	13.01.2018	Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera Oficjalna publikacja: Boletín Oficial del Estado (B.O.E); Numer: 284/2018; Data publikacji: 2018-11-24; Strona: 14474-14568
Francja	13.01.2018	LOI n° 2008-776 du 4 août 2008 de modernisation de l'économie Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2008-08-05
Francja	13.01.2018	Ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2009-07-16
Francja	13.01.2018	Décret n° 2009-934 du 29 juillet 2009 pris pour l'application de l'ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de services de paiement et portant création des établissements de paiement Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2009-07-31
Francja	13.01.2018	LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2016-10-08

Francja	13.01.2018	LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2016-12-10
Francja	13.01.2018	Ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-08-10
Francja	13.01.2018	Décret n° 2017-1313 du 31 août 2017 portant transposition de la directive n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-09-02
Francja	13.01.2018	Décret n° 2017-1314 du 31 août 2017 portant transposition de la directive n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-09-02
Francja	13.01.2018	Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009 relatif aux relations entre les prestataires de services de paiement et leurs clients en matière d'obligations d'information des utilisateurs de services de paiement et précisant les principales stipulations devant figurer dans les conventions de compte de dépôt et les contrats-cadres de services de paiement Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-09-02
Francja	13.01.2018	Arrêté du 31 août 2017 modifiant l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-09-02
Francja	13.01.2018	Arrêté du 31 août 2017 modifiant l'arrêté du 20 mai 2015 portant réglementation prudentielle et comptable en matière bancaire et financière en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-09-02
Francja	13.01.2018	Arrêté du 31 août 2017 modifiant l'arrêté du 2 mai 2013 portant sur la réglementation prudentielle des établissements de monnaie électronique Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-09-02
Francja	13.01.2018	Arrêté du 31 août 2017 modifiant l'arrêté du 29 octobre 2009 portant sur la réglementation prudentielle des établissements de paiement Oficjalna publikacja: Journal Officiel de la République Française (JORF); Data publikacji: 2017-09-02
Chorwacja	13.01.2018	Zakon o elektroničkom novcu Oficjalna publikacja: Narodne Novine; Numer: 64/18; Data publikacji: 1001-01-01
Chorwacja	13.01.2018	Zakon o platnom prometu Oficjalna publikacja: Narodne Novine; Numer: 66/18; Data publikacji: 1001-01-01

Chorwacja	13.01.2018	Odluka o zaštiti novčanih sredstava korisnika platnih usluga Oficjalna publikacja: Narodne Novine; Numer: 73/2018; Data publikacji: 1001-01-01
Chorwacja	13.01.2018	Odluka o regulatornom kapitalu institucija za platni promet Oficjalna publikacja: Narodne Novine; Numer: 73/2018; Data publikacji: 1001-01-01
Chorwacja	13.01.2018	Odluka o regulatornom kapitalu institucija za elektronički novac Oficjalna publikacja: Narodne Novine; Numer: 73/2018; Data publikacji: 1001-01-01
Włochy	13.01.2018	Recepimento della direttiva 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento UE n.1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento UE n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. Oficjalna publikacja: Gazzetta Ufficiale della Repubblica Italiana; Numer: 10; Data publikacji: 2018-01-13
Cypr	13.01.2018	Ο περί της Παροχής και Χρήσης Υπηρεσιών Πληρωμών και Πρόσβασης στα Συστήματα Πληρωμών Νόμος του 2018. Oficjalna publikacja: Cyprus Gazette; Numer: 4649; Data publikacji: 2018-04-18; Strona: 00176-00243
Cypr	13.01.2018	Ο Περί Ηλεκτρικού Χρήματος (Τροποποιητικός) Νόμος του 2018. Oficjalna publikacja: Cyprus Gazette; Numer: 4649; Data publikacji: 2018-04-18; Strona: 00173-00175
Cypr	13.01.2018	Ο περί της εξ Αποστάσεως Εμπορίας Χρηματοοικονομικών Υπηρεσιών προς τους Καταναλωτές(Τροποποιητικός) Νόμος του 2018. Oficjalna publikacja: Cyprus Gazette; Numer: 4649; Data publikacji: 2018-04-18; Strona: 00172-00172
Cypr	13.01.2018	Ο Περί Εργασιών Πιστωτικών Ιδρυμάτων (Τροποποιητικός) Νόμος του 2018. Oficjalna publikacja: Cyprus Gazette; Numer: 4649; Data publikacji: 2018-04-18; Strona: 00171-00171
Cypr	13.01.2018	Ο περί της Παροχής και Χρήσης Υπηρεσιών Πληρωμών και Πρόσβασης στα Συστήματα Πληρωμών (Τροποποιητικός) Νόμος του 2019. Oficjalna publikacja: Cyprus Gazette; Numer: 4690; Data publikacji: 2019-03-15; Strona: 00083-00084
Łotwa	13.01.2018	Grozījumi Maksājumu pakalpojumu un elektroniskās naudas likumā Oficjalna publikacja: Latvijas Vēstnesis; Numer: 132 (6218); Data publikacji: 2018-07-04
Litwa	13.01.2018	Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas Nr. VIII-1864. Lietuvos Respublikos civilinis kodeksas. (Suvestinė redakcija nuo 2018-07-01 iki 2018-12-31) Oficjalna publikacja: Valstybės žinios; Numer: 74-2262; Data publikacji: 2000-09-06
Litwa	13.01.2018	Lietuvos Respublikos bankų įstatymas Nr. IX-2085 Oficjalna publikacja: Valstybės žinios; Numer: 54-1832; Data publikacji: 2004-04-15
Litwa	13.01.2018	Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135 Oficjalna publikacja: Valstybės žinios; Numer: 69-2382; Data publikacji: 2004-04-30
Litwa	13.01.2018	Lietuvos Respublikos bankų įstatymo 2, 14, 20, 46, 53, 55, 65, 69, 72, 90, 91, 92 straipsnių ir priedo pakeitimo įstatymas Nr. X-273 Oficjalna publikacja: Valstybės žinios; Numer: 84-3110; Data publikacji: 2005-07-12

Litwa	13.01.2018	Lietuvos Respublikos bankų įstatymo 2, 5, 8, 17, 23, 24, 25, 26, 34, 66 straipsnių bei priedo pakeitimo ir papildymo įstatymas Nr. XI-201 Oficjalna publikacja: Valstybės žinios; Numer: 38-1440; Data publikacji: 2009-04-04
Litwa	13.01.2018	Lietuvos Respublikos finansų įstaigų įstatymo 1, 2, 3 straipsnių pakeitimo ir priedo papildymo įstatymas Nr. XI-554 Oficjalna publikacja: Valstybės žinios; Numer: 153-6892; Data publikacji: 2009-12-28
Litwa	13.01.2018	Lietuvos Respublikos bankų įstatymo Nr. IX-2085 2, 3, 4, 5, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 23, 24, 34, 35, 36, 40, 44, 48, 52, 53, 57, 59, 61, 64, 65, 67, 69, 70, 70-1, 71, 72, 73, 74, 75, 76, 78, 81, 82, 86 straipsnių ir priedo pakeitimo, įstatymo papildymo 65-1, 68-1 ir 70-2 straipsniais ir 6, 7, 8, 18, 26, 37, 38, 39, 43, 49, 50 straipsnių pripažinimo netekusiais galios įstatymas Nr. XII-1545 Oficjalna publikacja: Teisės aktų registras; Numer: 2015-04828; Data publikacji: 2015-03-31
Litwa	13.01.2018	Lietuvos Respublikos bankų įstatymo Nr. IX-2085 2, 10, 61, 62, 67, 71, 72, 73, 75, 76, 77, 83, 84, 85, 87 straipsnių, priedo pakeitimo, Įstatymo papildymo 36-1, 75-1, 75-2 straipsniais, 76-1 straipsnio ir tryliktojo skirsnio pripažinimo netekusiais galios įstatymas Nr. XII-2055 Oficjalna publikacja: Teisės aktų registras; Numer: 2015-19165; Data publikacji: 2015-12-02
Litwa	13.01.2018	Lietuvos Respublikos bankų įstatymo Nr. IX-2085 24 straipsnio pakeitimo įstatymas Nr. XII-2077 Oficjalna publikacja: Teisės aktų registras; Numer: 2015-19285; Data publikacji: 2015-12-03
Litwa	13.01.2018	Lietuvos Respublikos vartotojų teisių apsaugos įstatymo Nr. I-657 2, 5, 10, 11, 12, 40 straipsnių, šeštojo skirsnio ir Įstatymo priedo pakeitimo įstatymas Nr. XII-2083 Oficjalna publikacja: Teisės aktų registras; Numer: 2015-19362; Data publikacji: 2015-12-07
Litwa	13.01.2018	Lietuvos banko valdybos 2016 m. sausio 28 d. nutarimas Nr. 03-11 „Dėl Lietuvos banko valdybos 2012 m. sausio 26 d. nutarimo Nr. 03-23 „Dėl Vartotojų ir finansų rinkos dalyvių ginčų nagrinėjimo tvarkos aprašo patvirtinimo“ pakeitimo Oficjalna publikacja: Teisės aktų registras; Numer: 2016-01773; Data publikacji: 2016-01-29
Litwa	13.01.2018	Lietuvos Respublikos Lietuvos banko įstatymo Nr. I-678 47 straipsnio pakeitimo įstatymas Nr. XII-2562 Oficjalna publikacja: Teisės aktų registras; Numer: 2016-20316; Data publikacji: 2016-07-13
Litwa	13.01.2018	Lietuvos Respublikos mokėjimų įstatymo Nr. VIII-1370 pakeitimo įstatymas Nr. XIII-1092 Oficjalna publikacja: Teisės aktų registras; Numer: 2018-06727; Data publikacji: 2018-04-27
Litwa	13.01.2018	Lietuvos Respublikos mokėjimo įstaigų įstatymo Nr. XI-549 pakeitimo įstatymas Nr. XIII-1093 Oficjalna publikacja: Teisės aktų registras; Numer: 2018-06729; Data publikacji: 2018-04-27
Litwa	13.01.2018	Lietuvos Respublikos finansų įstaigų įstatymo Nr. IX-1068 2, 18, 44 straipsnių ir priedo pakeitimo įstatymas Nr. XIII-1097 Oficjalna publikacja: Teisės aktų registras; Numer: 2018-06736; Data publikacji: 2018-04-27
Litwa	13.01.2018	Lietuvos Respublikos vartotojų teisių apsaugos įstatymo Nr. I-657 1 straipsnio ir priedo pakeitimo įstatymas Nr. XIII-1096 Oficjalna publikacja: Teisės aktų registras; Numer: 2018-06735; Data publikacji: 2018-04-27
Litwa	13.01.2018	Lietuvos Respublikos elektroninių pinigų ir elektroninių pinigų įstaigų įstatymo Nr. XI-1868 pakeitimo įstatymas Nr. XIII-1094 Oficjalna publikacja: Teisės aktų registras; Numer: 2018-06730; Data publikacji: 2018-04-27

Litwa	13.01.2018	Lietuvos Respublikos Lietuvos banko įstatymo Nr. I-678 47 straipsnio ir 1 priedo pakeitimo įstatymas Nr. XIII-1095 Oficjalna publikacja: Teisės aktų registras; Numer: 2018-06731; Data publikacji: 2018-04-27
Litwa	13.01.2018	Lietuvos banko valdybos 2018 m. gegužės 24 d. nutarimas Nr. 03-83 „Dėl Elektroninių pinigų įstaigų ir mokėjimo įstaigų pradinio kapitalo ir nuosavo kapitalo skaičiavimo taisyklių ir elektroninių pinigų įstaigų (mokėjimo įstaigų) pradinio kapitalo ir nuosavo kapitalo skaičiavimo ataskaitos formų patvirtinimo“ Oficjalna publikacja: Teisės aktų registras; Numer: 2018-08416; Data publikacji: 2018-05-25
Litwa	13.01.2018	Lietuvos banko valdybos 2018 m. birželio 12 d. nutarimas Nr. 03-100 „Dėl Lietuvos banko valdybos 2009 m. gruodžio 24 d. nutarimo Nr. 238 „Dėl Lietuvos banko išduodamų leidimų elektroninių pinigų ir mokėjimo įstaigoms“ pakeitimo“ Oficjalna publikacja: Teisės aktų registras; Numer: 2018-09879; Data publikacji: 2018-06-14
Litwa	13.01.2018	Lietuvos banko valdybos 2018 m. birželio 12 d. nutarimas Nr. 03-101 „Dėl Lietuvos banko valdybos 2012 m. vasario 23 d. nutarimo Nr. 03-43 „Dėl Užsienio valstybių elektroninių pinigų įstaigų filialų, įsteigtų Lietuvos Respublikoje, licencijavimo taisyklių“ pakeitimo“ Oficjalna publikacja: Teisės aktų registras; Numer: 2018-09880; Data publikacji: 2018-06-14
Luksemburg	13.01.2018	Loi du 20 juillet 2018 portant : 1° transposition de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/ CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/ CE; et 2° modification de la loi modifiée du 10 novembre 2009 relative aux services de paiement. Oficjalna publikacja: Journal officiel du Grand-Duché de Luxembourg – Mémorial A; Numer: 612; Data publikacji: 1001-01-01; Strona: 00001-00040
Węgry	13.01.2018	1997. évi CXXXII. törvény a külföldi székhelyű vállalkozások magyarországi fióktelepeiről és kereskedelmi képviseleteiről Oficjalna publikacja: Magyar Közlöny; Numer: 110; Data publikacji: 1997-12-10; Strona: 08130-08138
Węgry	13.01.2018	2000. évi C. törvény a számvitelről Oficjalna publikacja: Magyar Közlöny; Numer: 2000/95; Data publikacji: 2000-11-21; Strona: 05790-05868
Węgry	13.01.2018	A Kormány 250/2000. (XII. 24.) Korm. rendelete a hitelintézetek és a pénzügyi vállalkozások éves beszámoló készítési és könyvvezetési kötelezettségének sajátosságairól Oficjalna publikacja: Magyar Közlöny; Numer: 130; Data publikacji: 2000-12-24; Strona: 8893-8928
Węgry	13.01.2018	2003. évi C. törvény az elektronikus hírközlésről Oficjalna publikacja: Magyar Közlöny; Numer: 2003/136; Data publikacji: 2003-11-27; Strona: 10420-10483
Węgry	13.01.2018	2005. évi XXV. törvény a távértékesítés keretében kötött pénzügyi ágazati szolgáltatási szerzõdésekrõl Oficjalna publikacja: Magyar Közlöny; Numer: 2005/60.; Data publikacji: 1001-01-01; Strona: 03045-03049
Węgry	13.01.2018	2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 24955-24986
Węgry	13.01.2018	A Kormány 327/2009. (XII. 29.) Korm. rendelete az egyes pénz– és tőkepiaci szolgáltatásokat is végző egyéb vállalkozások éves beszámoló készítési és könyvvezetési kötelezettségének sajátosságairól Oficjalna publikacja: Magyar Közlöny; Numer: 47238-47246; Data publikacji: 1001-01-01

