Deloitte.

Deloitte | Legal

Newsletter prawny

Wydawany przez zespół Finansów i Bankowości Kancelarii Prawniczej Deloitte Legal

Grudzień 2015 r.

Spis treści

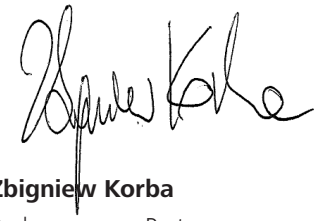
Szanowni Państwo,

Przedstawiam Państwu kolejny numer Newslettera przygotowanego przez prawników kancelarii prawniczej Deloitte Legal dla klientów z sektora finansowego.

Na początku przedstawiamy Państwu informacje na temat dyrektywy PAD (Payment Accounts Directive), której termin implementacji upływa 18 września 2016 r. Następnie mogą Państwo przeczytać artykuł na temat decyzji Generalnego Inspektora Ochrony Danych Osobowych z lutego 2015 r. na temat przetwarzania danych osobowych klienta po spłacie zadłużenia. Kolejno omawiamy wymogi techniczne i handlowe, jakie ustaliła Unia Europejska w odniesieniu do transakcji kartowych. W niniejszym numerze Newslettera będą mogli Państwo zapoznać się także z informacją na temat rekomendacji Komisji Nadzoru Finansowego dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie. Rekomendacja jest kierowana do banków, krajowych instytucji płatniczych, krajowych instytucji pieniądza elektronicznego oraz SKOK-ów. Na końcu przybliżamy wyrok Naczelnego Sądu Administracyjnego, dotyczący wykorzystania akcji wirtualnych w programach motywacyjnych dla pracowników, opartych o instrumenty pochodne.

Mamy nadzieję, że publikacja będzie pomocna w Państwa codziennej pracy.

Zapraszamy do lektury.



Zbigniew Korba
Radca prawny, Partner
Lider zespołu ds. Finansów i Bankowości
Kancelaria prawnicza Deloitte Legal

Dyrektywa PAD

Upowszechnienie obrotu bezgotówkowego na terenie Unii Europejskiej, a także zniesienie w tym zakresie barier rynkowych poprzez wprowadzenie instytucji podstawowego rachunku płatniczego oraz mechanizmów zwiększających świadomość i aktywność konsumentów w zakresie korzystania z usług płatniczych – to główne cele dyrektywy PAD (*Payment Accounts Directive*)[1].

Wprawdzie termin implementacji PAD upływa dopiero w dniu 18 września 2016 r., jednak już teraz prowadzone są przez dostawców usług płatniczych analizy wpływu dyrektywy na ich biznes, a co za tym idzie – projektowane konkretne rozwiązania.

Podstawowymi celami dyrektywy jest zapewnienie:

1) **transparentności i porównywalności opłat pobieranych od konsumentów w odniesieniu do ich rachunków płatniczych** prowadzonych na terytorium Unii Europejskiej; zmiany w tym zakresie mają za zadanie zwiększyć świadomość konsumentów na temat opłat pobieranych od nich przez dostawców rachunków płatniczych, co ułatwi konsumentom porównywanie ofert i przyczyni się do zwiększenia konkurencyjności rynku;
2) **możliwości przenoszenia rachunków płatniczych w obrębie państwa członkowskiego** oraz zasad ułatwiania konsumentom otwierania rachunków płatniczych za granicą, w tym poprzez ustanowienie minimalnych standardów dla takich rachunków;
3) **powszechnego dostępu konsumentów do podstawowego rachunku płatniczego** w celu zapewnienia, aby każdy konsument przebywający legalnie w Unii Europejskiej posiadał tani lub bezpłatny dostęp do podstawowych usług bankowych.

<u>Kogo dotyczy dyrektywa?</u>

Obowiązki wynikające z PAD odnoszące się do **transparentności i porównywalności opłat** (pkt 1 powyżej) oraz **przenoszenia rachunków płatniczych** (pkt 2 powyżej) obejmują wszystkich dostawców usług płatniczych w rozumieniu dyrektywy PSD[2].

Natomiast przepisy PAD odnoszące się do **dostępu konsumentów do podstawowego rachunku płatniczego oraz wprowadzające obowiązek tworzenia i prowadzenia takich rachunków** (pkt 3 powyżej) dotyczą jedynie instytucji kredytowych[3].

Ponadto, każde państwo członkowskie będzie musiało zdecydować czy ww. przepisy dotyczące podstawowego rachunku płatniczego będą dotyczyły wszystkich, czy też tylko części instytucji kredytowych[4].

