Załącznik do rozporządzenia Rady Ministrów
z dnia 22 sierpnia 2011 r. (poz. 1080)

WZÓR URZĘDOWEGO FORMULARZA ZGŁOSZENIA ZAINTERESOWANIA PRACAMI NAD PROJEKTEM ZAŁOŻEŃ PROJEKTU USTAWY, PROJEKTEM USTAWY LUB PROJEKTEM ROZPORZĄDZENIA

ZGŁOSZENIE
ZAINTERESOWANIA PRACAMI NAD PROJEKTEM - ZGŁOSZENIE ZMIANY DANYCH*

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku

(tytuł projektu założeń projektu ustawy, projektu ustawy lub projektu rozporządzenia - zgodnie z jego treścią udostępnioną w Biuletynie Informacji Publicznej lub informacją zamieszczoną w wykazie prac legislacyjnych Rady Ministrów, Prezesa Rady Ministrów albo ministrów)

A. OZNACZENIE PODMIOTU ZAINTERESOWANEGO PRACAMI NAD PROJEKTEM

1. Nazwa/imię i nazwisko**
Mastercard Europe SA Oddział w Polsce

2. Adres siedziby/adres miejsca zamieszkania**
Plac Europejski 1, 00-844, Warszawa

3. Adres do korespondencji i adres e-mail
krystian.ochecki@mastercard.com

B. WSKAZANIE OSÓB UPRAWNIONYCH DO REPREZENTOWANIA PODMIOTU WYMIENIONEGO W CZĘŚCI A W PRACACH NAD PROJEKTEM

Lp.	Imię i nazwisko	Adres
1	Krystian Ochęcki	
2	Mariusz Łaszczyk	
3		
4		
5		

C. OPIS POSTULOWANEGO ROZWIĄZANIA PRAWNEGO, ZE WSKAZANIEM INTERESU BĘDĄCEGO PRZEDMIOTEM OCHRONY

Uwagi Mastercard Europe S.A. w zakresie postulowanych zmian do ustawy Prawo bankowe (Dz. U. z 2020 r. poz. 1896, z późn. zm.), dotyczących tzw. outsourcingu bankowego.
(szczegółowe stanowisko znajduje się w załączniku do niniejszego formularza)

D. ZAŁĄCZONE DOKUMENTY	
1	Uwagi Mastercard Europe S.A. do projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku (numer z wykazu prac legislacyjnych: UD235)
2	
3	
4	
5	
6	
7	
8	

E. Niniejsze zgłoszenie dotyczy uzupełnienia braków formalnych/zmiany danych**
zgłoszenia dokonanego dnia .....
(podać datę z części F poprzedniego zgłoszenia)

F. OSOBA SKŁADAJĄCA ZGŁOSZENIE

Imię i nazwisko	Data	Podpis
Krystian Ochęcki	10/08/2021	

G. KLAUZULA ODPOWIEDZIALNOŚCI KARNEJ ZA SKŁADANIE FAŁSZYWYCH ZEZNAŃ

Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia
(podpis)

* Jeżeli zgłoszenie nie jest składane w trybie art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, treść: „— Zgłoszenie zmiany danych" skreśla się.
** Niepotrzebne skreślić.

Pouczenie:

1. Jeżeli zgłoszenie ma na celu uwzględnienie zmian zaistniałych po dacie wniesienia urzędowego formularza zgłoszenia (art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa) lub uzupełnienie braków formalnych poprzedniego zgłoszenia (§ 3 rozporządzenia Rady Ministrów z dnia 22 sierpnia 2011 r. w sprawie zgłaszania zainteresowania pracami nad projektami aktów normatywnych oraz projektami założeń projektów ustaw (Dz. U. Nr 181, poz. 1080)), w nowym urzędowym formularzu zgłoszenia należy wypełnić wszystkie rubryki, powtarzając również dane, które zachowały swoją aktualność.
2. Część B formularza wypełnia się w przypadku zgłoszenia dotyczącego jednostki organizacyjnej oraz w sytuacji, gdy osoba fizyczna, która zgłasza zainteresowanie pracami nad projektem założeń projektu ustawy lub projektem aktu normatywnego, nie będzie uczestniczyła osobiście w tych pracach.
3. W części D formularza, stosownie do okoliczności, uwzględnia się dokumenty, o których mowa w art. 7 ust. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, a także pełnomocnictwa do wniesienia zgłoszenia lub do reprezentowania podmiotu w pracach nad projektem aktu normatywnego lub projektu założeń projektu ustawy.
4. Część E formularza wypełnia się w przypadku uzupełnienia braków formalnych lub zmiany danych dotyczących wniesionego zgłoszenia.