Węgry	13.01.2018	2009. évi CLXII. törvény a fogyasztónak nyújtott hitelről Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 49503-49522
Węgry	13.01.2018	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 25449-25485
Węgry	13.01.2018	2013. évi V. törvény a Polgári Törvénykönyvről Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 02382-02663
Węgry	13.01.2018	2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 85961-86081
Węgry	13.01.2018	2013. évi CXXXIX. törvény a Magyar Nemzeti Bankról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 67824-67885
Węgry	13.01.2018	2013. évi CCXXXV. törvény az egyes fizetési szolgáltatókról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 85852-85887
Węgry	13.01.2018	2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 07692-07730
Węgry	13.01.2018	2016. évi CL. törvény az általános közigazgatási rendtartásról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 81898-81930
Węgry	13.01.2018	2017. évi CXLV. törvény egyes törvények biztosítási, illetve pénzforgalmi tárgyú jogharmonizációjával kapcsolatos módosításáról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 29889-29965
Węgry	13.01.2018	2014. évi LXXVII. törvény az egyes fogyasztói kölcsönszerződések devizanemének módosulásával és a kamatszabályokkal kapcsolatos kérdések rendezéséről Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 18192-18200
Węgry	13.01.2018	A Kormány 435/2016. (XII. 16.) Korm. rendelete a befektetési vállalkozások, a pénzforgalmi intézmények, az elektronikuspénz-kibocsátó intézmények, az utalványkibocsátók, a pénzügyi intézmények és a független pénzügyi szolgáltatás közvetítők panaszkezelésének eljárásával, valamint panaszkezelési szabályzatával kapcsolatos részletes szabályokról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 82379-82380
Węgry	13.01.2018	A pénzforgalom lebonyolításáról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 33806-33846
Węgry	13.01.2018	A Kormány 131/2018. (VII. 23.) Korm. rendelete egyes pénzforgalmi és számviteli tárgyú kormányrendeletek módosításáról Oficjalna publikacja: Magyar Közlöny; Data publikacji: 1001-01-01; Strona: 27139-27140
Malta	13.01.2018	CENTRAL BANK OF MALTA DIRECTIVE NO 1 in terms of the CENTRAL BANK OF MALTA ACT (Cap. 204 of the Laws of Malta), THE PROVISION AND USE OF PAYMENT SERVICES Oficjalna publikacja: The Malta government gazette; Data publikacji: 2018-01-09
Malta	13.01.2018	Various Financial Services Laws (Amendment) Act, 2019. Oficjalna publikacja: The Malta government gazette; Numer: 20,243; Data publikacji: 2019-08-02
Holandia	13.01.2018	Wet ter implementatie van de herziene richtlijn betalingsdiensten Oficjalna publikacja: Staatsblad (Bulletin des Lois et des Décrets royaux); Numer: 503; Data publikacji: 2018-12-27; Strona: 00001-00027

Holandia	13.01.2018	Implementatieregeling herziene richtlijn betaaldiensten Oficjalna publikacja: Staatscourant (Journal Officiel néerlandais); Numer: 7963; Data publikacji: 2019-02-15; Strona: 00001-00005
Holandia	13.01.2018	Besluit van 8 februari 2019 tot vaststelling van het tijdstip van inwerkingtreding van de Implementatiewet herziene richtlijn betaaldiensten en het Implementatiebesluit herziene richtlijn betaaldiensten Oficjalna publikacja: Staatsblad (Bulletin des Lois et des Décrets royaux); Numer: 60; Data publikacji: 2019-02-18; Strona: 00001-00003
Holandia	13.01.2018	Besluit ter implementatie van de herziene richtlijn betalingsdiensten Oficjalna publikacja: Staatsblad (Bulletin des Lois et des Décrets royaux); Numer: 59; Data publikacji: 2019-02-18; Strona: 00001-00039
Holandia	13.01.2018	Besluit van 5 maart 2019 tot wijziging van het Besluit van 8 februari 2019 tot vaststelling van het tijdstip van inwerkingtreding van de Implementatiewet herziene richtlijn betaaldiensten en het Implementatiebesluit herziene richtlijn betaaldiensten (Stb. 2019, 60) en tot vaststelling van het tijdstip van inwerkingtreding van artikel III, onderdeel J, van de Implementatiewet herziene richtlijn betaaldiensten Oficjalna publikacja: Staatsblad (Bulletin des Lois et des Décrets royaux); Numer: 2019 114; Data publikacji: 2019-03-15
Austria	13.01.2018	Zahlungsdienstegesetz 2018 Oficjalna publikacja: Bundesgesetzblatt für die Republik Österreich (BGBl.); Numer: BGBl I Nr. 17/2018; Data publikacji: 2018-04-24
Polska	13.01.2018	Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych Oficjalna publikacja: Dziennik Ustaw; Numer: 2017/2003 – t.j.; Data publikacji: 2017-10-27
Polska	13.01.2018	Ustawa z dnia 22 marca 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw Oficjalna publikacja: Dziennik Ustaw; Numer: 2018/864; Data publikacji: 2018-05-10
Polska	13.01.2018	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych Oficjalna publikacja: Dziennik Ustaw; Numer: 2018/1000; Data publikacji: 2018-05-24
Polska	13.01.2018	Ustawa z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw Oficjalna publikacja: Dziennik Ustaw; Data publikacji: 2018-06-05
Polska	13.01.2018	Rozporządzenie Ministra Finansów z dnia 6 czerwca 2018 r. w sprawie metody obliczania kwoty, o której mowa w art. 76 ust. 4 pkt 2 ustawy o usługach płatniczych Oficjalna publikacja: Dziennik Ustaw; Numer: 2018/1110; Data publikacji: 2018-06-08
Portugalia	13.01.2018	Decreto-Lei n.º 91/2018 de 12 de novembro – Aprova o novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, transpondo a Diretiva (UE) 2015/2366 Oficjalna publikacja: Diaro da Republica I ; Numer: 217/2018; Data publikacji: 2018-11-12; Strona: 05211-05260
Rumunia	13.01.2018	LEGE nr. 209 din 8 noiembrie 2019 privind serviciile de plată şi pentru modificarea unor acte normative Oficjalna publikacja: Monitorul Oficial al României; Numer: 913; Data publikacji: 2019-11-13; Strona: 00002-00037
Rumunia	13.01.2018	LEGE nr. 210 din 8 noiembrie 2019 privind activitatea de emitere de monedă electronică Oficjalna publikacja: Monitorul Oficial al României; Numer: 914; Data publikacji: 2019-11-13; Strona: 00002-00016

Słowenia	13.01.2018	Zakon o poštnih storitvah (ZPSto-2) Oficjalna publikacja: Uradni list RS; Numer: 51/2009; Data publikacji: 2009-07-03; Strona: 06929-06943
Słowenia	13.01.2018	Zakon o bančništvu Oficjalna publikacja: Uradni list RS; Numer: 25/2015; Data publikacji: 2015-04-13; Strona: 02833-02916
Słowenia	13.01.2018	Zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih Oficjalna publikacja: Uradni list RS; Numer: 7/2018; Data publikacji: 2018-02-07; Strona: 00979-01050
Słowenia	13.01.2018	Popravek predpisa 2018-01-0274 Oficjalna publikacja: Uradni list RS; Numer: 9/2018; Data publikacji: 2018-02-16; Strona: 01341-01341
Słowacja	13.01.2018	Zákon č. 460/1992 Zb. Ústava Slovenskej republiky Oficjalna publikacja: Zbierka zákonov SR; Numer: 92; Data publikacji: 1992-10-01; Strona: 2659-2678
Słowacja	13.01.2018	Zákon Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska Oficjalna publikacja: Zbierka zákonov SR; Numer: 113; Data publikacji: 1992-12-11; Strona: 3322-3329
Słowacja	13.01.2018	Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov Oficjalna publikacja: Zbierka zákonov SR; Numer: 193; Data publikacji: 2001-11-29; Strona: 5122-5164
Słowacja	13.01.2018	Zákon č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov Oficjalna publikacja: Zbierka zákonov SR; Numer: 304; Data publikacji: 2004-12-30
Słowacja	13.01.2018	Zákon č. 266/2005 Z. z. o ochrane spotrebiteľa pri finančných službách na diaľku a o zmene a doplnení niektorých zákonov Oficjalna publikacja: Zbierka zákonov SR; Numer: 116; Data publikacji: 2005-06-24
Słowacja	13.01.2018	Zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov Oficjalna publikacja: Zbierka zákonov SR; Numer: 172; Data publikacji: 2009-12-01
Słowacja	13.01.2018	Zákon č. 351/2011 Z. z. o elektronických komunikáciách Oficjalna publikacja: Zbierka zákonov SR; Numer: 111; Data publikacji: 2011-10-22
Słowacja	13.01.2018	Opatrenie Národnej banky Slovenska č. 14/2011 z 15. novembra 2011, ktorým sa ustanovujú niektoré podrobnosti povoľovania na výkon činnosti a podnikania platobných inštitúcií a inštitúcií elektronických peňazí Oficjalna publikacja: Vestník Národnej banky Slovenska; Numer: 25; Data publikacji: 2011-11-25
Słowacja	13.01.2018	Zákon č. 162/2015 Z. z. Správny súdny poriadok Oficjalna publikacja: Zbierka zákonov SR; Numer: 53; Data publikacji: 2015-07-17
Słowacja	13.01.2018	Zákon č. 160/2015 Z. z. Civilný sporový poriadok Oficjalna publikacja: Zbierka zákonov SR; Numer: 51; Data publikacji: 2015-07-17
Słowacja	13.01.2018	Zákon č. 391/2015 Z. z. o alternatívnom riešení spotrebiteľských sporov a o zmene a doplnení niektorých zákonov Oficjalna publikacja: Zbierka zákonov SR; Numer: 107; Data publikacji: 2015-12-18

Słowacja	13.01.2018	Zákon č. 281/2017 Z. z., ktorým sa mení a dopĺňa zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov Oficjalna publikacja: Zbierka zákonov SR; Data publikacji: 2017-11-22
Finlandia	13.01.2018	Laki maksulaitoslain muuttamisesta / Lag om ändring av lagen om betalningsinstitut (890/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 890/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	Laki ulkomaisen maksulaitoksen toiminnasta Suomessa annetun lain muuttamisesta / Lag om ändring av lagen om utländska betalningsinstituts verksamhet i Finland (891/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 891/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	Laki luottolaitostoiminnasta annetun lain 9 luvun 16 §:n muuttamisesta / Lag om ändring av 9 kap. 16 § i kreditinstitutslagen (892/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 892/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	Laki Finanssivalvonnasta annetun lain muuttamisesta / Lag om ändring av lagen om Finansinspektionen (893/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 893/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	1/13/18 Laki Finanssivalvonnan valvontamaksusta annetun lain 1 ja 6 §:n muuttamisesta / Lag om ändring av 1 och 6 § i lagen om Finansinspektionens tillsynsavgift (894/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 894/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	Laki maksupalvelulain muuttamisesta / Lag om ändring av betaltjänstlagen (898/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 898/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	Laki kuluttajansuojalain muuttamisesta / Lag om ändring av konsumentskyddslagen (899/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 899/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	Laki tietoyhteiskuntakaaren 125 ja 134 §:n muuttamisesta / Lag om ändring av 125 och 134 § i informationssamhällsbalken (900/2017) 14/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 900/2017; Data publikacji: 2017-12-19
Finlandia	13.01.2018	Valtiovarainministeriön asetus maksulaitoksen omien varojen laskemisessa käytettävistä menetelmistä / Finansministeriets förordning om metoder för beräkning av betalningsinstituts kapitalbas (1039/2017) 18/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 1039/2017; Data publikacji: 2017-12-28
Finlandia	13.01.2018	Valtiovarainministeriön asetus maksulaitoksen toimilupahakemukseen liitettävistä selvityksistä / Finansministeriets förordning om utredningar som ska fogas till ansökan om auktorisation för betalningsinstitut (1040/2017) 18/12/2017 Oficjalna publikacja: Suomen säädöskokoelma (SK); Numer: 1040/2017; Data publikacji: 2017-12-28