<u>Zakres produktowy PAD</u>

PAD obejmuje swoim zakresem wszystkie rachunki płatnicze o określonej w dyrektywie funkcjonalności – tj. rachunki płatnicze pozwalające na umieszczanie środków pieniężnych, wypłacanie gotówki oraz zlecanie i otrzymywanie transakcji płatniczych wobec stron trzecich i od nich, w tym realizowanie przelewów bankowych.

Natomiast z zakresu obowiązywania PAD wyłączone będą rachunki, które mają bardziej ograniczone funkcje – np. rachunki oszczędnościowe, rachunki powiązane z kartami kredytowymi, gdzie środki finansowe wpłacane są z reguły jedynie w celu spłaty zadłużenia z karty kredytowej, rachunki służące wyłącznie do spłaty kredytu hipotecznego (ang. *current account mortgages*) lub rachunki obsługujące pieniądz elektroniczny. Jednakże, gdy takie rachunki będą wykorzystywane do bieżących transakcji płatniczych i będą obejmować wszystkie wyżej wymienione funkcje, podlegać będą pod PAD[5].

Beneficjenci dyrektywy

Dyrektywa zasadniczo wskazuje jedynie konsumentów jako osoby uprawnione do korzystania z przyjętych w dyrektywie rozwiązań. W zakresie przepisów dotyczących **transparentności i porównywalności opłat** oraz **przenoszenia rachunków płatniczych** zyskają konsumenci, którzy posiadają już rachunki płatnicze i rozważają ich przeniesienie lub otwarcie nowych. Natomiast przepisy dotyczące **dostępu do podstawowego rachunku płatniczego** mają na celu zapewnienie dostępu do podstawowych usług bankowych na terenie całej Unii wszystkim konsumentom legalnie w niej przebywającym, niezależnie od obywatelstwa i miejsca zamieszkania.

Implementacja PAD w Polsce

Na stronie Rządowego Centrum Legislacji jest już dostępny projekt ustawy o zmianie ustawy o usługach płatniczych oraz o nadzorze nad rynkiem finansowym[6], implementujący postanowienia PAD do prawa polskiego. Należy jednak podkreślić, że projekt został przygotowany przez Rząd poprzedniej kadencji i jego finalne brzmienie może ulec zmianom w trakcie dalszych prac legislacyjnych.

[1] Dyrektywa Parlamentu Europejskiego i Rady 2014/92/UE z dnia 23 lipca 2014 r. w sprawie porównywalności opłat związanych z rachunkami płatniczymi, przenoszenia rachunku płatniczego oraz dostępu do podstawowego rachunku płatniczego (ang. Payment Accounts Directive).

[2] Dyrektywa 2007/64/WE Parlamentu Europejskiego I Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Dz. U. UE. L 319 z dnia 5 grudnia 2007 r. str. 1).

[3] w znaczeniu art. 4 ust. pkt 1 Rozporządzenia CRR tj. rozporządzenia Parlamentu Europejskiego i Rady nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz. U. UE. L 176 z dnia 27 czerwca 2013 r. str. 1).

[4] Z analizy dotychczasowego projektu polskiej ustawy implementującej PAD, o którym mowa w dalszej części opracowania, wynika, że w Polsce obowiązek prowadzenia podstawowego rachunku płatniczego będzie spoczywał na wszystkich instytucjach kredytowych (włączając SKOKi), a niewypełnienie tego obowiązku będzie podlegało karze pieniężnej do 1.000.000 zł.

[5] Warto w tym miejscu wskazać również opcję narodową zawartą w art. 1 ust. 6 PAD, na podstawie której państwa członkowskie mogą podjąć decyzję o stosowaniu wszystkich lub niektórych przepisów dyrektywy PAD również do rachunków płatniczych innych niż rachunki o wskazanej podstawowej funkcjonalności.

[6] http://legislacja.rcl.gov.pl/projekt/12275502.

Podejście polskiego ustawodawcy

Wspomniany powyżej projekt polskiej ustawy zakłada, zgodnie z postanowieniami dyrektywy PAD, szereg nowych obowiązków spoczywających na instytucjach kredytowych i innych instytucjach płatniczych. Należą do nich m.in.:

- nowe obowiązki informacyjne względem konsumenta, w tym przesyłanie i udostępnianie konsumentowi dokumentu dotyczącego opłat, słowniczka terminów oraz co najmniej raz w roku zestawienia opłat pobranych w związku z prowadzeniem rachunku,
- obowiązek świadczenia usługi przeniesienia rachunku płatniczego, oraz
- obowiązek oferowania i prowadzenia przez instytucje kredytowe podstawowego rachunku płatniczego.