Warszawa, 10 sierpnia 2021 r.

Minister Finansów, Funduszy i Polityki Regionalnej

Uwagi Mastercard Europe S.A. do *projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku*
(numer z wykazu prac legislacyjnych: UD235)

Szanowi Państwo,

W związku z pismem Ministra Finansów, Funduszy i Polityki Regionalnej z 20 lipca 2021 r., zawierającym wezwanie do zgłaszania uwag do do *projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku* (numer z wykazu prac legislacyjnych: UD235), poniżej przedstawiamy uwagi Mastercard Europe S.A. w zakresie postulowanych zmian do ustawy Prawo bankowe (Dz. U. z 2020 r. poz. 1896, z późn. zm.), dotyczących tzw. outsourcingu bankowego.

1. Łańcuch poddostawców

Brzmienie przepisu w projekcie ustawy (art. 6a ust. 7a ustawy Prawo bankowe):

"Przedsiębiorca lub przedsiębiorca zagraniczny, któremu powierzono wykonywanie określonych czynności zgodnie z ust. 7 pkt 1, po uzyskaniu pisemnej zgody banku może powierzyć innemu (dalszemu) przedsiębiorcy lub przedsiębiorcy zagranicznemu, w drodze odrębnej umowy, wykonywanie tych czynności, z zachowaniem tajemnicy prawnie chronionej".

Proponowane zmiany:

i. brak ograniczeń co do długości łańcucha poddostawców;

ii. obowiązek powiadomienia banku, przez głównego dostawcę usługi (insourcera), o zaangażowaniu poddostawców, w terminie 30 dni przed ich zaangażowaniem (lub dłuższym, o ile będzie to wymagane ze względu na potrzeby obowiązkowego oszacowania przez bank ryzyka związanego z zaangażowaniem nowych poddostawców). W tym terminie bank będzie mógł się sprzeciwić zaangażowaniu poddostawców, jeżeli poziom ryzyka związany z zaangażowaniem poddostawców będzie zbyt wysoki;

iii. ocena ryzyka dokonywana przez bank powinna uwzględniać długość łańcucha poddostawców insourcera oraz zakres czynności powierzanych poddostawcom;

iv. wynik oceny ryzyka związanego z zaangażowaniem poddostawców powinien być podstawą dopuszczalności zaangażowania poddostawców;

v. w przypadku braku sprzeciwu banku na zaangażowanie poddostawców w terminie, o którym mowa w pkt. ii. powyżej, poddostawca może być zaangażowany w świadczenie usługi (tzw. milcząca zgoda banku na zaangażowanie poddostawców);

vi. zgoda (na poziomie ustawy) na zmianę poddostawcy przez insourcera bez zgody banku, jeżeli jest to uzasadnione okolicznościami (np. brak możliwości korzystania z poprzedniego poddostawcy, na którego bank wyraził zgodę). W takiej sytuacji bank powinien zostać powiadomiony o zmianie poddostawcy niezwłocznie po jego zmianie i powinien mieć prawo do wypowiedzenia umowy outsourcingowej, jeżeli nie akceptuje nowego poddostawcy ze względu na zbyt wysoki poziom ryzyka związany z zaangażowaniem danego poddostawcy.

Proponowane brzmienie zmiany przepisów:

„1) W art. 6a ustawy Prawo bankowe po ust. 7 dodaje się ust. 7a o następującej treści:

7a. Przedsiębiorca lub przedsiębiorca zagraniczny, któremu powierzono wykonywanie określonych czynności zgodnie z ust. 7 pkt 1, może powierzyć innym (dalszym) przedsiębiorcom lub przedsiębiorcom zagranicznym, w drodze odrębnej umowy, wykonywanie określonych w umowie czynności służących realizacji głównego świadczenia wynikającego z tej umowy, z zachowaniem tajemnicy prawnie chronionej. Inni (dalsi) przedsiębiorcy lub przedsiębiorcy zagraniczni, którym powierzono wykonywanie określonych czynności zgodnie ze zdaniem poprzedzającym, mogą powierzać wykonywanie określonych w umowie czynności służących realizacji świadczenia wynikającego z tej umowy kolejnym przedsiębiorcom lub przedsiębiorcom zagranicznym."