Szwecja	13.01.2018	Lag (2010:751) om betaltjänster Oficjalna publikacja: Svensk författningssamling (SFS); Numer: 2010:751; Data publikacji: 1001-01-01
Szwecja	13.01.2018	1/13/18 Lag (2011:755) om elektroniska pengar Oficjalna publikacja: Svensk författningssamling (SFS); Numer: 2011:755; Data publikacji: 1001-01-01
Szwecja	13.01.2018	Förordning (2010:1008) om betaltjänster Oficjalna publikacja: Svensk författningssamling (SFS); Numer: 2010:1008; Data publikacji: 1001-01-01
Szwecja	13.01.2018	Förordning (2011:776) om elektroniska pengar Oficjalna publikacja: Svensk författningssamling (SFS); Numer: 2011:776; Data publikacji: 1001-01-01
Szwecja	13.01.2018	Finansinspektionen föreskrifter och allmänna råd (FFFS 2010:3) om betalningsinstitut och registrerade betaltjänstleverantörer Oficjalna publikacja: Finansinspektionens författningssamling (FFFS); Numer: 2010:3; Data publikacji: 1001-01-01
Szwecja	13.01.2018	Finansinspektionens föreskrifter och allmänna råd (FFFS 2011:49) om institut för elektroniska pengar och registrerade utgivare Oficjalna publikacja: Finansinspektionens författningssamling (FFFS); Numer: 2011:49; Data publikacji: 1001-01-01
Szwecja	13.01.2018	Finansinspektionen föreskrifter (FFFS 2018:4) om verksamhet för betaltjänstleverantörer Oficjalna publikacja: Finansinspektionens författningssamling (FFFS); Numer: 2018:4; Data publikacji: 1001-01-01
Szwecja	13.01.2018	Föreskrifter (2018:6) om ändring i Finansinspektionens föreskrifter och allmänna råd (FFFS 2010:3) om betalningsinstitut och registrerade betaltjänstleverantörer Oficjalna publikacja: Finansinspektionens författningssamling (FFFS); Numer: 2018:6; Data publikacji: 1001-01-01
Wielka Brytania	13.01.2018	The Payment Services Regulations 2017 (S.I. 2017/752 Oficjalna publikacja: Her Majesty's Stationery Office (HMSO); Numer: 2017/752; Data publikacji: 1001-01-01
Wielka Brytania	13.01.2018	The Payment Services and Systems and Electronic Money (Miscellaneous Amendments) Regulations 2017 (S.I. 2017/1173) Oficjalna publikacja: Her Majesty's Stationery Office (HMSO); Numer: 2017 No. 1173; Data publikacji: 1001-01-01
Wielka Brytania	13.01.2018	The Financial Services (Payment Services) Regulations 2018. Oficjalna publikacja: Gibraltar Gazette; Numer: 4427; Data publikacji: 2018-01-11

Elementy dyskusyjne

Problem	Testowanie
Opis	Niezawodność platform testowych, głębokośc przypadków użycia i dostępności danych, łatwość i szybkość testowania dla TPP, włączając w to informacje o koncie i płatności dostawcy usług inicjujących (AISP i PISP), a także emitenci instrumentów płatniczych opartych na karcie (CBPII) Automatyczne testy TPP, katalog przypadków możliwie jak najbardziej wyczeprujący, możliwość odczytu maszynowego specyfikacji API, ASPSP zapewnia odpowiednie wstarcie dla TPP
Propozycja	W art. 30 ust. 5 rozporządzenia Komisji (UE) 2018/389 (RTS w sprawie SCA i CSC) stwierdza się, że „dostawcy usług płatniczych prowadzący rachunek udostępniają instrument testowy, w tym wsparcie, w zakresie testowania połączeń i testów funkcjonalnych". Oznacza to, że dostawcy usług płatniczych prowadzący rachunek (ASPSP) są zobowiązani do zapewniania wsparcia, a także do dostarczania go zewnętrznym dostawcom (TPP) – dostawcom usług informacji o rachunku, dostawcom usług inicjowania płatności oraz wydawcom instrumentów płatniczych opartych na karcie (AISP, PISP i CBPII) – które są autoryzowane lub składają wniosek o autoryzację. Artykuł 30 ust. 3 RTS stanowi również, że ASPSP udostępniają dokumentację zawierającą specyfikację techniczną dowolnego dedykowanego interfejsu, „określając zestaw procedur, protokołów i narzędzi potrzebnych [PISP, AISP i CBPII] do umożliwienia ich oprogramowanie i aplikacje do współpracy z systemami [ASPSP] ". ASPSP nie są wymagane, ale może okazać się wydajne i leży w ich interesie, aby umożliwić TPP korzystanie z automatycznych programów testowych tam, gdzie to możliwe i udostępnianie dokumentacji w formacie do odczytu maszynowego. Prawdopodobnie zminimalizuje to wsparcie, które w przeciwnym razie ASPSP mogą być wymagane do zapewnienia każdemu TPP za pomocą narzędzia do testowania. Włączenie pewnego stopnia automatyzacji może również zwiększyć wskaźnik uczestnictwa TPP, ułatwić lepsze wyniki testowania i pomóc ASPSP osiągnąć „szerokie wykorzystanie" ich interfejsu produkcyjnego, co z kolei może być korzystne dla celów procesu wyłączenia, zgodnie z wytycznymi EBA w sprawie warunków korzystania ze zwolnienia z mechanizmu awaryjnego (EBA / GL / 2018/07). W szczególności w wytycznej 6.5 wymieniono elementy, które ASPSP powinni zezwalać autoryzowanym TPP (lub dostawcom usług płatniczych, którzy złożyli wnioski do swoich właściwych organów o odpowiednie zezwolenie) na przetestowanie. Wytyczna 6.6 z kolei wymaga, aby ASPSP przedstawili podsumowanie wyników badań właściwemu organowi (CA), w tym liczbę TPP, którzy korzystali z narzędzia do testowania, oraz informacje zwrotne ASPSP otrzymane od tych TPP.

Problem	Dostosowanie funkcjonalności i wymagań dotyczących danych między inicjatywami API (i bardziej ogólnie API)
Opis	Obawy, że dane i funkcje dostępne za pośrednictwem inicjatyw API nie zawsze są dostosowane do różnych inicjatyw API. Sugestia aby EBA zaprojektował ankietę, która zostanie wysłana do inicjatyw API w celu zidentyfikowania danych i funkcjonalności dostępnych w ramach każdej inicjatywy API.
Propozycja	Artykuł 30 ust. 3 RTS w sprawie SCA i CSC stanowi, że ASPSP udostępniają dokumentację zawierającą specyfikację techniczną dowolnego dedykowanego interfejsu „nie mniej niż 6 miesięcy przed datą zastosowania [RTS] lub przed datą docelową wprowadzenie na rynek interfejsu dostępu, gdy uruchomienie nastąpi po dniu [aplikacji] [RTS]. ”Oznacza to, że ASPSP są zobowiązani do udostępnienia dokumentacji nie później niż 14 marca 2019 r. To z kolei ułatwi przejrzystość na rynku w zakresie funkcjonalności oferowanych przez API, które powinny być pomocne dla TPP. Jak stwierdzono w punkcie I powyżej, ASPSP mogą uznać za wydajne i we własnym interesie udostępnienie dokumentacji w formacie do odczytu maszynowego, aby zminimalizować potrzebę zapewnienia wsparcia potrzebnego dla każdego TPP korzystającego z narzędzia do testowania oraz w celu proces zwolnienia. Inicjatywy API mogą również rozważyć zbadanie ASPSP wdrażających ich specyfikacje, oprogramowanie i / lub narzędzia implementacyjne oraz porównać i opublikować funkcje obsługiwane przez te ASPSP. Powinno to dodatkowo zwiększyć przejrzystość dla wszystkich uczestników rynku, w szczególności TPP, w odniesieniu do funkcjonalności dostępnych za pośrednictwem każdego API oraz wszelkich rozbieżności między ASPSP używającymi tego API.

Problem	**Lista kwalifikowanych dostawców usług zaufania (QTSP) wydających certyfikaty PSD2 eIDAS**
Opis	Obawa uczestników branżowych o to, że dostawcy usług płatniczych nie są w stanie zidentyfikować którzy QTSP wystawiają certyfikaty PSD2 eIDAS na liście QTSP opublikowanej przez Komisję Europejską na ich stronie internetowej. Obawy o to, że najwyraźniej nie ma QTSP, które oferowałyby certyfikaty PSD2 eIDAS i że lista stron internetowych Komisji Europejskiej nie jest w formacie do odczytu maszynowego. Sugestia wprowadzenia odpowiedniej zmiany treści i funkcjonalności strony internetowej Komisji Europejskiej
Propozycja	EBA tłumaczy, że istnieje lista QTSP (pod adresem: https://webgate.ec.europa.eu/tl-browser) oraz że zasady otrzymanie akredytacji są określone i odpowiednio opisane. Rozumie również, że lista nie określa, czy dany QTSP dostarcza certyfikaty PSD2 eIDAs, czy nie, ponieważ odpowiednie krajowe organy nadzorcze nie dostarczają takich informacji. W związku z tym EBA postanowiła zapytać QTSP wymienionych na powyższej stronie internetowej o to czy wydają lub zamierzają wydawać certyfikaty eIDAS do celów PSD2, w tym certyfikaty testowe. Udostęonili listę takich QTSP, którzy spełniają zapytanie oraz zawierają dodatkowe informacje, w tym dane kontaktowe oraz dostępny na wyżej wymienionej stronie internetowej Komisji Europejskiej: – Aruba Posta Elettronica Certificata S.p.A. (Włochy) – Buypass AS (Norwegia) – Evrotrust Technologies JSC (Bułgaria) – Pierwszy organ certyfikujący, a.s. (Republika Czeska) – InfoCert S.p.A. (Włochy) – Krajowa Izba Rozliczeniowa S.A. (Polska) – LuxTrust S.A. (Luksemburg) – Microsec Micro Software Engineering & Consulting Spółka Prywatna z ograniczoną odpowiedzialnością (Węgry) – MULTICERT – Serviços de Certificação Electrónica S.A. (Portugalia) – NETLOCK Informatics and Network Privacy services Limited Company (Węgry) Następujące dodatkowe QTSP wydają certyfikaty testowe do celów PSD2, ale nie rozpoczęły jeszcze wydawania certyfikatów PSD2 eIDAS: Bundesdruckerei GmbH (D-Trust GmbH) (Niemcy); FINA - Agencija Financijska (Chorwacja); CERTSIGN S.A. (Rumunia); Bank-Verlag (Niemcy) Około 10 spośród powyższych QTSP poinformowało EUNB, że wydaje/zamierza wydawać certyfikaty eIDAS do celów PSD2 i certyfikaty testowe TPP (i wnioskodawcom) upoważnionym/zarejestrowanym w innym państwie członkowskim niż państwo, w którym ma siedzibę QTSP. EBA informuje, że powyższa lista nie jest wyczerpująca i jest poprawna dopiero w chwili publikacji w dniu 11 marca 2019 r. Mogą istnieć inne QTSP upoważnione w UE, które wydają certyfikaty eIDAS do celów PSD2. EUNB rozumie również, że kilka dodatkowych QTSP zamierza w najbliższej przyszłości wydawać certyfikaty eIDAS do celów PSD2 i testować certyfikaty.

Problem	Wydajność API i wsparcie
Opis	Wymóg określonego w art. 32 rozporządzenia delegowanego Komisji (UE) 2018/389 (RTS w sprawie SCA i CSC) dotyczącego dostawców usług płatniczych prowadzących rachunek (ASPSP), aby zapewnić, że ich dedykowany interfejs oferuje „przez cały czas ten sam poziom dostępność, wydajność i wsparcie jako interfejsy twarzy zasilacza ”. Dwa rodzaje interfejsów nie są porównywalne, że dedykowane interfejsy będą musiały stawić czoła większemu ruchowi danych. Trudno byłoby zapewnić całodobową obsługę interfejsu API. Należy określić konkretne absolutne miary dla dedykowanych interfejsów
Propozycja	Artykuł 32 ust. 1 RTS w sprawie SCA i CSC wymaga, aby ASPSP zapewniały, aby ich dedykowany interfejs zapewniał „przez cały czas ten sam poziom dostępności, wydajności i wsparcia”, jak interfejsy udostępniane własnym użytkownikom usług płatniczych (PSU) bezpośrednio dostęp do ich kont płatniczych online. Oznacza to, że dostępność, wydajność i wsparcie dla dedykowanego interfejsu powinny co najmniej odpowiadać tym dla interfejsów zasilacza. Z tego powodu EBA nie może zdefiniować absolutnych poziomów odniesienia dla dedykowanych interfejsów ASPSP, ponieważ te ostatnie będą zależeć od wydajności, dostępności i wsparcia oferowanego przez każdy ASPSP jego własnym zasilaczom, gdy używane są interfejsy skierowane do PSU, i mogą się one różnić w zależności od ASPSP . Na przykład, jeśli dostępność interfejsu zasilacza wynosi 99,9%, interfejs dedykowany powinien (przynajmniej) być taki sam. Jeśli chodzi o wsparcie, z kolei zapewnienie w RTS oznacza, że ostatnie będą zależeć od wydajności, dostępności i wsparcia oferowanego przez każdy ASPSP jego własnym zasilaczom, gdy używane są interfejsy skierowane do PSU, i mogą się one różnić w zależności od ASPSP . Na przykład, jeśli dostępność interfejsu zasilacza wynosi 99,9%, interfejs dedykowany powinien (przynajmniej) być taki sam. Jeśli chodzi o wsparcie, z kolei zapewnienie w RTS oznacza, że poziom wsparcia oferowanego dla interfejsu dedykowanego musi być taki sam jak poziom oferowany interfejsom klienta przez cały czas, w tym poza godzinami pracy wsparcie. Na przykład, jeśli ASPSP oferuje swoim klientom wsparcie 24/7 podczas korzystania z interfejsów zasilających, powinien oferować taką samą obsługę TPP dla dedykowanego interfejsu. Ponadto art. 32 ust. 2 RTS w sprawie SCA i CSC oraz wytyczna 2.1 Wytycznych EBA w sprawie warunków korzystania ze zwolnienia z mechanizmu awaryjnego (EBA / GL / 2018/07) wymagają od ASPSP określenia kluczowych wskaźników wydajności (KPI) i cele na poziomie usług „w tym w zakresie rozwiązywania problemów, wsparcia poza godzinami pracy, monitorowania, planów awaryjnych i konserwacji” dla ich dedykowanych interfejsów, które są „co najmniej tak rygorystyczne jak” dla ich interfejsów (interfejsów) zasilających. Wreszcie, jak wyjaśniono w raporcie końcowym na temat wyżej wymienionych wytycznych, jeśli ASPSP oferuje więcej niż jeden interfejs zorientowany na klienta, wskaźniki KPI i cele poziomu usług dla interfejsu dedykowanego powinny odpowiadać najlepszym wskaźnikom KPI i celom poziomu usług we wszystkich Interfejsy zorientowane na klienta ASPSP. Z tego powodu wytyczna 3.2 wymaga od ASPSP publikowania danych na temat dostępności i wydajności dedykowanego interfejsu oraz każdego z interfejsów udostępnianych PSU.