Zgodnie z dotychczasowym projektem ustawy implementującej PAD, instytucje kredytowe będą zobowiązane prowadzić podstawowe rachunki płatnicze nieodpłatnie (wymóg ten nie dotyczy jednak opłat z tytułu użytkowania karty płatniczej). Projekt ustawy zakłada również, że opłaty za wykonywanie usługi polecenia przelewu oraz opłaty za przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki będą mogły być pobierane od posiadacza podstawowego rachunku płatniczego dopiero po przekroczeniu 10 transakcji wykonanych w ciągu miesiąca.

Bank nie zawsze będzie uprawniony do przetwarzania danych osobowych klienta po spłacie zadłużenia

Banki są uprawnione do przetwarzania danych osobowych klientów, którzy spłacili swoje zobowiązania w celu oceny ich zdolności kredytowej oraz analizy ryzyka kredytowego - gdy klienci ci nie wykonywali zobowiązań lub dopuścili się zwłoki w ich wykonaniu - również bez zgody klienta. Jednak w takim przypadku konieczne jest wcześniejsze spełnienie przesłanek wskazanych w prawie bankowym.

Takie stanowisko przedstawił Generalny Inspektor Ochrony Danych Osobowych w decyzji z lutego 2015 r. (nr DOLiS/DEC-176/15). W stanie faktycznym, do którego odnosi się przedmiotowa decyzja, skarżąca zażądała zaprzestania przetwarzania przez bank jej danych stanowiących tajemnicę bankową. Podniosła przy tym, iż pomimo opóźnienia w spłacaniu zadłużenia, bank nie miał prawa do przetwarzania jej danych (w tym przekazania ich do BIK) po wygaśnięciu zobowiązania. **Nie została ona bowiem** (wbrew temu, co nakazują przepisy prawa bankowego) **poinformowana o zamiarze przetwarzania danych bez jej zgody.**

GIODO zgodził się z argumentacją skarżącej. Zauważył, że na podstawie art. 105a ust. 3 prawa bankowego banki mogą przetwarzać informacje stanowiące tajemnicę bankową, dotyczące osób fizycznych, również po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem bez zgody osoby, której informacje dotyczą - jednak pod warunkiem łącznego spełnienia następujących przesłanek:

- osoba, której dane dotyczą nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem oraz
- po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby przez bank o zamiarze przetwarzania informacji bez jej zgody.

Ponadto, zdaniem GIODO, to bank powinien dysponować dowodami na to, iż skutecznie poinformował klienta o zamiarze przetwarzania jego danych. W szczególności nie będzie wystarczająca wyłącznie deklaracja banku, że informacja została wysłana.

Podstawa prawna:

Ustawa z dnia 29 sierpnia 1997 r. prawo bankowe (tj. Dz.U. z 2015 r. poz. 128)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2014 r. poz. 1182)

Decyzja GIODO nr DOLiS/DEC-176/15

Łukasz Czujko
Adwokat
Managing Associate
Deloitte Legal

Przetwarzanie danych osobowych jest dopuszczalne na gruncie polskiego prawa tylko wtedy, gdy spełniona zostanie jedna z przesłanek wymienionych w art. 23 ustawy o ochronie danych osobowych. Przetwarzanie danych osobowych klientów bez ich zgody na podstawie art. 105a ust. 3 prawa bankowego, jest przykładem spełnienia przesłanki niezbędności dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Należy pamiętać, iż możliwość przetwarzania danych na podstawie art. 105a ust. 3 prawa bankowego jest ograniczona w czasie do 5 lat od dnia wygaśnięcia zobowiązania. Po upływie tego okresu należy zaprzestać przetwarzania danych.

Wrześniowa nowelizacja ustawy o nadzorze finansowym oraz niektórych innych ustaw (którą dokonano m.in. zmian w ustawie o kredycie konsumenckim) wpłynęła na treść przepisów dotyczących wymiany danych klientów stanowiących tajemnicę bankową (art. 104, 105, 105a oraz 106d prawa bankowego). Od października 2015 r. również instytucje pożyczkowe (udzielające kredytów konsumenckich) mogą pozyskiwać informacje np. z BIK w zakresie niezbędnym do oceny zdolności kredytowej konsumenta i analizy ryzyka kredytowego.

Zmianie uległy również zasady dotyczące przekazywania informacji o klientach do biur informacji gospodarczej. Nowe przepisy przewidują np. że zgoda klienta na przekazanie danych może być również wyrażona w postaci elektronicznej. Instytucje przekazujące dane konsumenta do biura informacji gospodarczej będą zobowiązane wcześniej sprawdzić, czy konsument wyraził zgodę na udostępnienie tych informacji.