Uzasadnienie:

Realia rynkowe wskazują, że w świadczenie usług przez insourcera zaangażowanych jest wiele podmiotów. Złożoność i zaawansowanie technologiczne świadczonych w ramach outsourcingu usług, powoduje, że insourcer nie jest w stanie zapewnić świadczenia usługi bez korzystania z poddostawców. To samo dotyczy poddostawców insourcera. Wydaje się, że obowiązek przeprowadzenia przez bank szacowania ryzyka związanego z powstawaniem długich łańcuchów poddostawców, którego wynik będzie determinował możliwość zaangażowania poddostawcy, jest wystarczające, aby zaadresować ryzyko z tym związane. Tożsame podejście (tj. podejście oparte o ocenę ryzyka) wydaje się wykazywać EBA (patrz pkt 67 Wytycznych EBA w sprawie outsourcingu (EBA/GL/2019/02)).

2. Outsourcing poza EOG

Zmiana wskazana w projekcie (art. 6d ust. 1 ustawy Prawo bankowe):

"Bank zawiadamia Komisję Nadzoru Finansowego o zamiarze zawarcia umowy, o której mowa w art. 6a ust. 1, 7 lub 7a, z przedsiębiorcą zagranicznym niemającym miejsca stałego zamieszkania lub nieposiadającym siedziby na terytorium państwa członkowskiego lub umowy przewidującej, że powierzone czynności będą wykonywane poza terytorium państwa członkowskiego, co najmniej na 30 dni przed jej zawarciem".

Proponowane zmiany:

i. Bank zawiadamia KNF o planowanym outsourcingu czynności poza EOG, na 30 dni przed planowanym powierzeniem czynności;

ii. Bank załącza do zawiadomienia wszystkie dokumenty i informacje istotne dla KNF z perspektywy nadzoru – np. kraj siedziby dostawcy lub kraj, w którym ma być wykonywana usługa lub plan zarządzania ryzykiem itp.;

iii. KNF analizuje zawiadomienie i wydaje milczącą zgodę, tj. jeżeli nie wyrazi sprzeciwu to outsourcing poza EOG może się rozpocząć zgodnie z planem (tj. w dniu wskazanym zawiadomieniu), ale po upływie minimalnego terminu – 30 dni od zawiadomienia. W przepisach powinno być wyraźnie wskazane, że po upływie 30 dni, w przypadku braku sprzeciwu KNF, outsourcing poza EOG może dojść do skutku. Brak sprzeciwu ze strony KNF potwierdza także, że w kraju siedziby dostawcy lub kraju, w którym ma być wykonywana usługa, może wykonywać efektywny nadzór.

Uzasadnienie:

W praktyce bardzo często zdarza się, że w ramach prowadzonej działalności bank korzysta z poddostawców. Często, ze względu na specyfikę usługi albo na konieczność optymalizacji kosztów, dostawca usługi (insourcer) ma siedzibę lub wykonuje usługę, bądź jej część, poza granicami EOG. Sam fakt posiadania przez insourcera siedziby lub wykonywania usługi poza granicami EOG, niekoniecznie związany jest z podwyższonym ryzykiem dla banku. W związku z powyższym, wydaje się, że bezcelowe jest każdorazowe wypowiadanie się KNF w kwestii danego poddostawcy, a wystarczające jest, przy założeniu braku zastrzeżeń KNF do poddostawcy, wydanie tzw. milczącej zgody.

Ponadto, wątpliwości budzi treść zaproponowanego brzmienia nowego art. 6d ust. 2 ustawy Prawo bankowe, który mówi, że umowa outsourcingowa nie może zostać zawarta, jeżeli w państwie, w którym powierzone czynności mają być wykonywane, obowiązujące prawo, uniemożliwia Komisji Nadzoru Finansowego wykonywanie efektywnego nadzoru. Ustawodawca nie wskazuje jednak w projekcie kto i na jakich zasadach powinien się w tym zakresie wypowiedzieć. W związku z tym, wydaje się, że tzw. milcząca zgoda KNF na outsourcing poza EOG jest tym bardziej zasadna. Jeżeli KNF uzna, że efektywny nadzór nie jest możliwy, to powinna zgłosić sprzeciw w tym zakresie.