Problem	Lista TPP zainteresowanych testowaniem
Opis	Brak opublikowanej listy zainteresowanych dostawców zewnętrznych (TPP) do celów testowania może powodować, że ASPSP mogą mieć trudności z dentyfikacją TPP chętnych do przetestowania interfejsów opracowanych przez ASPSP. Wytworzyła się sugestia utworzenia centralnej listy TPP (i innych podmiotów działających jako TPP), którzy są zainteresowani estowaniem interfejsów API ASPSP, a najlepiej, aby EBA utworzył taką listę. Wymaganie łatwo dostępnych informacji w celu zidentyfikowania ASPSP, które mają interfejs gotowy do estowania.
Propozycja	Artykuł 30 ust. 5 RTS w sprawie SCA i CSC wymaga, aby ASPSP udostępniali „narzędzie testujące, w tym wsparcie, w zakresie testowania połączeń i działania" interfejsu dostępu, który opracowują dla TPP, aby umożliwić TPP przetestowanie swojego „oprogramowania i aplikacji" . Takie testy będą miały podstawowe znaczenie dla TPP, ponieważ będą musieli zintegrować interfejs ASPSP z oprogramowaniem i aplikacjami służącymi do oferowania użytkownikom usług płatniczych. Testowanie jest równie ważne dla ASPSP, zanim uruchomią interfejs produkcyjny. Ponadto jedno z czterech kryteriów, które należy spełnić zgodnie z art. 33 ust. 6 RTS w sprawie SCA i CSC w przypadku, gdy ASPSP opracuje dedykowany interfejs i chce uzyskać zwolnienie, aby interfejs ten został przetestowany zgodnie z art. 30 ust. 5 RTS. W tym kontekście wytyczna 6.6 wytycznych EBA dotyczących zwolnienia z mechanizmu awaryjnego stanowi, że „ASPSP powinien przekazać właściwemu organowi streszczenie wyników badań, o których mowa w art. 30 ust. 5 RTS. Obejmuje to iczbę TPP, którzy korzystali z narzędzia do testowania, a także informacje zwrotne otrzymane przez ASPSP od tych TPP. Zdanie EBA: ' branża jest lepiej przygotowana do rozwiązania tego problemu" oraz ' na rynku opracowano szereg inicjatyw mających pomóc ASPSP w identyfikacji TPP dostępnych do testowania i odwrotnie, w informowaniu TPP o tym, które ASPSP opracowali interfejsy PSD2, które są gotowe do testowania". Istnieje dziewięć takich inicjatyw reprezentowanych w grupie roboczej EBA ds. Interfejsów API. EBA z zadowoleniem przyjmuje takie inicjatywy branżowe i zachęca uczestników branżowych, w tym wszystkie rodzaje stowarzyszeń branżowych (reprezentujących TPP lub ASPSP), do publikowania informacji na temat obiektów testowych ASPSP (w tym linków do portali programistów ASPSP) oraz TPP dostępnych do testowania w celu wsparcia okres testowy.

Problem	Testowanie przez podmioty, które nie są autoryzowanymi TPP
Opis	W jaki sposób ASPSP zidentyfikowaliby podmioty, które złożyły wniosek o autoryzację jako TPP? Czy ASPSP powinny oferować dostęp do swojej infrastruktury testowej podmiotom, które nie są (1) autoryzowanymi dostawcami usług płatniczych lub (2) podmiotami, które złożyły wniosek o autoryzację jako TPP (np. Dostawcy usług technicznych)? Jeśli odpowiedź brzmi „tak" to czy ASPSP powinien oferować ten sam poziom usług skierowanym podmiotom?
Propozycja	Konieczność prawnej interpretacji istniejących wymagań określonych w PSD2 i / lub instrumentach prawnych EBA, dlatego też została udzielona jako odpowiedź w narzędziu pytań i odpowiedzi EBA, jak w pytaniach i odpowiedziach 4609 opublikowanych 29 marca 2019 r.

Problem	Timelines for the fall-back exemption process
Opis	Większa przejrzystość w odniesieniu do terminów obowiązujących w 28 państwach członkowskich UE w odniesieniu do procesu do 14 września 2019 r. W przypadku wniosków ASPSP o zwolnienie z mechanizmu awaryjnego na mocy art. 33 ust. 6 RTS w sprawie SCA i CSC.
Propozycja	Tabelę odnajdziemy w zakładce Documents pod linkiem poniżej. Tabela zawiera orientacyjne terminy dla wszystkich państw członkowskich UE. https://eba.europa.eu/eba-publishes-clarifications-to-the-second-set-of-issues-raised-by-its– working-group-on-apis-under-psd2

Problem	Możliwość przenoszenia danych dotyczących "szerokiego wykorzystania" między państwami członkowskimi
Opis	Wykorzystanie zgromadzonych danych wykazujących "szerokie użytkowanie" dedykowanego interfejsu, opracowanych w państwie państwie członkowskim przez ASPSP należącego do grupy ASPSP, jako dowodu na spełnienie warunku "szerokie stosowanie" w innym państwie członkowskim w odniesieniu do odrębnego ASPSP należącego do tej samej grupy, pod warunkiem że oba podmioty stosują ten sam dedykowany interfejs.
Propozycja	Na to pytanie udzielono odpowiedzi za pomocą narzędzia Q&A EBA, opublikowanego 26 kwietnia 2019 r., jako Q&A nr 4638.

Problem	Certyfikaty paszportowe i certyfikaty eIDAS
Opis	Konieczność sprawdzenia przez ASPSP , czy TPP są upoważnione do działania w swoim państwie członkowskim w ramach swobodnego świadczenia usług lub prawa przedsiębiorczości, biorąc pod uwagę, że certyfikaty PSD2 eIDAS nie zawierają żadnych informacji paszportowych.
Propozycja	Na to pytanie udzielono odpowiedzi za pomocą narzędzia Q&A EBA, opublikowanego 26 kwietnia 2019 r., jako Q&A nr 4432.

Problem	Stosowanie certyfikatów eIDAS w okresie "szerokiego użytkowania" przed 14.09.2019 r.
Opis	Czy stosowanie certyfikatów eIDAS jest obowiązkowe w trzymiesięcznym okresie "szerokiego wykorzystania", określonym w art. 33 ust. 6 lit. c) RTS w sprawie SCA&CSC, w celu uzyskania dostępu do rachunków płatniczych za pośrednictwem API przed datą zastosowania RTS, tj. 14 września 2019 r.
Propozycja	Na to pytanie udzielono odpowiedzi za pomocą narzędzia Q&A EBA, opublikowanego 26 kwietnia 2019 r., jako Q&A nr 4430.

Problem	Korzystanie przez TPP z usług agentów i zleceniobiorców w celu uzyskania dostępu do danych z rachunków płatniczych
Opis	Czy ASPSP jest zobowiązany do sprawdzenia jedynie głównego TPP określonego w certyfikacie? Nawet w przypadku gdy agent wykorzystywany przez TPP jest zarejestrowany i pojawia się w rejestrze krajowym, ASPSP nie ma prawnego obowiązku sprawdzenia istnienia lub statusu takiego agenta. Niektóre inicjatywy API, takie jak STET, opracowały podejście, dzięki któremu TPP mogą oświadczyć, że wniosek pochodzi od agenta, ale wyjaśnili, że zgodnie ze standardami STET jest to opcja dla TPP, a nie wymóg. Jeżeli API pozwala na przesyłanie takich informacji, należy zachęcić ASPSP do dostarczania tych informacji do użytkownika usług płatniczych. Powinien istnieć automatyczny mechanizm zwrotu w przypadku, gdy agent jest oszustem lub został wykreślony z rejestru, oraz że w przypadku braku takiego mechanizmu ASPSP powinien mieć możliwość ostrzeżenia użytkownika usług płatniczych
Propozycja	Zgodnie z art. 34 Commission Delegated Regulation (UE) 2018/389 (RTS w sprawie SCA&CSC), TPP muszą zidentyfikować się wobec ASPSP w celu uzyskania dostępu do danych dotyczących rachunków płatniczych klientów, przy użyciu certyfikatu eIDAS. Jak wyjaśniono w pkt 21 opinii EBA w sprawie stosowania certyfikatów eIDAS w ramach RTS dotyczących SCA&CSC (EBA-Op-2018-7), jeżeli certyfikat eIDAS przedstawiany jest przez agenta lub TSP działającego w imieniu TPP, certyfikat powinien jednoznacznie określać główną TPP, w imieniu której działa agent lub TSP.Ponadto, jak wyjaśniono w opinii EBA, o której mowa powyżej, TPP pozostaje w pełni odpowiedzialna i odpowiedzialna za działania swoich agentów i dostawców usług zewnętrznych, jak również za unieważnienie i aktualizację wykorzystywanych przez nich certyfikatów eIDAS. Ponadto TPP powinny zapewnić przestrzeganie przez nie własnych wymogów w zakresie informacji i ujawniania informacji wobec użytkownika usług płatniczych, jak określono w tytule III dyrektywy w sprawie usług płatniczych2. EUNB zauważa również, że art. 19 ust. 6 dyrektywy w sprawie usług płatniczych2 wyraźnie zobowiązuje instytucje płatnicze do zapewnienia, aby agenci działający w ich imieniu informowali użytkowników usług płatniczych o tym fakcie. Dlatego też ASPSP nie jest odpowiedzialny za poinformowanie użytkownika usług płatniczych, że TPP działa za pośrednictwem agenta. W odniesieniu do podejść opracowanych najwyraźniej w ramach niektórych inicjatyw API w zakresie identyfikacji agentów EBA powtarza, że chociaż podejścia te mogą rzeczywiście ułatwić identyfikację agenta ubiegającego się o dostęp w imieniu TPP, ASPSP są prawnie zobowiązane jedynie do identyfikacji TPP, a nie jej agenta.W odniesieniu do możliwości ostrzegania przez ASPSP użytkowników usług płatniczych lub blokowania dostępu EBA zauważa, że zgodnie z art. 68 ust. 5 dyrektywy w sprawie usług płatniczych2 ASPSP jest uprawniony do blokowania dostępu do danych dotyczących rachunków płatniczych TPP z "obiektywnie uzasadnionych i należycie udokumentowanych powodów", które powinny być związane jedynie z "nieuprawnionym lub nieuczciwym dostępem do rachunku płatniczego" przez TPP.W takim przypadku, zgodnie z art. 68 ust. 6 dyrektywy w sprawie usług płatniczych2 , ASPSP powinien niezwłocznie zgłosić incydent do krajowego organu ochrony konkurencji, podając powody podjęcia takiego działania. PSD2 nie ogranicza ASPSP w zakresie informowania PSU o tym, że dokonał takiego blokady oraz o przyczynach takiego działania.

Problem	"Szeroko stosowany" oraz "projekt spełniający warunki TPP"
Opis	EUNB złagodził wymogi dotyczące udziału TPP w procesie przyznawania wyłączenia dla API, jak stwierdzono w SCA&CSC RTS, w szczególności warunki określone w art. 3 ust. 1 lit. b) i c). 33 ust. 6 lit. b) i c) RTS dotyczących SCA&CSC w odniesieniu do projektowania i testowania w sposób zadowalający dla TPP i warunków szerokiego zastosowania. Pojawiają się obawy, że może to pozostawić otwarte drzwi dla obowiązkowego stosowania nieodpowiednich API.
Propozycja	Jak opisano w sprawozdaniu końcowym dotyczącym wytycznych w sprawie warunków korzystania z wyłączenia spod mechanizmu rezerwowego (EUNB/GL/2018/07), EUNB otrzymał te same uwagi, gdy jesienią 2018 r. konsultował się w sprawie projektu wytycznych, zgodził się, że obawy te są uzasadnione i wprowadził szereg zmian w celu rozwiązania tych obaw, zanim opublikował ostateczne wytyczne. W szczególności EUNB usprawnił sposób, w jaki można zaangażować TPP w proces wyłączeń. Na przykład wytyczna 6 wymaga, aby APSP przekazywały właściwemu organowi krajowemu (NCA) informacje zwrotne otrzymane od TPP, które wzięły udział w badaniu, oraz wyjaśniały, w jaki sposób rozwiązały problemy zgłoszone przez TPP. Wytyczne wymagają również, aby ASPSP przekazywały krajowym organom ds. konkurencji informacje na temat ich współpracy z TPP oraz wyjaśniają, że aby spełnić warunek "projektowania", ASPSP muszą udowodnić, że ich API jest zgodne ze wszystkimi wymogami prawnymi dotyczącymi dostępu do danych w PSD2 i RTS, w tym z wymogiem nietworzenia "przeszkód" w przekazywaniu informacji o rachunkach i usługach inicjowania płatności, jak przewidziano w art. 33 ust. 2 RTS dotyczących SCA&CSC. W wytycznych wyjaśniono również, że warunek "szerokiego wykorzystania" należy ocenić, biorąc pod uwagę liczbę TPP, które korzystały z interfejsu produkcyjnego ASPSP w celu oferowania usług swoim klientom, liczbę udanych wniosków przesłanych przez TPP za pośrednictwem dedykowanego interfejsu w ciągu trzymiesięcznego okresu użytkowania, ale także inne czynniki, takie jak kroki podjęte przez ASPSP w celu osiągnięcia "szerokiego wykorzystania". EUNB zdecydowanie zachęca TPP do testowania interfejsów API opracowywanych przez ASPSP oraz do przekazywania ASPSP informacji zwrotnych na temat wszelkich problemów, które napotykają w związku z interfejsami testowymi lub produkcyjnymi, tak aby ASPSP mogły zająć się tymi problemami i opracować API o wysokiej wydajności i zorientowane na klienta.