MIF Reg

Karty płatnicze są najczęściej stosowanym elektronicznym instrumentem płatniczym w przypadku zakupów detalicznych. Aby ułatwić sprawne funkcjonowanie wewnętrznego rynku płatności, realizowanych za pośrednictwem kart płatniczych zarówno „tradycyjnie", przez Internet, jak i przy udziale urządzeń przenośnych, a tym samym – poprawić sytuację konsumenta – UE ustanowiła jednolite wymogi techniczne i handlowe w odniesieniu do transakcji kartowych.

Zostały one wprowadzone Rozporządzeniem 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 . Akt ten znajdzie zastosowanie w odniesieniu do transakcji wykonywanych kartą płatniczą realizowanych na terenie Unii Europejskiej, w przypadku, gdy zarówno dostawca usług płatniczych płatnika, jak i dostawca usług płatniczych odbiorcy będą mieć swoje siedziby na terenie UE.

Rozporządzenie składa się z dwóch części. Pierwsza z nich ustanawia maksymalną wysokość opłat *interchange* dla transakcji kartą debetową (0,2% wartości transakcji) oraz kredytową (0,3% wartości transakcji). Warto podkreślić, iż z maksymalnych stawek opłaty *interchange* wyłączone są transakcje realizowane za pomocą kart biznesowych, transakcje realizowane przy użyciu kart wydanych przez trójstronne systemy kart płatniczych oraz wypłata gotówki w bankomatach. Ponadto, maksymalne stawki opłaty *interchange* będą mogły zostać ograniczone przez państwa członkowskie, jednak tylko w odniesieniu do transakcji krajowych, to jest transakcji, w których wydawca i agent rozliczeniowy znajdują się w tym samym państwie członkowskim lub gdy wydawca karty i punkt sprzedaży, w którym ma miejsce płatność kartą, znajdują się w tym samym państwie członkowskim. W przypadku, gdy system płatniczy nie rozróżnia transakcji kartą debetową od transakcji kartą kredytową zastosowanie ma opłata właściwa dla kart debetowych.

W drugiej części Rozporządzenia zostały omówione szczegółowo zasady biznesowe oraz wymagania techniczne regulujące transakcje dokonywane za pomocą kart płatniczych. W szczególności regulują one zagadnienia takie jak:

a) rozdzielność rachunkowa, organizacyjna i decyzyjna systemów kartowych i podmiotów obsługujących transakcję;

b) zakaz stosowania zasad utrudniających lub uniemożliwiających opatrywanie kart więcej niż jedną marką (*co-badging*);

c) zmiany w stosowaniu zasady honorowania wszystkich kart;

d) unblending, czyli zobowiązanie agenta rozliczeniowego do indywidualnego określania opłat akceptanta w odniesieniu do poszczególnych kategorii i poszczególnych marek kart płatniczych;

e) obowiązki informacyjne agentów rozliczeniowych wobec akceptantów w tym m.in. dotyczące kwoty wszelkich opłat należnych z tytułu transakcji płatniczej przekazywanych co najmniej raz w miesiącu;

f) zakaz stosowania w umowach licencyjnych lub regulaminach systemów kartowych ograniczeń terytorialnych oraz obowiązków uzyskania licencji lub zezwoleń na prowadzenie działalności transgranicznej (a także środków równoważnych) w odniesieniu do wydawania kart płatniczych lub świadczenia usługi acquiringu.

Z zakresu stosowania Rozporządzenia wyłączone są instrumenty płatnicze działające w ramach ograniczonej sieci dostawców, instrumenty, które można stosować do ograniczonego asortymentu towarów lub usług oraz instrumenty wydawane przez władze publiczne w szczególnych celach społecznych lub podatkowych.

Przepisy dotyczące maksymalnych stawek opłaty *interchange*, udzielania licencji i obowiązków informacyjnych wejdą w życie w dniu 9 grudnia 2015 r. W zakresie dotyczącym rozdzielności systemów kart płatniczych i podmiotów obsługujących transakcje, co-badgingu, unblendingu opłat i modyfikacji zasady honorowania wszystkich kart Rozporządzenie będzie stosowane od dnia 9 czerwca 2016 r.