3. Odpowiedzialność insourcera i poddostawców

Zmiana wskazana w projekcie (art. 6b ust. 1 ustawy Prawo bankowe):

„Odpowiedzialności przedsiębiorcy lub przedsiębiorcy zagranicznego, o którym mowa w art. 6a ust. 1, wobec banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy, o której mowa w art. 6a ust. 1, 7 i 7a, nie można wyłączyć ani ograniczyć".

Proponowane zmiany:

i. wprowadzenie do ustawy Prawo bankowe definicji „outsourcingu funkcji krytycznych" na wzór Wytycznych EBA w sprawie outsourcingu (EBA/GL/2019/02);

ii. utrzymanie zakazu ograniczenia lub wyłączania odpowiedzialności insourcera lub jego poddostawców, o którym mowa w art. 6b ust. 1 ustawy Prawo bankowe, ale tylko w przypadku outsourcingu funkcji krytycznych;

iii. wprowadzenie obowiązku posiadania ubezpieczenia odpowiedzialności cywilnej przez insourcera z tytułu szkody wyrządzonej klientom banku;

albo

i. wskazanie w ustawie Prawo bankowe, domyślnej zasady ponoszenia przez insourcera odpowiedzialności wobec banku za szkody wyrządzone przez insourcera lub przez jego poddostawców klientom banku;

ii. wskazanie, że insourcer jest podmiotem odpowiedzialnym za sprawdzenie swoich poddostawców, a także, że jest punktem kontaktowym dla KNF w sprawie swoich poddostawców, tj. na życzenie KNF kontroluje działalność swoich poddostawców pod kątem zgodności z prawem; Bank oraz KNF powinny realizować efektywny nadzór przez i z wykorzystaniem insourcera, który biorąc odpowiedzialność za swoich poddostawców powinien zapewnić zgodność ich działalności z odnośnymi wymaganiami prawa oraz wytycznymi nadzoru i wymogami samego banku (także w zakresie przedstawiania stosownych informacji i dokumentów za pośrednictwem insourcera);

iii. utrzymanie zakazu wyłączania lub ograniczania odpowiedzialności insourcera za szkody wyrządzone klientom banku;

iv. wprowadzenie obowiązku posiadania ubezpieczenia odpowiedzialności cywilnej przez insourcera z tytułu szkody wyrządzonej klientom banku.

Uzasadnienie:

Doświadczenie wskazuje, że banki korzystają z insourcerów, którzy posiadają siedziby poza Polską. Ze względu na odmienność przepisów obowiązujących w innych krajach, dotyczących zakazu ograniczania odpowiedzialności poddostawców insourcera wobec banku za szkody wyrządzone klientom banku, poddostawcy nie są chętni do zawierania umów outsourcingowych z polskimi bankami lub proces zawarcia takiej umowy znacząco się przedłuża. Często w ramach podoutsourcingu delegowane są mało znaczące czynności, nie wiążące się z możliwością wygenerowania dla banku i jego klientów dużej szkody. Zatem utrzymanie zakazu wyłączania lub

ograniczania odpowiedzialności poddostawców tylko w przypadku tzw. outsourcingu funkcji krytycznych wydaje się zasadne. Natomiast, wprowadzenie domyślnej zasady odpowiedzialności insourcera za szkody wyrządzone przez jego poddostawców, pozwoli na wyeliminowanie problemów związanych z odmiennością przepisów dotyczących odpowiedzialności poddostawców insourcera w innych krajach, przy jednoczesnym braku uszczerbku dla interesów banku i jego klientów – za wyrządzoną szkodę odpowiedzialność będzie ponosił insourcer. Ponadto, w praktyce, mogą być problemy z ustaleniem podmiotu odpowiedzialnego za szkodę, co tym bardziej przemawia za domyślną odpowiedzialnością insourcera za szkody wyrządzone przez jego poddostawców. Należy również zaznaczyć, że ze względu na odpowiedzialność insourcera za swoich poddostawców, wydaje się, że poddostawcy insourcera będą należycie sprawdzani, a insourcer będzie wykonywał żądania KNF w zakresie przekazania dokumentów i informacji o działalności jego poddostawców.