Problem	ASPSP polegające na certyfikatach eIDAS
Opis	Obawy, że może wystąpić potencjalne niedopasowanie informacji zawartych w certyfikacie PSD2 systemu eIDAS do informacji zawartych w EUNB i rejestrach krajowych, w szczególności w przypadku cofnięcia zezwolenia. Uczestnicy rynku wyrazili również obawy, że ASPSP nie mogą polegać na informacjach zawartych w rejestrach EUNB i rejestrach krajowych w celu identyfikacji TPP po dacie rozpoczęcia stosowania RTS dotyczących SCA&CSC oprócz stosowania certyfikatów eIDAS. W opinii tych uczestników krajowe organy ds. ochrony konkurencji powinny powiadamiać o cofnięciu zezwolenia dla TPP dostawcę kwalifikowanych usług zaufania (QTSP), który wydał odpowiedni certyfikat eIDAS PSD2 (i który może również cofnąć wspomniany certyfikat), zgodnie z pkt 32 opinii EUNB w sprawie obowiązkowego stosowania certyfikatów eIDAS.Jeden z uczestników sektora zapytał również, czy istnieje odpowiedni czas na zapewnienie dostępu do danych rachunku TPP, której zezwolenie zostało cofnięte z rejestrów, ale której certyfikat eIDAS nadal obowiązuje.
Propozycja	Zgodnie z art. 34 RTS dotyczących SCA&CSC, do celów identyfikacji, o której mowa w art. 30 ust. 1 lit. a), dostawcy usług płatniczych polegają na kwalifikowanych certyfikatach pieczęci elektronicznych, o których mowa w art. 3 ust. 30 rozporządzenia (UE) nr 910/2014, lub uwierzytelnianiu stron internetowych, o którym mowa w art. 3 ust. 39 tego rozporządzenia (rozporządzenie w sprawie systemu identyfikacji elektronicznej). Oznacza to, że jeżeli TPP identyfikuje się wobec ASPSP za pomocą certyfikatu eIDAS PSD2 , ASPSP udziela dostępu do TPP do określonego rachunku. ASPSP mogą jednak zdecydować się na przeprowadzenie dodatkowych kontroli statusu autoryzacji/rejestracji TPP w odpowiednich EUNB lub rejestrach krajowych, pod warunkiem że w ten sposób ASPSP nie stwarzają przeszkód w świadczeniu usług inicjowania płatności lub usług w zakresie informacji o rachunku, zgodnie z wymogami art. 32 ust. 3 RTS. W odniesieniu do aktualizacji informacji publicznych w przypadku cofnięcia zezwolenia art. 13 ust. 3 dyrektywy w sprawie usług płatniczych2 wymaga, aby krajowe organy ds. ochrony konkurencji podawały do wiadomości publicznej każde cofnięcie zezwolenia, w tym w swoich rejestrach krajowych i rejestrze EBA PSD2 . W odniesieniu do publikowania informacji w wykazach branżowych ani EBA, ani krajowe organy ds. ochrony konkurencji nie mają obowiązku aktualizowania takich wykazów i w związku z tym nie ponoszą żadnej odpowiedzialności za dokładność jakichkolwiek dostarczonych przez nie informacji.W odniesieniu do sugestii, aby krajowe organy ds. ochrony konkurencji były zobowiązane do odgrywania aktywnej roli w unieważnieniu certyfikatów PSD2 systemu eIDAS, należy zauważyć, że zgodnie z wymogami rozporządzenia w sprawie systemu eIDAS, w pkt 31 opinii EBA w sprawie stosowania certyfikatów eIDAS w ramach RTS dotyczących SCA&CSC (EBA-Op-2018-7) wyjaśnia się, że "dostawcy kwalifikowanych usług zaufania są odpowiedzialni za sprawdzanie ważności informacji zawartych w certyfikatach eIDAS w momencie wydawania certyfikatu, a zarówno dostawcy usług QTSP, jak i dostawcy usług płatniczych są odpowiedzialni za zapewnienie aktualności informacji oraz za cofnięcie certyfikatów". Aby rozwiać obawy zgłaszane przez branżę w czasie przygotowywania opinii, pkt 32 tej samej opinii EBA idzie o krok dalej, ustanawiając proces, w ramach którego krajowe organy ds. ochrony konkurencji mogą wnioskować o cofnięcie certyfikatu eIDAS w przypadku cofnięcia zezwolenia dostawcy usług płatniczych, ale nie zostały poinformowane ani przez podmiot świadczący usługi żeglugi powietrznej, ani przez dostawcę usług płatniczych, że certyfikat tego ostatniego został cofnięty. Krajowe organy ds. ochrony konkurencji nie są zobowiązane do przestrzegania tego procesu na mocy prawa UE, instrumentu prawnego EBA, prawa krajowego lub przepisów krajowych. Proces ten stanowi raczej mechanizm, którego należy przestrzegać na zasadzie dobrowolności, polegający na tym, że krajowe organy ds. ochrony konkurencji powiadamiają odpowiedni krajowy organ ds. ochrony danych o zmianie statusu upoważnienia lub zakresu działalności danego PSP, umożliwiając tym samym krajowym organom ds. ochrony danych przeprowadzanie kontroli, które są one zobowiązane przeprowadzić na mocy rozporządzenia w sprawie systemu eIDAS w celu cofnięcia certyfikatu. Należy zauważyć, że dostawcy usług QTSP pozostają po swojej stronie odpowiedzialni za sprawdzanie wiarygodności certyfikatów, które wydają na mocy rozporządzenia w sprawie systemu eIDAS. Z kolei dostawcy usług płatniczych pozostają w podobny sposób odpowiedzialni za wiarygodność wykorzystywanych przez siebie certyfikatów. Należy zauważyć, że wskazówki zawarte w załączniku nie gwarantują, że krajowy organ ds. bezpieczeństwa zażąda cofnięcia certyfikatu eIDAS w każdym przypadku, ponieważ specyfika cofnięcia zezwolenia może wymagać od krajowego organu ds. bezpieczeństwa podjęcia innych działań.

Problem	Potwierdzenie dokonania płatności
Opis	Czy od ASPSP wymaga się dostarczania informacji na temat inicjowania i realizacji transakcji płatniczej, w tym aktualizacji, w celu zapewnienia zgodności dostawcy usług inicjowania płatności (PISP) z art. 46 lit. a) PSD2
Propozycja	Na to pytanie udzielono odpowiedzi za pomocą narzędzia Q&A EBA, opublikowanego 7 czerwca 2019 r., jako Q&A nr 4061.

Problem	Biometria i uwierzytelnianie w aplikacjach mobilnych
Opis	Dostawcy usług płatniczych powinni umożliwiać dostawcom AIS i PIS poleganie na wszystkich procedurach uwierzytelniania zapewnianych przez ASPSP swoim użytkownikom usług płatniczych. ASPSP wspierające wykorzystanie danych biometrycznych w swoich kanałach komórkowych/online powinny również wspierać uwierzytelnianie poprzez dane biometryczne w swoich dedykowanych interfejsach. Jest to niezbędne w celu zapewnienia bezproblemowego doświadczenia klienta, a nie stwarzania przeszkód w dostarczaniu AIS i PIS.
Propozycja	ASPSP powinny dopilnować, aby ich dedykowany interfejs nie przeszkodził PISP i AISP w poleganiu na procedurze(-ach) uwierzytelniania zapewnianej(-ych) przez ASPSP swoim użytkownikom usług płatniczych. Dedykowane interfejsy ASPSP powinny obsługiwać wszystkie metody uwierzytelniania udostępniane przez ASPSP swoim użytkownikom usług płatniczych w przypadku korzystania z AISP lub PISP. W związku z tym metoda dostępu lub połączenie metod, które powinien obsługiwać dedykowany interfejs, będzie zależeć od procedur uwierzytelniania, które ASPSP oferuje swoim użytkownikom usług płatniczych, oraz od tego, czy poświadczenia bezpieczeństwa mogą być przekazywane (takie jak hasła), czy też nie (takie jak dane biometryczne).

Problem	Dostęp do informacji o rachunkach niedotyczących płatności
Opis	Stosowanie przez TPP różnych metod dostępu do danych rachunków, w zależności od rodzaju rachunku, do którego uzyskują dostęp (np. używać interfejsów API w celu uzyskania dostępu do danych rachunków płatniczych, a interfejs klienta w celu uzyskania dostępu do rachunków niedotyczących płatności). Przy uzyskiwaniu dostępu do danych z rachunków niedotyczących płatności przy użyciu interfejsu klienta, na przykład poprzez screen-scraping, w szczególności dla dostawców AIS, zapewnienie, że nie uzyskują oni również przypadkowo dostępu do danych dotyczących rachunków płatniczych jest bardzo trudne dla TPP, zważywszy, że TPP mogą nie być w stanie odróżnić rachunków będących rachunkami płatniczymi od rachunków niedotyczących płatności. Czy TPP uzyskujące dostęp do danych dotyczących rachunków niedotyczących płatności za pośrednictwem interfejsu klienta powinny mieć również możliwość dostępu do podlegających im danych dotyczących rachunków płatniczych: -Identyfikacja takich rachunków na poziomie podsumowania, bez uwzględniania szczegółów transakcji, tam gdzie to możliwe; -Usunięcie danych dotyczących płatności przechwyconych w tym procesie (dane dotyczące rachunków płatniczych nie powinny być przetwarzane w sposób wykraczający poza to, co jest konieczne do ich identyfikacji). API WG uznało jednak, że na TPP spoczywa odpowiedzialność za zapewnienie zgodności TPP z wymogami PSD2 i RTS w zakresie dostępu do rachunków płatniczych oraz że ASPSP nie mają prawnego obowiązku udostępniania danych dotyczących rachunków innych niż płatnicze dostawcom zewnętrznym, ani dokumentowania, w jaki sposób TPP mogą uniknąć przechwytywania zbiorów danych PSD2 podczas skrawania ekranu w celu uzyskania danych dotyczących rachunków innych niż płatnicze. Jeden z uczestników grupy roboczej ds. API zauważył również, że ASPSP muszą mieć podstawę prawną zgodnie z ogólnym rozporządzeniem o ochronie danych (PKBR), aby móc udostępniać dane dotyczące rachunków innych niż płatnicze TPP.
Propozycja	Wymogi określone w PSD2 i RTS dotyczące dostępu TPP do danych z rachunków klientów mają zastosowanie wyłącznie w odniesieniu do rachunków płatniczych i nie obejmują innych rodzajów rachunków płatniczych. Rachunek płatniczy jest zdefiniowany w art. 4 ust. 12 PSD2 jako "rachunek prowadzony w imieniu jednego lub większej liczby użytkowników usług płatniczych, wykorzystywany do realizacji transakcji płatniczych".Definicja rachunków płatniczych została doprecyzowana w orzecznictwie Europejskiego Trybunału Sprawiedliwości (ETS) – zob. w szczególności wyrok ETS z dnia 4 października 2018 r., w sprawie C-191/17, dostępny pod adresem: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-191/17. Chociaż wyrok ETS został wydany w odniesieniu do rachunku oszczędnościowego na mocy dyrektywy 2007/64/WE (PSD1), określone w nim zasady mają również zastosowanie w kontekście PSD2, biorąc pod uwagę fakt, że definicja "rachunków płatniczych" w ramach PSD2 pozostała zasadniczo taka sama jak w ramach PSD1 . Od dnia 14 września 2019 r. elektrownie TPP powinny mieć dostęp do danych dotyczących rachunków płatniczych zgodnie z wymogami określonymi w dyrektywie w sprawie usług płatniczych2 i w RTS.Jak podkreślono w art. 66 ust. 3 lit. g) i art. 67 ust. 2 lit. f) PSD2, obowiązkiem AISP/PISP jest zapewnienie, aby nie wykorzystywały, nie uzyskiwały dostępu ani nie przechowywały danych, które nie są niezbędne do wykonania AIS/PIS, których zażądał użytkownik usług płatniczych; obowiązek ten nie spoczywa na ASPSP. Ponadto zarówno ASPSP, jak i TPP są zobowiązane do przestrzegania swoich zobowiązań wynikających z prawodawstwa UE w zakresie ochrony danych (GDPR), które stosuje się do wszystkich przetwarzanych przez nie danych osobowych.

Problem	Testy warunków skrajnych
Opis	Czy testy wytrzymałościowe dedykowanych interfejsów ASPSP mogą być przeprowadzane w środowisku testowym o cechach bardzo zbliżonych do rzeczywistego środowiska produkcyjnego i czy byłoby to zgodne z wytycznymi EBA w sprawie wyłączenia z mechanizmu awaryjnego w art. 33 ust. 4 RTS. – Testy warunków skrajnych wiążą się z obsługą dużych ilości wniosków od TPP i nie jest łatwo włączyć taką ilość wniosków w środowisku produkcyjnym bez rzeczywistych użytkowników (i zgody użytkownika) stojących za tymi usługami; – Testy warunków skrajnych w środowisku produkcyjnym mogłyby mieć wpływ na poziomy usług już uzgodnione z zasilaczem w przypadku innych interfejsów internetowych i serwerów wykorzystujących to samo środowisko produkcji.
Propozycja	Jak określono w wytycznej 4.1 wytycznych EUNB w sprawie warunków korzystania z wyłączenia spod mechanizmu rezerwowego (EUNB/GL/2018/07), "Do celów testów warunków skrajnych, o których mowa w art. 32 ust. 2 RTS, ASPSP powinien posiadać procedury ustanawiania i oceny sposobu działania dedykowanego interfejsu w przypadku poddania go wyjątkowo dużej liczbie wniosków ze strony PISP, AISP i CBPII, pod względem wpływu, jaki taki nacisk wywiera na dostępność i działanie dedykowanego interfejsu oraz określone cele w zakresie poziomu usług".Można to osiągnąć, przeprowadzając testy warunków skrajnych w środowisku o takiej samej infrastrukturze i funkcjach jak w przypadku produkcji dedykowanych interfejsów i nie ma potrzeby angażowania rzeczywistych klientów. Takie podejście jest zgodne z wymogami wyżej wymienionych wytycznych EBA, pod warunkiem że wymogi określone w tych wytycznych są spełnione.