Podstawa prawna:

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. Urz. UE L 123/1 z 19.05.2015)

Agata Jankowska-Galińska
Radca Prawny
Managing Associate
Deloitte Legal

Z praktycznego punktu widzenia problematyczne może okazać się terminowe zapewnienie zgodnego z Rozporządzeniem rozdzielenia systemów kart płatniczych i podmiotów obsługujących transakcje. Przepisy nakładające na strony obowiązek dokonania takiego podziału wchodzą wprawdzie w życie dopiero w dniu 9 czerwca 2016 – jednakże znacznie wcześniej, gdyż do 9 grudnia 2015 r. Europejski Urząd Nadzoru Bankowego (EBA) miał przygotować właściwe standardy techniczne dot. rozdzielności. EBA zapowiedział już jednak, że do końca 2015 roku będzie gotowy tylko pierwszy projekt standardów, który następnie zostanie poddany pod konsultacje publiczne. Oznacza to, iż ostateczny tekst standardów technicznych zostanie opracowany najprawdopodobniej dopiero w okolicach maja 2016 roku. Tak krótki okres pomiędzy uchwaleniem ostatecznych standardów a datą wejścia w życie zapisów Rozporządzenia - powoduje znaczne ryzyko z jednej strony nie dotrzymania terminu przez podmioty zobowiązane, a z drugiej – przeprowadzenie rozdzielności w sposób sprzeczny z oczekiwaniami i stanowiskiem EBA.

Nowe zasady wykonywania transakcji płatniczych w Internecie – rekomendacja KNF

Na posiedzeniu w dniu 17 listopada 2015 r. KNF przyjęła rekomendację dotyczącą bezpieczeństwa transakcji płatniczych wykonywanych w Internecie, kierowaną do banków, krajowych instytucji płatniczych, krajowych instytucji pieniądza elektronicznego oraz SKOK-ów.

Dokument reguluje trzy podstawowe obszary:

1) zasady i organizację procesu zarządzania oraz oceny ryzyka,

2) szczególne środki kontroli i bezpieczeństwa w zakresie płatności internetowych, a także

3) działania edukacyjne wobec klientów oraz zasady komunikacji z klientami korzystającymi z usług płatniczych wykonywanych drogą internetową.

Celem rekomendacji jest wzmocnienie bezpieczeństwa płatności internetowych poprzez nałożenie minimalnych wymogów dotyczących inicjowania i wykonywania płatności. Co istotne, dokument określa cele, jakie powinny zostać osiągnięte, jednak pozostawia podmiotom zobowiązanym swobodę, co do wyboru środków niezbędnych do ich realizacji.

Rekomendacja stanowi zasadniczo wdrożenie końcowych wytycznych Europejskiego Urzędu Nadzoru Bankowego (EBA) w sprawie bezpieczeństwa płatności internetowych z 19 grudnia 2014 r. i powinna być traktowana jako uzupełnienie Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa teleinformatycznego w bankach oraz Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach.

Nakłada ona na dostawców usług płatniczych obowiązek stworzenia **formalnej polityki bezpieczeństwa** (wraz z określeniem odrębnej funkcji ds. ryzyka) w stosunku do płatności internetowych oraz usług powiązanych, dokonywania analiz ryzyka oraz oceny zastosowanych rozwiązań technologicznych. Dostawcy usług płatniczych będą musieli również wdrożyć odpowiednie, skoordynowane z politykami bezpieczeństwa, środki bezpieczeństwa, polegające w szczególności na budowaniu wielopoziomowych zabezpieczeń w taki sposób, aby przełamanie jednego poziomu było niwelowane przez kolejną linię zabezpieczeń (tzw. „obrona w głąb"). Rekomenduje się również dokonywanie tzw. utwardzania, czyli wyłączania w serwerach wszystkich zbędnych funkcji, co ma wzmocnić ich ochronę.

Ponadto, podczas całej sesji konieczne będzie **stosowanie bezpiecznego szyfrowania danych typu „end-to-end"** (tzn. pomiędzy aplikacją klienta a serwerem zawierającym usługi, do których aplikacja uzyskuje dostęp, na takiej zasadzie, że szyfrowanie danych odbywa się w systemie źródłowym, a deszyfrowanie w systemie docelowym). Dostawcy usług płatniczych powinni też wprowadzić ograniczenie liczby nieudanych prób logowania lub uwierzytelniania, po których dostęp do usługi będzie blokowany oraz określić maksymalny czas trwania sesji. Konieczne będzie również ustalenie limitów dla usług płatności internetowych (np. dla indywidualnej transakcji lub dla transakcji w danym okresie).

Monitorując zagrożenia, dostawcy internetowych usług płatniczych powinni brać pod uwagę m.in. ryzyko związane z wybranymi rozwiązaniami technologicznymi, architekturą aplikacji czy technikami -programistycznymi zarówno po swojej stronie, jak i po stronie klienta. Dostawcy będą więc musieli **uwzględniać dla celów bezpieczeństwa również środowisko techniczne klientów**.