4. Outsourcing a uwierzytelnienie z wykorzystaniem technologii podmiotu trzeciego

Proponowane zmiany:

i. Wyłączenie stosowania reżimu outsourcingu bankowego i outsourcingu płatniczego (tj. powierzenia czynności operacyjnych przez krajową instytucję płatniczą lub krajową instytucję pieniądza elektronicznego) w przypadku, gdy bank, krajowa instytucja płatnicza lub krajowa instytucja pieniądza elektronicznego korzysta z technologii podmiotu trzeciego (np. czytnik odcisku palca w urządzeniu mobilnym), rozwiązania technologicznego podmiotu trzeciego lub urządzenia uwierzytelniającego podmiotu trzeciego na potrzeby uwierzytelnienia użytkownika.

ii. Bank, krajowa instytucja płatnicza lub krajowa instytucja pieniądza elektronicznego będą akceptować uwierzytelnienie użytkownika przeprowadzone z wykorzystaniem technologii podmiotu trzeciego, rozwiązania technologicznego podmiotu trzeciego lub urządzenia uwierzytelniającego podmiotu trzeciego na podstawie zawartej z takim podmiotem umowy lub na podstawie umowy z użytkownikiem.

iii. W każdym przypadku podmiot trzeci będący dostawcą technologii lub urządzeń będzie zobowiązany na podstawie ustawy przestrzegać wymogów w zakresie bezpieczeństwa i uwierzytelnienia wynikających z Rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego 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.

iv. Całkowitą odpowiedzialność wobec użytkownika w przypadku skorzystania z takich rozwiązań będzie ponosić odpowiednio bank, krajowa instytucja płatnicza lub krajowa instytucja pieniądza elektronicznego.

Proponowane brzmienie zmiany przepisów:

„1) W art. 6a ustawy Prawo bankowe po ust 2 dodaje się ust. 2a – 2e o następującej treści:

2a. Zawarcie przez bank umowy, na podstawie której bank akceptuje uwierzytelnienie użytkownika w rozumieniu art. 32i ust. 1 ustawy o usługach płatniczych, poprzez urządzenie, oprogramowanie lub rozwiązanie teleinformatyczne dostarczane przez innego przedsiębiorcę lub przedsiębiorcę zagranicznego, nie stanowi umowy, o której mowa w art. 6a – 6d, pod warunkiem, że przed zawarciem przez bank umowy, o której mowa w ust. 1, procedury bezpieczeństwa i uwierzytelniania użytkownika stosowane przez przedsiębiorcę lub przedsiębiorcę zagranicznego zostały udokumentowane, zbadane oraz poddane ocenie audytora, o którym mowa w art. 3 ust. 1 i 2 Rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym 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, oraz w okresie trwania umowy są okresowo badane i poddawane ocenie tego audytora.

2b. Przedsiębiorca lub przedsiębiorca zagraniczny zawierający z bankiem umowę, o której mowa w ust. 2a, przestrzega wymogów w zakresie bezpieczeństwa i uwierzytelnienia wskazanych w Rozporządzeniu delegowanym Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym 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.

2c. W przypadku zawarcia umowy, o której mowa w ust. 2a, przedsiębiorca lub przedsiębiorca zagraniczny ponosi odpowiedzialność wobec banku oraz wobec klientów za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy, o której mowa w ust. 2a. Odpowiedzialności, o której mowa w zdaniu poprzedzającym, nie można wyłączyć ani ograniczyć.

2d. Zawarcie przez bank umowy, o której mowa w ust. 2a, nie zwalnia banku z obowiązku przestrzegania wymogów ustawy, w tym w szczególności art. 32i ustawy o usługach płatniczych.

2e. Przepisy ust. 2a – 2d stosuje się odpowiednio w sytuacji, gdy bank, na podstawie umowy zawartej z użytkownikiem, akceptuje uwierzytelnienie użytkownika przeprowadzone z zastosowaniem urządzenia, oprogramowania lub rozwiązania teleinformatycznego dostarczanego przez innego przedsiębiorcę lub przedsiębiorcę zagranicznego.