Problem	Kwalifikowane certyfikaty eIDAS dla ASPSP
Opis	Czy instytucja kredytowa pełniąca rolę TPP musi uwzględnić te role w swoim certyfikacie eIDAS zgodnie z art. 34 RTS
Propozycja	Jak wyjaśniono w pkt 27 opinii EBA w sprawie stosowania certyfikatów eIDAS w ramach RTS dotyczących SCA&CSC (EBA-Op-2018-7), "instytucje kredytowe mogą świadczyć wszystkie usługi płatnicze, o których mowa w załączniku I do PSD2, w ramach zezwolenia udzielonego im na mocy dyrektywy 2013/36/UE bez uzyskania zezwolenia w odniesieniu do każdej świadczonej przez nie usługi płatniczej. Dlatego też instytucjom kredytowym, które działają w charakterze dostawcy będącego stroną trzecią (niezależnie od tego, czy jest to AISP, PISP czy CBPII), należy przypisać jednocześnie trzy role "inicjowania płatności", "informacji o rachunku" i "wydawania instrumentów płatniczych opartych na kartach".28 wspomnianej opinii wyjaśnia dalej, że "w scenariuszu, w którym dostawca usług płatniczych działa w charakterze ASPSP i oferuje użytkownikom usług płatniczych, które są dostępne online, wspomnianemu dostawcy usług płatniczych należy przypisać rolę "obsługi rachunku". Zostało to również wyjaśnione w Q&A 4413.

Problem	Dzielenie numeru rachunku płatniczego z PISP
Opis	Propozycja aby ASPSP dzieliły rachunek płatniczy IBAN/numer identyfikacyjny z PISP. Ryzyko oszustwa jest szczególnie wysokie w przypadku zwrotów dokonywanych przez handlowca za pośrednictwem PISP, ponieważ proces zwrotu może być potencjalnie wykorzystywany przez oszustów w celu otrzymania pieniędzy na innym koncie. W przypadku wniosku o zwrot pieniędzy, handlowcy zazwyczaj zwracają pieniądze klientowi w ten sam sposób, w jaki klient dokonał pierwotnej płatności, oraz że w celu otrzymania zwrotu pieniędzy klient potrzebuje jedynie numeru referencyjnego zamówienia, opisu produktu lub jego danych adresowych. Uczestnik twierdził, że oszustom stosunkowo łatwo jest uzyskać te informacje, a następnie ubiegać się o zwrot pieniędzy na inne konto.
Propozycja	W odniesieniu do dzielenia numeru rachunku przez ASPSP z PISP, w Q&A4188 wyjaśniono, że ASPSP są zobowiązane jedynie do dostarczania lub udostępniania PISP informacji niezbędnych do zapewnienia PISP.To samo pytanie i odpowiedzi wyjaśnia, że ponieważ to zawsze użytkownik usług płatniczych określa rachunek, z którego ma zostać zainicjowana transakcja, nie ma potrzeby, aby ASPSP dostarczał dostawcy PIS lub udostępniał mu wykaz wszystkich numerów rachunków użytkownika usług płatniczych, "o ile nie stworzyłoby to przeszkód w udostępnianiu PIS zgodnie z art. 32 ust. 3 [RTS]".W związku z tym EUNB wyjaśnił również w sprawozdaniu końcowym dotyczącym wytycznych EUNB w sprawie warunków korzystania z wyłączenia z mechanizmu awaryjnego (tabela informacji zwrotnej, strona 71, uwaga 80), że "jeżeli użytkownik usług płatniczych nie wybierze rachunku w domenie PISP, a rachunek nie jest z góry znany, [....]" ASPSP może zwrócić się do klienta o wybranie konta w domenie ASPSP, w ramach etapu uwierzytelniania, zanim klient zostanie przekierowany z powrotem do interfejsu PISP, co nie stanowi przeszkody". Refundacja transakcji zainicjowanej przez PISPmay lub nie implikuje użycia PISP. W takim przypadku sprzedawca i PSU uzgadniają sposób dokonania zwrotu oraz rachunek płatniczy, na którym zwrot zostanie uznany.

Problem	Machine-readability centralnego rejestru EUNB w ramach PSD2
Opis	Publikacja dokumentu wyjaśniającego pola danych i właściwości wykorzystywane w pliku JSON z zawartością centralnego rejestru strefy euro w ramach PSD2
Propozycja	EBA zgadza się, że wyjaśnienie pól danych w pliku JSON do odczytu maszynowego z informacjami zawartymi w centralnym rejestrze EBA w ramach PSD2 umożliwi uczestnikom rynku lepszą interpretację informacji zawartych w rejestrze. W związku z tym w dniu 5 sierpnia 2019 r. EBA opublikował dokument zawierający specyfikację właściwości danych pliku JSON z zawartością centralnego rejestru EBA w ramach PSD2, dostępny po prawej stronie powyższej strony internetowej.

Problem	Pomiar czasów reakcji dedykowanego interfejsu.
Opis	Co należy uwzględnić przy obliczaniu kluczowego wskaźnika skuteczności działania (KPI) dotyczącego czasu reakcji zgodnie z wytyczną 2.3 wytycznych EUNB w sprawie wyłączenia z mechanizmu awaryjnego? Czy obliczenia te powinny obejmować czas potrzebny na przeprowadzenie SCA czy też czas potrzebny ASPSP na weryfikację zezwoleń/rejestracji dostawców będących osobami trzecimi (TPP)?
Propozycja	Jak wyjaśniono w sprawozdaniu końcowym dotyczącym wytycznych EBA w sprawie warunków korzystania z wyłączenia z mechanizmu awaryjnego, czas na udzielenie odpowiedzi zgodnie z wytyczną 2.3 obejmuje "odstęp czasu pomiędzy momentem otrzymania wniosku przez ASPSP od PISP, AISP lubCBPII a momentem, w którym wszystkie żądane informacje (lub, w stosownych przypadkach, potwierdzenie tak/nie) zostały odesłane z powrotem przez ASPSP" (strona 43 tabeli informacji zwrotnych, uwagi 15). Na pytanie, czy czas potrzebny na przeprowadzenie SCA powinien być uwzględniony przy obliczaniu czasu odpowiedzi, udzielono odpowiedzi w Q&A 4661 opublikowanym w dniu 9 sierpnia 2019 r.

Problem	Mechanizm awaryjny w Art. 33 ust. 4 RTS – dane, do których można uzyskać dostęp.
Opis	Czy APSP muszą dokonywać jakichkolwiek zmian w istniejących interfejsach klienta w celu zastosowania mechanizmu awaryjnego, o którym mowa w art. 3 ust. 1 lit. a) i b)? 33 UST. 4 RTS. Czy ASPSP muszą ograniczać dane, do których TPP mogą uzyskać dostęp przez interfejs PSU przy użyciu mechanizmu awaryjnego, o którym mowa w art. 33 ust. 4 RTS? 33 UST. 4 RTS?
Propozycja	Zgodnie z art. 33 ust. 5 RTS, do celów mechanizmu awaryjnego, o którym mowa w art. 33 ust. 5 RTS, do celów mechanizmu awaryjnego, o którym mowa w art. 3 ust. 1 lit. b), nie ma potrzeby stosowania mechanizmu awaryjnego. 33 ust. 4 RTS, ASPSP powinny zapewnić możliwość identyfikacji TPP, co oznacza, że TPP są w stanie zidentyfikować się w stosunku do ASPSP przy użyciu certyfikatów eIDAS zgodnie z art. 34(1)RTS oraz że TPP mogą polegać na procedurach uwierzytelniania zapewnianych przez ASPSP swoim użytkownikom usług płatniczych. Mechanizm awaryjny powinien również umożliwiać TPP wykonywanie działań określonych w art. 1) RTS oraz że TPP mogą polegać na procedurach uwierzytelniania dostarczonych przez ASPSP swoim użytkownikom usług płatniczych. 30 ust. 1 RTS, a mianowicie do: – umożliwienie AISP "bezpiecznej komunikacji w celu żądania i otrzymywania informacji na temat jednego lub więcej wyznaczonych rachunków płatniczych i powiązanych transakcji płatniczych"; oraz – umożliwiającym PISP "bezpieczne komunikowanie się w celu zainicjowania zlecenia płatniczego z rachunku płatniczego płatnika i otrzymywanie wszelkich informacji o zainicjowaniu transakcji płatniczej oraz wszelkich informacji dostępnych dla ASPSP dotyczących realizacji transakcji płatniczej".

Problem	Dokumentacja mechanizmu awaryjnego, o którym mowa w art. 33(4) RTS
Opis	Czy ASPSP są wymagane do udokumentowania dostępu awaryjnego w Art. 33(4), a jeśli tak, to do kiedy.
Propozycja	Dostawcy usług płatniczych obsługujący rachunki uwzględniają w projekcie dedykowanego interfejsu strategię i plany dotyczące środków awaryjnych na wypadek, gdyby interfejs nie działał zgodnie z art. 32, gdyby interfejs był niedostępny w sposób nieplanowany oraz gdyby nastąpiła awaria systemów". RTS nie określa terminu, w którym ASPSP powinny udokumentować dostęp poprzez mechanizm awaryjny.

Problem	Dostępność i poleganie na certyfikatach eIDAS na podstawie art. 34 RTS
Opis	Trudności z uzyskaniem certyfikatów eIDAS (QWAC i QSealC), o których mowa w Art. 34 RTS od dostawców kwalifikowanych usług zaufania (QTSP).
Propozycja	EBA rozumie, że jedną z przyczyn opóźnień i trudności w wydawaniu certyfikatów eIDAS przez podmioty świadczące usługi obsługi klienta była niepewność co do interpretacji odniesienia do "numeru zezwolenia" w art. 34 ust. 2 RTS. W odpowiedzi EUNB wyjaśnił już w odpowiedzi na pytania i odpowiedzi 4679, że odniesienie do "numeru zezwolenia" w art. 34 ust. 2 RTS obejmuje "wszystkie formy krajowych numerów identyfikacyjnych, które są używane przez krajowe organy ds. ochrony konkurencji na mocy dyrektywy w sprawie usług płatniczych2 i umożliwiają jednoznaczną identyfikację dostawców usług płatniczych (PSP) w rejestrach krajowych na mocy dyrektywy w sprawie usług płatniczych2 i dyrektywy w sprawie wymogów kapitałowych (CRDIV), a także w rejestrach EUNB PSD2 i rejestrów instytucji kredytowych". Niemniej jednak, aby umożliwić podmiotom świadczącym usługi obsługi klienta lepszą interpretację informacji dostępnych w rejestrach PSD2 EBA i rejestrów instytucji kredytowych, EBA opublikował w dniu 31 lipca 2019 r. szereg dokumentów technicznych istotnych dla opinii EBA w sprawie stosowania certyfikatów ofeIDAS w ramach RTS dotyczących SCA&CSC (EBA-Op-2018-7), które są dostępne po prawej stronie powyższej strony internetowej. Obejmują one dokument z numerami identyfikacyjnymi stosowanymi w rejestrach EBA, wyjaśniający rodzaje krajowych numerów identyfikacyjnych stosowanych przez każdy krajowy organ ds. ochrony konkurencji w tych rejestrach. Ponadto w celu zapewnienia dodatkowej pewności podmiotom świadczącym usługi społeczeństwa informacyjnego w procesie wydawania certyfikatów PSD2 w ramach eIDAS EBA opublikował również w dniu 31 lipca 2019 r. dwa dodatkowe dokumenty ze skrótami NCA w celu włączenia ich do certyfikatów eIDAS oraz adresy poczty elektronicznej właściwych organów w celu wymiany powiadomień z QTSPs

National Competent Authority

Kraj	Kod	Nazwa (ang.)	Nazwa
Austria	AT_FMA	Austrian Financial Market Authority	Finanzmarktaufsicht
Belgia	BE_NBB	National Bank of Belgium	National Bank van Belgie / Banque Nationale de Belgique
Bułgaria	BG_BNB	Bulgarian National Bank	Българска народна банка
Cypr	CY_CBC	Central Bank of Cyprus	Κεντρική Τράπεζα της Κύπρου
Czechy	CZ_CNB	Czech National Bank	Česká národní banka
Niemcy	DE_BAFIN	Federal Financial Supervisory Authority	Bundesanstalt für Finanzdienstleistungsaufsicht
Dania	DK_DFSA	Danish Financial Supervisory Authority	Finanstilsynet
Estonia	EE_FI	Estonian Financial Supervision Authority	Finantsinspektsioon
Hiszpania	ES_BE	Bank of Spain	Banco de España
Finlandia	FI_FIN-FSA	Finnish Financial Supervisory Authority	Finanssivalvonta / Finansinspektionen
Francja	FR_ACPR	Prudential Supervisory and Resolution Authority	Autorité de Contrôle Prudentiel et de Résolution
Wielka Brytania	GB_FCA	Financial Conduct Authority (FCA)	
Grecja	GR_BOG	Bank of Greece	Η Τράπεζα της Ελλάδος
Chorwacja	HR_HNB	Croatian National Bank	Hrvatska Narodna Banka
Węgry	HU_CBH	Central Bank of Hungary	Magyar Nemzeti Bank
Irlandia	IE_CBI	Central Bank of Ireland	
Islandia	IS_FME	Financial Supervisory Authority	Fjarmalaeftirlitid
Włochy	IT_BI	Bank of Italy	Banca d