Dostawcy usług płatniczych powinni, co do zasady, zawsze stosować mechanizm s**ilnego uwierzytelniania klienta** (*strong authentication*) w sytuacji inicjowania płatności internetowej oraz w sytuacji uzyskiwania dostępu do wrażliwych danych płatniczych (tj. danych umożliwiających zainicjowanie zlecenia płatniczego, czy też uwierzytelnienie tożsamości klienta). Silne uwierzytelnianie dotyczy również transakcji wykonywanych za pomocą kart płatniczych. Odstąpienie od tej zasady może nastąpić jedynie w wyjątkowych przypadkach[1].

Silne uwierzytelnienie oznacza, iż w celu dokonania identyfikacji klienta, dostawca usług stosuje co najmniej dwa spośród następujących elementów:

4) wiedza – coś, co jedynie użytkownik wie (np. kod, PESEL, hasło statyczne),

5) posiadanie – coś, co jedynie użytkownik posiada (np. token, karta inteligentna, telefon komórkowy),

6) indywidulana cecha klienta (np. cecha biometryczna, odcisk palca).

Przy czym co najmniej jeden z tych elementów (oprócz indywidualnej cechy klienta) powinien być niemożliwy do ponownego użycia i nieodtwarzalny, a nieautoryzowane pozyskanie go w Internecie - niewykonalne.

Wśród wyjątków od silnego uwierzytelniania znajdują się m.in. odbiorcy z tzw. „**białych list**", tj. określonych przez klienta grup zaufanych odbiorców. Z kolei dostawcy „**rozwiązań portfelowych**" powinni wymagać silnego uwierzytelniania przez wydawcę karty płatniczej, przynajmniej gdy posiadacz po raz pierwszy rejestruje dane karty.

Ochrona klientów ma się odbywać m.in. poprzez wdrożenie w ramach środków bezpieczeństwa **zasady minimalnych uprawnień**, zgodnie z którą każdemu użytkownikowi przydzielane są jedynie takie uprawnienia, które są dla niego niezbędne do wykonywania pracy na danym stanowisku.

Dostawcy usług powinni również dążyć do tego, aby gromadzić, przesyłać, czy w inny sposób przetwarzać jak najmniejszą ilość danych klienta, konieczną do przeprowadzenia transakcji (zasada minimalizacji danych).

[1] Wymóg stosowania silnego uwierzytelniania przewiduje także dyrektywa PSD 2 (por. w szczególności art. 4 oraz art. 87 PSD 2).

Umowy ramowe z klientami powinny ponadto przewidywać możliwość zablokowania transakcji ze względów bezpieczeństwa. Rekomendacja nakłada również obowiązek jasnego określenia zakresu odpowiedzialności dostawcy usług oraz klienta, np. poprzez wprowadzenie zakazu udostępniania podmiotom trzecim wrażliwych danych płatniczych.

W zakresie edukacji i komunikacji z klientem dostawcy usług płatniczych mają za zadanie zapewnić co najmniej jeden bezpieczny kanał komunikacji na potrzeby bieżącej komunikacji dedykowany dla płatności internetowych oraz wsparcie w zakresie wszelkich pytań dotyczących usług płatności internetowych.

Katarzyna Sawicka
Aplikantka adwokacka
Associate
Deloitte Legal

Rekomendacja KNF odnosi się do wielu obszarów dotyczących płatności internetowych i kreuje szereg nowych obowiązków dla dostawców usług płatniczych. Tym bardziej warto zwrócić uwagę na znaczny zakres wyłączeń przewidzianych w rekomendacji. Po pierwsze, nie będzie ona stosowana do usług internetowych innych niż usługi płatnicze, nawet jeśli usługi te oferowane są poprzez strony internetowe dostawców przeznaczone do dokonywania płatności. Z zakresu rekomendacji zostały wyłączone więc np. umowy zawierane online i elektroniczne usługi maklerskie. Dokument nie dotyczy też płatności mobilnych innych niż realizowane przy użyciu przeglądarki internetowej, tj. np. płatności zlecanych za pomocą telefonów, poczty głosowej, czy sms, a także transakcji płatniczych dokonywanych przez przedsiębiorstwa poprzez dedykowane sieci.

Pomiędzy wytycznymi KNF a wytycznymi EBA, których polska rekomendacja ma być zasadniczo wdrożeniem, występują również pewne różnice. Są one skutkiem stanowisk konsekwentnie prezentowanych przez KNF w ostatnim czasie. Wytyczne EBA nie dotyczą, w przeciwieństwie do rekomendacji KNF, np. poleceń przelewu, w przypadku których dostęp do rachunku płatnika uzyskuje strona trzecia, a także płatności przy użyciu anonimowych, jednorazowych kart przedpłaconych (w tym wirtualnych), gdy nie występuje trwała relacja pomiędzy wydawcą a posiadaczem karty.