2) W art. 86 ustawy o usługach płatniczych po ust. 4 dodaje się ust. 4a – 4e o następującej treści:

4a. Zawarcie przez krajową instytucję płatniczą umowy, na podstawie której krajowa instytucja płatnicza akceptuje uwierzytelnienie użytkownika w rozumieniu art. 32i ust. 1 ustawy o usługach płatniczych, poprzez urządzenie, oprogramowanie lub rozwiązanie teleinformatyczne dostarczane przez innego przedsiębiorcę lub przedsiębiorcę zagranicznego, nie stanowi umowy, o której mowa w ust. 1 – 3, pod warunkiem, że przed zawarciem przez krajową instytucję płatniczą umowy, o której mowa w ust. 1 - 3, procedury bezpieczeństwa i uwierzytelniania użytkownika stosowane przez przedsiębiorcę lub przedsiębiorcę zagranicznego zostały udokumentowane, zbadane oraz poddane ocenie audytora, o którym mowa w art. 3 ust. 1 i 2 Rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym 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, oraz w okresie trwania umowy są okresowo badane i poddawane ocenie tego audytora.

4b. Przedsiębiorca lub przedsiębiorca zagraniczny zawierający z krajową instytucją płatniczą umowę, o której mowa w ust. 4a, przestrzega wymogów w zakresie bezpieczeństwa i uwierzytelnienia wskazanych w Rozporządzeniu delegowanym Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym 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.

4c. W przypadku zawarcia umowy, o której mowa w ust. 4a, przedsiębiorca lub przedsiębiorca zagraniczny ponosi odpowiedzialność wobec krajowej instytucji płatniczej oraz wobec użytkowników za szkody wyrządzone użytkownikom wskutek niewykonania lub nienależytego wykonania umowy, o której mowa w ust. 4a. Odpowiedzialności, o której mowa w zdaniu poprzedzającym, nie można wyłączyć ani ograniczyć.

4d. Zawarcie przez krajową instytucję płatniczą umowy, o której mowa w ust. 4a, nie zwalnia krajowej instytucji płatniczej z obowiązku przestrzegania wymogów ustawy, w tym w szczególności art. 32i.

4e. Przepisy ust. 4a – 4d stosuje się odpowiednio w sytuacji, gdy krajowa instytucja płatnicza, na podstawie umowy zawartej z użytkownikiem, akceptuje uwierzytelnienie użytkownika przeprowadzone z zastosowaniem urządzenia, oprogramowania lub rozwiązania teleinformatycznego dostarczanego przez innego przedsiębiorcę lub przedsiębiorcę zagranicznego."

Uzasadnienie:

W obecnym stanie prawnym wykorzystanie przez bank, krajową instytucję płatniczą lub krajową instytucję pieniądza elektronicznego technologii podmiotu trzeciego na potrzeby uwierzytelniania użytkownika tego banku, krajowej instytucji płatniczej lub krajowej instytucji pieniądza elektronicznego może być potencjalnie potraktowane jako tzw. outsourcing bankowy, czyli powierzenie przez bank czynności przedsiębiorcy lub przedsiębiorcy zagranicznemu na podstawie umowy, o której mowa w art. 6a – 6d ustawy Prawo bankowe lub tzw. outsourcing płatniczy, czyli powierzenie przez krajową instytucję płatniczą innemu przedsiębiorcy wykonywania określonych czynności operacyjnych związanych ze świadczeniem usług płatniczych na podstawie umowy, o której mowa w art. 86 ust. 1 ustawy o usługach płatniczych (odpowiednio powierzenie przez krajową instytucję pieniądza elektronicznego, na podstawie umowy o której mowa w art. 132v ustawy o usługach płatniczych).

Jednakże korzystanie przez bank, krajową instytucję płatniczą lub krajową instytucję pieniądza elektronicznego z urządzenia, oprogramowania lub rozwiązania teleinformatycznego dostarczanego przez innego przedsiębiorcę lub przedsiębiorcę zagranicznego nie powinno być traktowane jako outsourcing. Tzw. outsourcing bankowy oraz outsourcing płatniczy oznacza powierzenie przez bank lub odpowiednio krajową instytucję płatniczą/krajową instytucję pieniądza elektronicznego określonych czynności faktycznych związanych z działalnością bankową (art. 6a ust. 1 pkt 2 ustawy Prawo bankowe; outsourcing bankowy może także obejmować powierzenie przez