Lichtenstein	LI_FMA	Financial Market Authority Liechtenstein	Finanzmarktaufsicht Liechtenstein
Litwa	LT_BL	Bank of Lithuania	Lietuvos Bankas
Luksemburg	LU_CSSF	Commission for the Supervision of Financial Sector	Commission de Surveillance du Secteur Financier
Łotwa	LV_FCMC	Financial and Capital Market Commission	Finanšu un kapitāla tirgus komisija
Malta	MT_MFSA	Malta Financial Services Authority	
Holandia	NL_DNB	The Netherlands Bank	De Nederlandsche Bank
Norwegia	NO_FSA	The Financial Authority of Norway	Finanstilsynet
Polska	PL_PFSA	Polish Financial Supervision Authority	Polish Financial Supervision Authority Komisji Nadzoru Finansowego
Portugalia	PT_BP	Bank of Portugal	Banco de Portugal
Rumunia	RO_NBR	National Bank of Romania	Banca Naţională a României
Szwecja	SE_FINA	Swedish Financial Supervisory Authority	Finansinspektionen
Słowenia	SI_BS	Bank of Slovenia	Banka Slovenije
Słowacja	SK_NBS	National Bank of Slovakia	Národná banka Slovenska

Rejestr krajowy

Kraj	Kod	Nazwa właściwego organu	Link do strony	Link do rejestru i/ lub rejestracji i/lub instrukcji jak stać się instytucją płatniczą
AUSTRIA	AT-FMA	Financial Market Authority (FMA)	link	link
BELGIUM	BE-NBB	National Bank of Belgium (NBB)	link	link
BULGARIA	BG_BNB	Financial Supervision Commission (FSC)	link	link
CROATIA	HR-HNB	Hrvatska Narodna Banka (HNB)	link	
CYPRUS	CY_CBC	Central Bank of Cyprus (CBC)	link	
CZECH REPUBLIC (THE)	CZ_CNB	Czech National Bank (CNB)	link	
DENMARK	DK-DFSA	finanstilsynet (FSA)	link	
ESTONIA	EE-FI	FINANTSINSPEKTSIOON (FSA)	link	
FINLAND	FI-FINFSA	Finanssivalvonta (FIN-FSA)	link	
FRANCE	FR-ACPR	Autorité de Controle Prudentiel (ACPR) "Regafi"	link	
GERMANY	DE-BAFIN	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	link	
GREECE	GR-BOG	Bank Of Greece	link	
HUNGARY	HU-CBH	Magyar Nemzeti Bank (MNB)	link	
ICELAND	IS-FME	Narodna Banka Slovenska (NBS)	link	
IRELAND	IE-CBI	Central Bank of Ireland (CBI)	link	
ITALY	IT-BI	Banca d'Italia	link	
LATVIA	LV-FCMC	Finansu un Kapital Tirgus Komisija (FKTK)	link	
LIECHTENSTEIN	LI-FMA	Finanzmarktaufsicht Liechtenstein (FMA)	link	

LITHUANIA	LT-BL	Bank of Lithuania (LB)	link
LUXEMBOURG	LU-CSSF	Commission de Surveillance du Secteur Financier (CSSF)	link
MALTA	MT-MFSA	Malta Financial Services Authority (MFSA)	link
NETHERLANDS (THE)	NL-DNB	De Nederlandsche Bank (DNB)	link
NORWAY	NO-FSA	Finanstilsynet (FSA)	link
POLAND	PL-PFSA	Komisja Nadzoru Finansowego (KNF)	link
PORTUGAL	PT-BP	Banco De Portugal	link
ROMANIA	RO-NBR	Banca Nationala a Romaniei (BNR)	link
SLOVAKIA	SK-NBS	Narodna Banka Slovenska (NBS)	link
SLOVENIA	SI-BS	Banka Slovenije (BSI)	link
SPAIN	ES-BE	Banco de Espana (BDE)	link
SWEDEN	SE-FINA	Finansinspektionen (FI)	link
UNITED KINGDOM	GB-FCA	Financial Conduct Authority (FCA)	link

Właściwe Organy Krajowe do włączenia certyfikatów eIDAS do celów PSD2

Kod	Kraj	Tytył/Nazwa urzędu po angielsku	Tytuł/Nazwa Urzędu
AT-FMA	Austria	Austrian Financial Market Authority	Austriacki Urząd ds.. Rynku Finansowego
BE-NBB	Belgia	National Bank of Belgium	Narodowy Bank Belgii
BG-BNB	Bułgaria	Bulgarian National Bank	Bułgarski Bank Narodowy
HR-HNB	Chorwacja	Croatian National Bank	Chorwacki Bank Narodowy
CY-CBC	Cypr	Central Bank of Cyprus	Centralny Bank Cypru
CZ-CNB	Czechy	Czech National Bank	Czeski Bank Narodowy
DK-DFSA	Dania	Danish Financial Supervisory Authority	Duńska Komisja Nadzrou Finansowego
EE-FI	Estonia	Estonia Financial Supervisory Authority	Estońska Komisja Nazdrozu Finansowego
FI-FINFSA	Finlandia	Finnish Financial Supervisory Authority	Fińska Komisja Nadzoru Fianansowego
FR-ACPR	Francja	Prudential Supervisory and Resolution Authority	
DE-BAFIN	Niemcy	Federal Financial Supervisory Authority	Federalna Komisja Nadzoru Finansowego
GR-BOG	Grecja	Bank of Greece	Bank Grecji
HU-CBH	Węgry	Central Bank of Hungary	Centralny Bank Węgier
IS-FME	Islandia	Financial Supervisory Authority	Komisja Nadzoru Finansowego
IE-CBI	Irlandia	Central Bank of Ireland	Centralny Bank Irlandii
IT-BI	Włochy	Bank of Italy	Bank Włoch

LI-FMA	Lichtenstein	Financial Market Authority Liechtenstein	Urząd ds. Rynku Finansowego Liechtenstein
LV-FCMC	Łotwa	Financial and Capital Markets Commission	Komisja Rynków Finansowych i Kapitałowych
LT-BL	Litwa	Bank of Lithuania	Bank Litwy
LU-CSSF	Luksemburg	Commission for the Supervision of Financial Sector	Komisja Nadzoru Sektrora Finansowego
N0-FSA	Norwegia	The Financial Supervisory Authority of Norway	Komisja Nadzoru Finansowego Norwegii
MT-MFSA	Malta	Malta Financial Services Authority	Maltańska Komisja Nadzoru Finansowego
NL-DNB	Holandia	The Netherlands Bank	Bank holenderski
PL-PFSA	Polska	Polish Financial Supervision Authority	Polska Komisja Nadzoru Fiansowego
PT-BP	Portugalia	Bank of Portugal	Bank Portugalii
RO-NBR	Rumunia	National Bank of Romania	Narodowy Bank Ruminii
SK-NBS	Słowacja	National Bank of Slovakia	Narodowy Bank Słowacji
SI-BS	Słowenia	Bank of Slovenia	Bank Słowenii
ES-BE	Hiszpania	Bank of Spain	Bank Hiszpanii
SE-FINA	Szwecja	Swedish Financial Supervisiory Authority	Szwedzka Komisja Nadzoru Finansowego
GB-FCA	Wielka Brytania	Financial Conduct Authority	

Lista członków grupy EBA (European Banking Authority) dot. API zgodnych z PSD2

API initiatives		
Maciej Kostro	Polish API initiative (within Polish Banking Association)	Polska
Chris Michael	Open Banking Implementation Entity	Wielka Brytania
Petr Michalík	Czech API initiative (within Czech Banking Association)	Czechy
Miguel Mauricio	SIBS	Portugalia
Hervé Robache	STET	Francja
Dr Ortwin Scheja	Berlin Group	Europa
Fabio Sorrentino	CBI	Włochy
Miguel Torres	Redsys	Hiszpania
Borica		Bułgaria

Account Servicing Payment Service Providers		
Jordi Belmonte Bexa	Caixbank	Hiszpania
Alain Benedetti	BNP Paribas	Francja
Oliver Bieser	Deutsche Bank	Niemcy
Julie Connor	Bank of Irleand	Irlandia
Julian Dressig	Paypal	Luksemburg
Ville Lauttamus	Nordea	Finlandia
Hetal Popat	HSBC	Wielka Brytania
Manfred Richels	Unicredit	Włochy
Sven Schenkel	ING	Holandia

Third Party Providers (AISPs, PISPs and CBPIIs)		
Roman Bignon	Budget Insight	Francja
Yoann Ciabaud	Linxo	Francja
George Parks Davie	Sofort	Niemcy
Manish Garg	Avinalytics	Wielka Brytania
Lukas Gratte	Trustly	Szwecja
Mark Norman	Truelayer	Wielka Brytania
Jesus Orbegozo	Fintonic	Hiszpania
Tomas Prochazka	Tink	Szwecja
	Numbrs Luxemburg SA	Luksemburg

Other		
Joerg Luedtke	Finanz Informatik	Niemcy (technical service provider)
Pascal Spittler	Ikea	Belgia (payment service user)
James Whittle	Pay.UK	Wielka Brytania (standardisation bodies)

Aktorzy w procesie otwartych API

Aktor	Rola	Opis
ASPSP (Account Servicing Payment Service Provider)	Dostawca	Bank – dostawca usług płatniczych zapewniający i utrzymujący rachunek płatniczy dla płatnika
TPP (Third Party Providers)	Dostawca, Trzecia strona	Trzecia strona, dostawca usług płatniczych. Realizuje płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu (PIS) oraz dostarcza zagregowanej informacji o stanie rachunków bankowych (AIS)
	Dostarczyciel	Banki, firmy, organizacje. Podmiot dostarczający zagregowaną informację o stanie rachunków bankowych – kilku, w różnych bankach – dając łatwy wgląd online w stan wszystkich finansów
API (Application Programming Interface)	Interfejs	Interfejs programistyczny aplikacji. Zestaw reguł, który opisuje w jaki sposób aplikacje i systemy mogą się ze sobą komunikować. Dzięki temu jedna aplikacja może wykorzystywać inną do pozyskiwania informacji lub wykonywania zadań
PSU (Payment Services Users)	Odbiorca	Konsument, klient, płatnik. Odbiorca usług, aktor posiadający dostęp do konta, inicjujący elektroniczne transakcje płatności zdalnych lub wykonujący wszelkie inne działania za pośrednictwem kanałów zdalnych
PISP (Payment Initiation Service Providers)	Inicjator płatności	Uregulowane podmioty, które za zgodą klienta mogą realizować płatności z wykorzystaniem rachunku bankowego klienta w jego imieniu.
EBA (Eropean Banking Authority)	Niezależny organ regulacyjny i nadzorujący	Europejski Urząd Nadzoru Bankowego (EUNB). Organ zapewniający spójność regulacji i nadzór w europejskim sektorze bankowym
CISP (Card Issuing Service Provider)/ PIISP – Payment Instrument Issuing Service Provider	Dostawca usług kartowych	Dostawcy usług kartowych, wydający instrumenty płatnicze (np. Karty) Informuje o dostępności środków na transakcjach płatniczych PSD2 opartych na kartach płatniczych. Dostarczone usługi powiązane można określić jako FCS (potwierdzenie dostępności usługi funduszy).

Regulatory Technical Standards

Sygnatura	Nazwa	Opis
EBA/RTS/2017/10 EBA/ITS/2017/07	Technical Standards on the EBA Register under PSD2	Dokument zawiera opis standardów technicznych oraz wykonawczych, jakie należy spełnić przy prowadzeniu centralnego Rejestru EBA. Zostały tam określone zarówno wymogi dotyczące opracowania, prowadzenia i utrzymania rejestru oraz informacji, jak i same informacje, które mają być w nim zawarte
EBA/RTS/2018/03	RTS on Home-Host cooperation under PSD2	Dokument określa ramy współpracy i wymiany informacji między właściwymi organami państwa państw członkowskich a przyjmujących państw, precyzuje rodzaj informacji i szablony, które instytucje płatnicze mają stosować przy zgłaszaniu właściwym organom przyjmującego państwa członkowskiego sprawozdań z działalności gospodarczej w zakresie płatności prowadzonej na ich terytoriach.
EBA/RTS/2017/09	RTS on central contact points under PSD2	Dokument określa kryteria pozwalające wskazać, kiedy właściwe jest wyznaczenie centralnego punktu kontaktowego na mocy PSD2 oraz jakie funkcje powinny pełnić te punkty kontaktowe.
EBA/RTS/2016/05	RTS on Payment card shemes and processing entities under the IFR (Interchange Fee Regulation)	Dokument wprowadza szczególne wymogi związane z niezależnością systemów kart płatniczych i podmiotów przetwarzających płatności. Dokument został opracowany zgodnie z art. 7 ust. 6 rozporządzenia w sprawie opłat interchange (IFR)
EBA/RTS/2017/02	RTS on SCA and common ans secure communication under PSD2	Dokument zawiera regulacyjne standardy techniczne dotyczące silnego uwierzytelniania klientów i bezpiecznej komunikacji. Dokument ma szczególne znaczenie, ponieważ stanowi klucz do osiągnięcia założeń PSD2, czyli: zwiększenie ochrony konsumentów, promowanie innowacji i poprawa bezpieczeństwa usług płatniczych w całej Unii Europejskiej