Agata Jankowska-Galińska
Radca Prawny
Managing Associate
Deloitte Legal

Rekomendacja **będzie miała wpływ na kształtowanie stosunków umownych pomiędzy dostawcami usług (bankami, ale też agentami rozliczeniowymi) oraz akceptantami**. Zgodnie z nowymi zasadami, określeni dostawcy będą zobligowani zobowiązać akceptantów w umowach z nimi zawieranych m.in. do tego, że (i) akceptanci będą współpracować z dostawcami oraz z organami ścigania w zakresie poważnych incydentów bezpieczeństwa płatności, (ii) wdrożą odpowiednie środki bezpieczeństwa IT, (iii) będą stosować systemy umożliwiające silne uwierzytelnienie posiadacza karty, (iv) **zapewnią wyraźne oddzielenie procesów dokonywania płatności od dokonywania zakupów online**, aby klient miał świadomość, na jakim etapie komunikuje się z dostawcą usługi, a kiedy z odbiorcą płatności. Wymóg ten może być spełniony np. poprzez otwieranie odrębnego okna, przez co proces płatności nie będzie widoczny na stronie akceptanta.

W przypadku gdy akceptant nie będzie stosował się do powyższych obowiązków, dostawca będzie miał obowiązek podjąć działania w celu wyegzekwowania zobowiązania lub rozwiązać umowę.

Podobnie w przypadku korzystania z **outsourcingu**, dostawcy będą musieli zawrzeć w umowie z podmiotem, któremu powierzają wykonanie czynności z zakresu bezpieczeństwa płatności internetowych, zobowiązanie podmiotu upoważnionego do przestrzegania zasad określonych w rekomendacji KNF.

Należy zwrócić uwagę, że wytyczne EBA przygotowane zostały w oparciu o przepisy dyrektywy w sprawie usług płatniczych. Mają one mieć charakter przejściowy, aż do zakończenia transpozycji do porządków krajowych przepisów nowej dyrektywy PSD 2, o której mówi się, że zrewolucjonizuje rynek usług płatniczych. Już teraz jednak wytyczne EBA oraz wytyczne państw członkowskich wydane na ich podstawie (np. omawiana rekomendacja KNF) **powinny być interpretowane, na ile to możliwe, biorąc pod uwagę treść i cele dyrektywy PSD 2**.

Wykorzystanie akcji wirtualnych jako element programu motywacyjnego

Wyrok Naczelnego Sądu Administracyjnego z dnia 30 stycznia 2014 r. II FSK 324/12

W przedmiotowej sprawie - spółka wyemitowała na mocy uchwały Nadzwyczajnego Zgromadzania Wspólników akcje wirtualne, które zostały nabyte przez osobę fizyczną w osobie prezesa jej zarządu. Stosownie do uchwały Nadzwyczajnego Zgromadzenia Wspólników akcje wirtualne zostały nabyte na podstawie osobnej umowy zawartej pomiędzy prezesem, a spółką. Zgodnie z tą umową pojęcie „akcja wirtualna bez prawa głosu" oznaczało prawo do otrzymania kwoty równej wartości jednej zwykłej akcji spółki po wartości księgowej obliczonej według ostatniego zweryfikowanego sprawozdania, podzielonej przez liczbę akcji z prawem głosu lub też w takiej samej proporcji obliczonej wartości jednego udziału w kwocie pieniężnej, papierach wartościowych lub innej formie zapłaty, jaka może być otrzymana za sprzedaż, wymianę akcji lub w publicznej ofercie. Choć umowa wymieniła kilka zdarzeń inicjujących, to w praktyce należało - zdaniem wnioskodawcy - oczekiwać, że będzie nim złożenie przez prezesa spółki akcji wirtualnych w celu ich wykupu przez spółkę. Po wykupie akcji spółka miała dokonać ich umorzenia.

Zdaniem NSA - samo uzależnienie ceny akcji wirtualnych od ceny akcji spółki nie czyni jeszcze z akcji wirtualnych pochodnych instrumentów finansowych. Aby można mówić o pochodnych instrumentach finansowych należy spojrzeć nie tylko na treść art. 2 ust. 1 pkt 2 ustawy o obrocie instrumentami finansowymi, ale na cały akt prawny. Zgodnie bowiem z art. 1 ust. 1 stawy o obrocie instrumentami finansowymi „ustawa reguluje zasady, tryb i warunki podejmowania i prowadzenia działalności w zakresie obrotu papierami wartościowymi i innymi instrumentami finansowymi, prawa i obowiązki podmiotów uczestniczących w tym obrocie oraz wykonywanie nadzoru w tym zakresie".