bank innemu przedsiębiorcy wykonywania pośrednictwa w zakresie czynności bankowych) lub czynności operacyjnych związanych ze świadczeniem usług płatniczych lub z działalnością w zakresie wydawania pieniądza elektronicznego (art. 86 ust. 1 ustawy o usługach płatniczych). Kluczową kwestią pozwalającą uznać dane uzgodnienie za outsourcing bankowy lub outsourcing płatniczy jest to, że w przypadku outsourcingu to bank lub krajowa instytucja płatnicza (krajowa instytucja pieniądza elektronicznego) powierza wykonywanie określonych czynności innemu przedsiębiorcy. Natomiast w przypadku wykorzystania przez bank, krajową instytucję płatniczą lub krajową instytucję pieniądza elektronicznego technologii lub urządzenia dostarczanego przez podmiot trzeci na potrzeby uwierzytelniania użytkownika nie ma miejsca żadne „powierzenie" czynności. W przypadku wykorzystywania takich technologii lub urządzeń na potrzeby uwierzytelnienia, czynność uwierzytelnienia użytkownika jest przeprowadzana przez sam bank lub krajową instytucję płatniczą (krajową instytucję pieniądza elektronicznego) i to ten podmiot, nie dostawca technologii czy urządzenia, podejmuje decyzję o uwierzytelnieniu użytkownika lub odmowie uwierzytelnienia. Zewnętrzny dostawca dostarcza jedynie rozwiązanie techniczne lub urządzenie umożliwiające przeprowadzenie tego uwierzytelnienia.

Wykorzystanie przez bank, krajową instytucję płatniczą lub krajową instytucję pieniądza elektronicznego technologii podmiotu trzeciego na potrzeby uwierzytelniania użytkownika tego banku, krajowej instytucji płatniczej lub krajowej instytucji pieniądza elektronicznego nie stanowi także outsourcingu w rozumieniu Wytycznych EBA w sprawie outsourcingu (EBA/GL/2019/02). Zgodnie z tymi Wytycznymi, w celu uznania danej usługi za outsourcing, konieczne jest spełnienie następujących wymogów: (i) usługa jest świadczona na rzecz banku lub instytucji płatniczej, (ii) usługa jest świadczona cyklicznie lub w sposób stały, a także (iii) usługa ta stanowi czynność, która mogłaby zostać wykonana przez sam bank lub instytucję płatniczą. Żaden z tych wymogów nie jest spełniony w odniesieniu do uwierzytelnienia na podstawie technologii podmiotu trzeciego: (i) technologia podmiotu trzeciego jest bowiem dostarczana użytkownikowi, nie bankowi lub instytucji płatniczej, (ii) nie ma charakteru stałego – uwierzytelnienie z wykorzystaniem tej technologii jest przeprowadzane okazjonalnie, obok innych metod uwierzytelnienia wykorzystywanych przez bank lub instytucję płatniczą, a ponadto (iii) bank ani instytucja płatnicza nie mógłby uwierzytelniać użytkowników z wykorzystaniem takiej technologii – nie dostarcza bowiem użytkownikom urządzeń ani technologii to umożliwiających.

Możliwość traktowania technologii dostarczanych bankom i instytucjom płatniczych za czynność niestanowiącą outsourcingu została dopuszczona przez Europejski Urząd Nadzoru Bankowego w ramach odpowiedzi na jedno z pytań zawartych w ramach narzędzia Single Rulebook (https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4047), w którym korzystanie przez bank z technologii podmiotu trzeciego jest wskazywane jako rozwiązanie alternatywne wobec outsourcingu. Oznacza to, że wymogi w zakresie bezpieczeństwa nałożone przez Dyrektywę 2015/2366 (dyrektywa PSD2) oraz przez 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, nie stoją na przeszkodzie możliwości korzystania przez dostawcę usług płatniczych z technologii podmiotu trzeciego. Co więcej, korzystanie z takiej technologii jest możliwe poza reżimem outsourcingowym.

Ponadto proponowana zmiana umożliwia dostawcom usług płatniczych korzystanie z zewnętrznych narzędzi uwierzytelniających na potrzeby uwierzytelnienia użytkowników w rozumieniu art. 32i ustawy o usługach płatniczych, w tym narzędzi uwierzytelniających umożliwiających uwierzytelnienie u wielu dostawców.