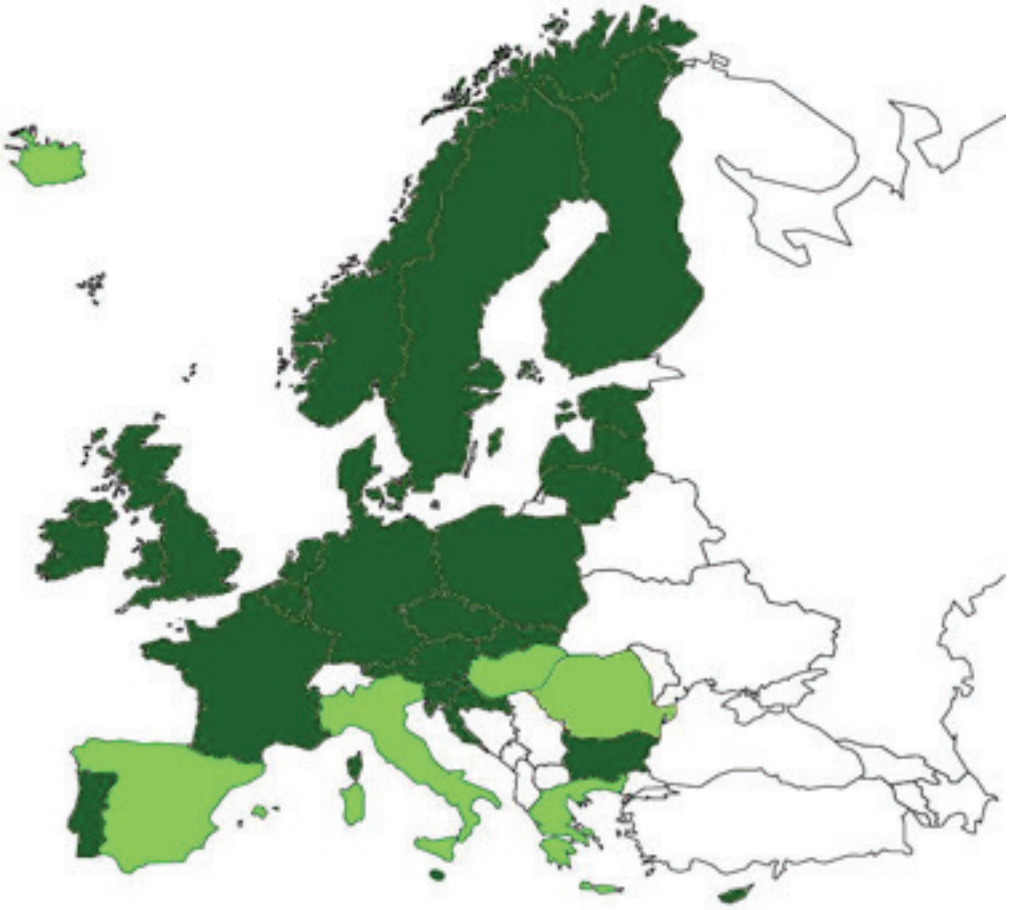
EBA/GL/2017/08	Wytyczne dotyczące kryteriów określania wysokości minimalnej kwoty pieniężnej Ubezpieczenia odpowiedzialności z tytułu prowadzenia działalności zawodowej z tytułu prowadzenia działalności zawodowej lub innej porównywalnej gwarancji zgodnie z art. 5 ust. 4 dyrektywy (UE) 2015/2366	Dokument zawiera wytyczne, które określają kryteriów ustalania warunków minimalnej kwoty pieniężnej ubezpieczenia od odpowiedzialności zawodowej (PII) lub innej porównywalnej gwarancji na usługi inicjowania płatności (PIS) i usługi informacji o rachunku (AIS). Właściwe organy opisane w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk, również jeżeli wytyczne są skierowane przede wszystkim do instytucji.
EBA/GL/2017/09	Wytyczne dotyczące informacji, które należy przedstawić w celu uzyskania zezwo lenia przez instytucje płatnicze i instytucje pieniądza elektronicznego oraz zarejestrowania dostawców świadczących usługi dostępu do informacji o rachunku zgodnie z art. 5 ust. 5 dyrektywy (UE) 2015/2366	Dokument zawiera wytyczne pokazujące stanowisko EBA w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo europejskie w konkretnym obszarze. Właściwe organy opisane w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk, również jeżeli wytyczne są skierowane przede wszystkim do instytucji.
EBA/GL/2017/10	Wytyczne dotyczące zgłaszania poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2)	Wytyczne określają kryteria, progi i metodykę stosowane przez dostawców usług płatniczych w celu ustalenia czy zdarzenie operacyjne lub związane z bezpieczeństwem należy uznać za poważne. Ponadto określa również czy owe zdarzenie należy zgłosić właściwemu organowi w rodzimym państwie członkowskim.
EBA/GL/2017/13	Wytyczne dotyczące procedur składania skarg w związku z możliwymi naruszeniami przepisów drugiej dyrektywy w sprawie usług płatniczych	Dokument określa wytyczne dotyczące procedur składania skarg w związku z możliwymi naruszeniami przepisów PSD2. W dokumencie zawarto informacje określające: sposób składania skarg, treść jaka powinna być zawarta, wytyczne dotyczące odpowiedzi oraz wytyczne dotyczące analizy.
EBA/GL/2017/17	Wytyczne w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych na mocy dyrektywy (UE) 2015/2366 (druga dyrektywa w sprawie usług płatniczych)	Dokument określa wytyczne dotyczące środków bezpieczeństwa określonych ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych w ramach PSD2.
EBA/GL/2018/05	Wytyczne w sprawie wymogów zgłaszania nadużyć finansowych na podstawie art. 96 ust. 6 drugiej dyrektywy w sprawie usług płatniczych (PSD2)	Dokument określa wytyczne wymagane od dostawców usług płatniczych w 28 państwach członkowskich UE gromadzenia i zgłaszania danych o transakcjach płatniczych i fraudach przy użyciu jednolitego języka (określonej metodologii, definicji i podziału danych).

EBA/GL/2018/07	Wytyczne w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389 (w sprawie regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji)	Dokument zawiera wytycznych w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389. Dokument określa w jakich przypadkach można skorzystać z funkcji tzw. fallback-u.

Wytyczne w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych

Zaktualizowana mapa „Wytyczne w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389 (w sprawie regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji)"

Nawiązany został również kontakt z przedstawicielami NCA z Rumuni, jednak nie uzyskaliśmy odpowiedzi przed wskazanym terminem oddania projektu.



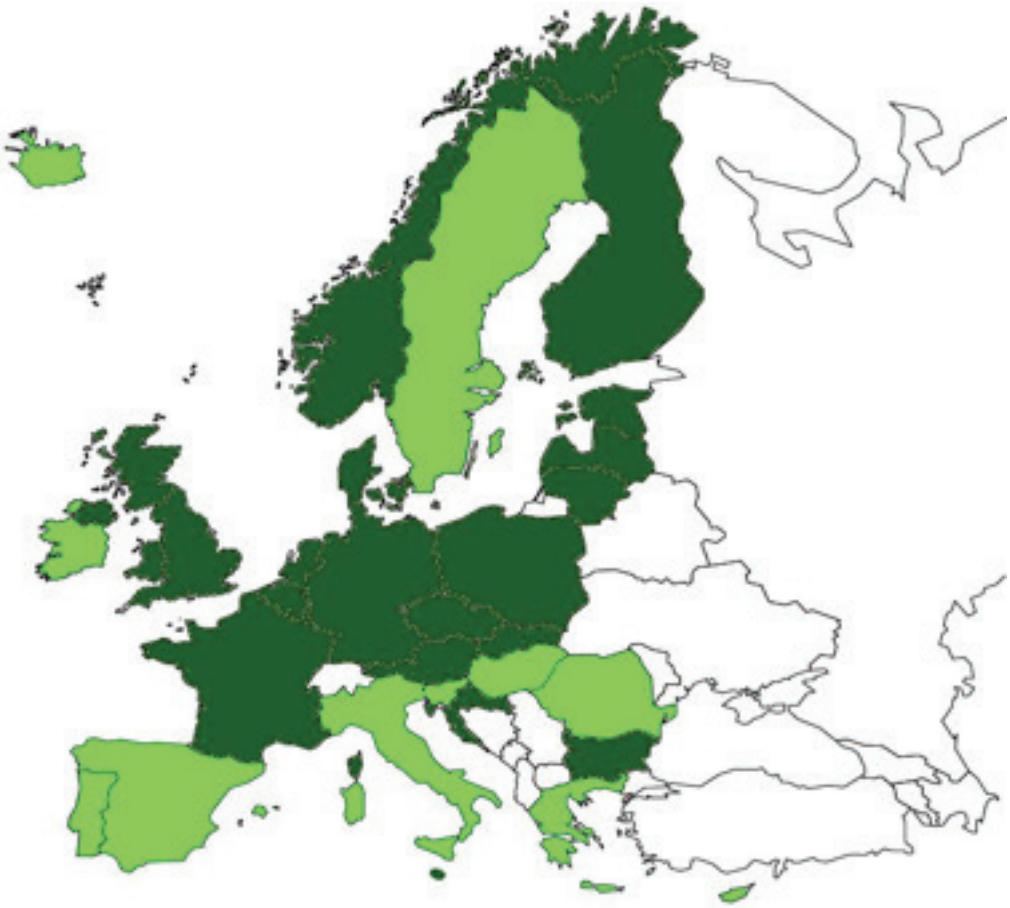
Legenda

przyjęły wytyczne

zobowiązały się do przyjęcia wytycznych

Zaktualizowana mapa „Wytyczne dotyczące informacji, które należy przedstawić w celu uzyskania zezwolenia przez instytucje płatnicze i instytucje pieniądza elektronicznego oraz zarejestrowania dostawców świadczących usługi dostępu do informacji o rachunku zgodnie z art. 5 ust. 5 dyrektywy (UE) 2015/2366”

Nawiązany został również kontakt z przedstawicielami NCA ze Szwecji, Holandii, Luksemburga, Rumuni jednak nie uzyskaliśmy odpowiedzi przed wskazanym terminem oddania projektu.



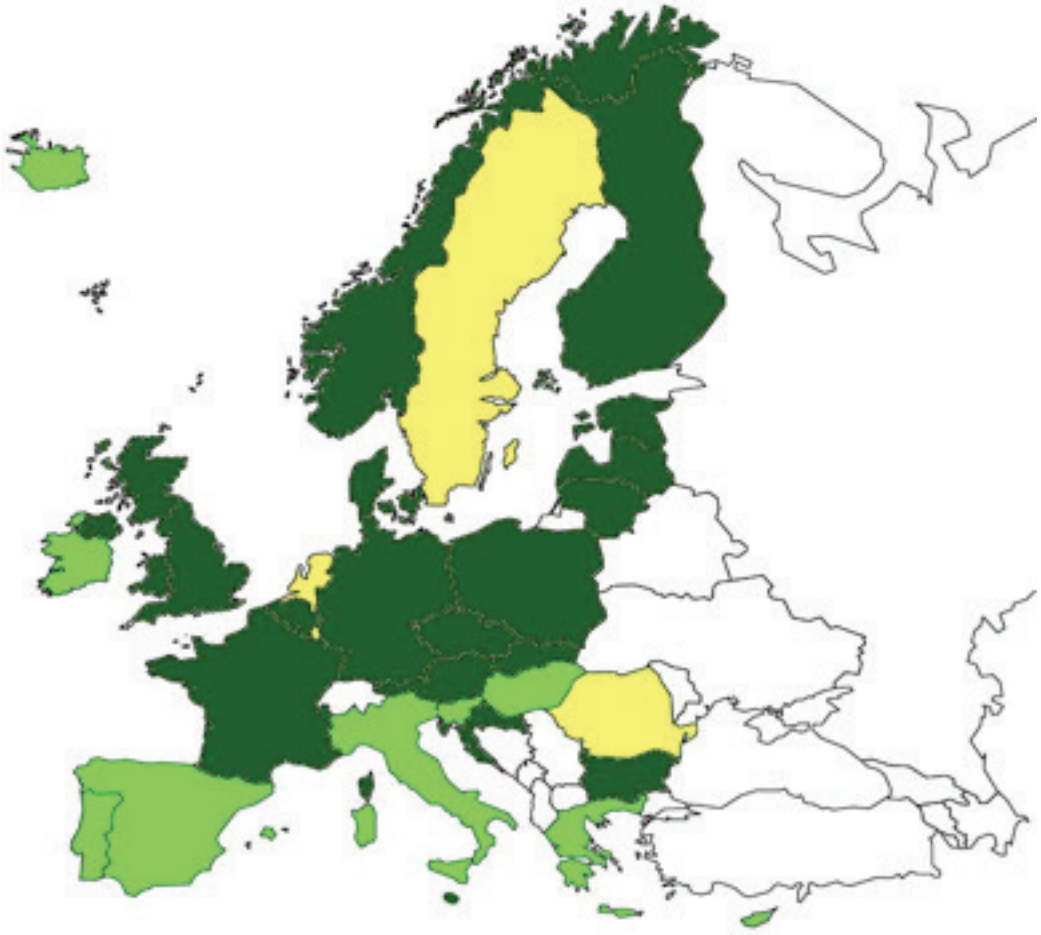
Legenda

przyjęły wytyczne

zobowiązały się do przyjęcia wytycznych

Zaktualizowana mapa „Wytyczne w sprawie warunków skorzystania z wyłączenia z obowiązku ustanowienia mechanizmów awaryjnych zgodnie z art. 33 ust. 6 rozporządzenia (UE) 2018/389 (w sprawie regulacyjnych standardów technicznych (RTS) dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji)"

Nawiązany został również kontakt z przedstawicielami NCA z Rumuni, jednak nie uzyskaliśmy odpowiedzi przed wskazanym terminem oddania projektu.



Legenda

przyjęły wytyczne

zobowiązały się do przyjęcia wytycznych

został nawiązany kontakt