Aby instrument finansowy mógł być przedmiotem jakiegokolwiek obrotu bez wątpienia musi być zmaterializowany - czyli musi istnieć. Tymczasem w przedmiotowej sprawie de facto instrument ten nie istnieje. Jest to coś wirtualnego, coś czego nie ma - jak wskazała bowiem spółka w stanie faktycznym „termin: akcje wirtualne oznacza (...)", a więc nie istnieją żadne akcje (akcje wirtualne nie stanowią akcji w rozumieniu Kodeksu spółek handlowych) a terminem takim nazwano jedynie podstawę do ustalenia kwoty, którą ma otrzymać prezes spółki - tylko i wyłącznie na potrzeby zawartej między spółką, a jej prezesem umowy.

Akcje, o których mowa w zagadnieniu nie mają odzwierciedlenia w kapitale spółki - jak wskazała sama spółka - i nie dają nabywcy żadnych praw udziałowych w stosunku do spółki. Posiadacz akcji wirtualnych nie jest uważany za akcjonariusza spółki z tytułu posiadania tych akcji, ani za jakiegokolwiek jej uczestnika.

W związku z powyższym – akcje wirtualne nie mogą stanowić, zdaniem NSA, pochodnego instrumentu finansowego w rozumieniu przepisów art. 2 ust. 1 pkt 2 ustawy o obrocie instrumentami finansowymi.

Agata Jankowska-Galińska
Radca Prawny
Managing Associate
Deloitte Legal

Cytowane wyżej orzeczenie odnosi się do coraz szerzej stosowanych w praktyce programów motywacyjnych dla kadry menadżerskiej najwyższego szczebla opartych na pochodnych instrumentach finansowych. Polegają one na przyznaniu pracownikowi (przez pracodawcę lub spółkę z grupy) pochodnego instrumentu finansowego, odzwierciedlającego prawo do otrzymania w przyszłości wypłaty w gotówce, której wysokość zależeć będzie od instrumentu bazowego (np. wyników czy wskaźników finansowych spółki). Programy takie mogą być niezwykle korzystne - zarówno dla spółki (zwiększenie motywacji pracownika poprzez powiązanie wysokości należnego mu świadczenia z „wartością" spółki, ograniczenie kosztów pracowniczych), jak i samego pracownika (odpowiednio ukształtowane – są korzystne podatkowo, gdyż podlegają opodatkowaniu według stawki podatkowej w wysokości 19%). Kluczowym m.in. jednak jest, aby tak przyznane pracownikowi prawo stanowiło pochodny instrument finansowy w rozumieniu przepisów ustawy o obrocie instrumentami finansowymi.

W Deloitte pomagamy kompleksowo m.in. w stworzeniu programów motywacyjnych opartych na pochodnych instrumentach finansowych zarówno z perspektywy prawnej, podatkowej, jak i rachunkowej.

Dowiedz się więcej

Alerty prawne

Wybrane publikacje:

Finanse i bankowość
Nowe zasady oferowania usług finansowych (21/2015)
Autor: Katarzyna Sawicka, Associate, Deloitte Legal

Prawo pracy
Nowe zasady dot. uprawnień rodzicielskich już od stycznia 2016 r. (20/2015)
Autorzy:
Marcin Sękowski, Radca prawny, Managing Associate, Deloitte Legal
Ewa Boroń, Radca prawny, Senior Associate, Deloitte Legal

Finanse i bankowość
PSD 2 zmieni rynek nowoczesnych usług płatniczych (19/2015)
Autor: Agata Jankowska-Galińska, Radca prawny, Managing Associate, Deloitte Legal

Nieruchomości
Użytkowanie wieczyste: konsekwencje nieskutecznego przekształcenia w prawo własności) (18/2015)
Autorzy:
Konstanty Dobiejewski, Radca prawny, Partner Associate, Deloitte Legal
Justyna Olszowy, Radca prawny, Managing Associate, Deloitte Legal

Wydarzenia organizowane przez kancelarię Deloitte Legal

Prawo pracy
Seminarium: Umowa o pracę na czas określony – fundamentalne zmiany

Finanse i bankowość
Śniadanie biznesowe: Usługi finansowe – nowy obraz rynku w 2016 r.

Webcasty

Prawo pracy
Webcast: Wyzwania dla pracodawców w 2016 r. Zmiany w PIT, ZUS i prawie pracy

Odwiedź naszą stronę: www.deloittelegal.pl

Subskrypcja

Newsletter prawny Zespołów Finansów i Bankowości Deloitte Legal
www.deloitte.com/pl/subskrybcje

Kontakt

Zbigniew Korba
Partner, Radca prawny
Deloitte Legal
+48 22 348 35 56
zkorba@deloitteCE.com

Diana Kawala
Business Development & Marketing
Deloitte Legal
+48 22 348 35 88
dkawala@deloitteCE.com