Wreszcie, delegacja uwierzytelniania użytkownika banku, krajowej instytucji płatniczą lub krajowej instytucji pieniądza elektronicznego będzie możliwa tylko w przypadku, gdy zewnętrzny dostawca technologii lub urządzenia zapewnienia zgodność z wymogami bezpieczeństwa wskazanymi w art. 8-9 Rozporządzenia delegowanego Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającego 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. Wymogi te nie są relewantne z punktu widzenia celu Wytycznych EBA w sprawie outsourcingu (EBA/GL/2019/02). Wprowadzenie ustawowego obowiązku przestrzegania tych wymogów przez dostawców technologicznych zapewni bezpieczeństwo korzystania przez użytkowników z dostarczanych przez nich rozwiązań i ograniczy po stronie banków i krajowych instytucji płatniczych (krajowych instytucji pieniądza elektronicznego) ryzyko wynikające z zaufania rozwiązaniom dostarczanym przez dostawców technologicznych w procesie uwierzytelnienia użytkowników.

5. Korzystanie przez banki z usług podmiotów trzecich a tajemnica bankowa

Proponowane zmiany:

i. Proponuje się, aby w przypadku korzystania przez bank z rozwiązań technologicznych oferowanych przez podmioty trzecie poza reżimem outsourcingu bankowego dopuszczalne było przekazywanie przez bank takim podmiotom trzecim informacji objętych tajemnicą bankową, bez konieczności uzyskiwania upoważnienia osoby, której informacje te dotyczą na ich ujawnienie, to jest upoważnienia, o którym mowa w art. 104 ust. 3 ustawy Prawo bankowe. Proponowana zmiana zakłada rozszerzenie katalogu podmiotów, o których mowa w art. 104 ust. 2 ustawy Prawo bankowe.

ii. W takim przypadku wystarczające powinno być zawiadomienie przez bank osoby, której przekazywane dane dotyczą, o ich przekazaniu podmiotowi trzeciemu.

iii. Przekazywanie tych danych przez bank podmiotowi trzeciemu oraz zasady ich przetwarzania przez podmiot trzeci byłoby objęte wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Uzasadnienie:

Reżim tajemnicy bankowej, jaki wynika z przepisów ustawy Prawo bankowe, nie jest powszechnie stosowany w państwach członkowskich Unii Europejskiej. W państwach takich jak Niemcy, Włochy, Belgia i Holandia brak jest szczególnego reżimu tajemnicy bankowej, przy czym przetwarzanie, przekazywanie takich danych przez banki podlega ogólnym przepisom dotyczącym informacji

poufnych i przetwarzania danych osobowych, w tym w szczególności przepisom Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Proponowana zmiana nie obejmuje tak daleko idącej zmiany jak całkowite zrezygnowanie z objęcia szczególną ochroną wszystkich informacji dotyczących czynności bankowej, uzyskanych w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje. Zmiana ta sprowadza się jednak do wyłączenia stosowania reżimu ujawniania tajemnicy bankowej do informacji, które bank przekazuje innemu przedsiębiorcy lub przedsiębiorcy zagranicznemu, który świadczy na rzecz banku lub banku i klienta usługę, do której nie mają zastosowania przepisy art. 6a – 6d ustawy Prawo bankowe.

Odbiorca takich informacji byłby zobowiązany do ich przetwarzania zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, tj. z zachowaniem ich poufności i bezpieczeństwa.

Natomiast obecny stan prawny stanowi przeszkodę dla banków zamierzających korzystać z usług oferowanych przez zewnętrznych dostawców, w tym na przykład dostawców świadczących usługi wspierające dla banku w zakresie monitoringu transakcji czy analizy transakcji w celu wykrywania transakcji oszukańczych czy transakcji podejrzanych. Aktualnie, bank w celu skorzystania z takich rozwiązań zobowiązany jest uzyskać od wszystkich klientów upoważnienie do ujawnienia dostawcy takiego rozwiązania danych objętych tajemnicą bankową na podstawie art. 104 ust. 3 ustawy Prawo bankowe lub uznać taką usługę za usługę outsourcingu bankowego w rozumieniu art. 6a – 6d ustawy Prawo bankowe, także w sytuacji gdy bank nie powierza dostawcy zewnętrznemu swoich zadań w zakresie monitoringu transakcji, lecz jedynie rozwiązanie oferowane przez dostawcę stanowi narzędzie wspierające czynności faktyczne wykonywane przez sam bank. Proponowana zmiana zmierza więc do przeciwdziałania praktyce sztucznego uznawania tego typu usług za outsourcing bankowy jedynie w celu umożliwienia bankowi przekazywania dostawcom usług informacji objętych tajemnicą bankową bez konieczności uzyskiwania upoważnienia.