Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

PRAWO NOWYCH TECHNOLOGII I INTERNETU

**Publikacja przygotowana dla Polskiej Agencji Inwestycji i Handlu (PAIH)
przez prawników kancelarii APLAW Artur Piechocki**

Autorzy publikacji:

Artur Piechocki, radca prawny
artur.piechocki@aplaw.pl

Daniel Siciński, aplikant radcowski
daniel.sicinski@aplaw.pl

Nowe technologie stanowią bardzo ważny element polskiej gospodarki. Profesjonalizm i zaangażowanie polskich pracowników w wykonywaną przez nich pracę zostały docenione przez największe międzynarodowe koncerny, które chętnie umieszczają w Polsce centra usług wspólnych. Nadal niższe płace w porównaniu z Europą Zachodnią, czy Stanami Zjednoczonymi, a także wyższa jakość pracy oraz znajomość języków obcych wśród polskich pracowników, w porównaniu z rynkami dalekowschodnimi, czynią z Polski atrakcyjne miejsce do inwestowania. Z drugiej strony, lokalni przedsiębiorcy coraz częściej podejmują ekspansję zagraniczną, szczególnie w zakresie nowych technologii.

Lokalne wymogi prawne dotyczące prowadzenia działalności w sektorze nowych technologii sprzyjają inwestycjom. Przewidywalność, standaryzacja przepisów z dyrektywami i rozporządzeniami unijnymi pozwalają spokojnie planować długoterminowe inwestycje w Polsce.

W niniejszym opracowaniu koncentrujemy się na prezentacji kilku rynków związanych z nowymi technologiami: data center i hosting, e-commerce i marketing internetowy, świadczenie usług drogą elektroniczną oraz fintech. Wybór rynków nie jest przypadkowy, ponieważ rozwijają się one w najszybszym tempie, a jednocześnie zostały kompleksowo zabezpieczone odpowiednimi przepisami prawa, których stosowanie w praktyce wspierane jest przez instytucje administracji publicznej oraz sądy.

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

1. Polski rynek data center i hostingu

Centra danych (ang. *data center*) stanowią kompleksy pomieszczeń przeznaczonych do przechowywania infrastruktury informatycznej, połączone z obszarami wspierającymi jej funkcjonalność oraz zapewniającymi bezpieczeństwo i ciągłości działania serwerów. Centra danych oferują dwa rodzaje usług. Pierwsza z nich to usługa kolokacji serwerów, w ramach której usługobiorca może umieścić swój sprzęt w ramach infrastruktury data center. Zdecydowanie popularniejszą usługą jest jednak hostingu, w ramach którego dostawca usługi udostępnia zasoby na swoich serwerach, które może być wykorzystane do utrzymywania przykładowo stron internetowych, portali, czy grup dyskusyjnych.

Polski rynek usług wykorzystujących centra danych ma już ponad 10 lat, jednak dopiero w ostatnich latach wszedł on w fazę dynamicznego rozwoju [1]. Obecnie każdego roku w Polsce przybywa powierzchni w komercyjnych centrach przetwarzania danych. W rezultacie polski rynek usług kolokacji i hostingu jest największym w Europie Środkowo-Wschodniej, a przez to budzi coraz większe zainteresowanie inwestorów i zagranicznych klientów. Znaczna dynamika rozwoju rynku powiązana jest ze wzrostem popytu i podaży na tego rodzaju usługi, wzrostem znaczenia rozwiązań chmurowych, spadkiem cen usług infrastrukturalnych, a także koniecznością zapewnienia bezpieczeństwa zasobów. Poziom wykorzystania tego typu rozwiązań w Polsce sięga obecnie 20-25 proc., podczas gdy w krajach Europy Zachodniej jest to udział rzędu 80 proc. Wskazuje to na wciąż duży potencjał do wzrostu znaczenia outsourcingu IT na polskim rynku.

Polski rynek data center notuje bardziej dynamiczny wzrost niż w krajach Europy Zachodniej. W ostatnich latach ta dynamika w odniesieniu do usług kolokacji jak i hostingu wynosiła kilkanaście procent rocznie. Według raportu PMR „Rynek centrów danych w Polsce 2016. Analiza rynku i prognozy rozwoju na lata 2016-2021", wartość krajowego rynku data center w roku 2014 szacowana była na 1,2 mld zł, natomiast w roku 2015 wzrosła ona do 1,4 mld zł, co daje około 15 proc. przyrost. Zdaniem branżowych ekspertów w najbliższych latach utrzymywać się będzie dwucyfrowy wzrost wartości polskiego rynku data center.

Sam rynek hostingu w Polsce również znajduje się w europejskiej czołówce. Jak wynika z rankingu „*Global Web Hosting Market Share 2017*"[2] Polska zajmuje 8. miejsce w Europie pod względem udziału w rynku hostingu, natomiast w ujęciu globalnym jest to miejsce 13. Polski rynek usług hostingowych, wart ponad 400 mln dolarów, plasuje się przed takimi krajami jak Australia, Brazylia czy Indie. Sukces ten jest w dużej mierze zasługą konkurencyjnych cen oferowanych przez rodzimych operatorów, a także dużej innowacyjności w oferowanych usługach.

[1] *W analizie wykorzystano dane zawarte w raporcie firmy PMR „Rynek centrów danych w Polsce 2016. Analiza rynku i prognozy rozwoju na lata 2016-2021"*
[2] *https://hostadvice.com/marketshare (dostęp: 25 marca 2017 roku)*

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

2. Hosting – aspekty prawne

Rosnący udział w rynku IT centrów przetwarzania danych przekłada się także na wzrost popularności outsourcingu opartego na rozwiązaniach chmurowych oraz usłudze hostingu. W celu zapewnienia zgodności prowadzonej działalności z obowiązującymi przepisami, dostawcy tego rodzaju usług powinni pamiętać o szeregu regulacji prawnych mających do nich bezpośrednie zastosowanie.

2.1. Odpowiedzialność dostawcy usługi hostingu

Na szczególną uwagę zasługuje Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2016 r. poz. 1030, 1579), przede wszystkim w kontekście regulacji odpowiedzialności dostawców świadczących usługi hostingu.

Przepisy tej ustawy umożliwiają usługodawcy, przy spełnieniu określonych warunków, zwolnienie się z odpowiedzialności za treści umieszczane w ramach jego zasobów przez usługobiorcę, np. poprzez zamieszczenie ich na stronie internetowej. Generalną zasadą jest brak obowiązku po stronie host providera monitorowania przekazywanych, przechowywanych lub udostępnianych przez niego danych, a także poszukiwania w nich treści bezprawnych. Obowiązuje jednak w tym zakresie procedura tzw. *notice and takedown*, opierająca się na konieczności notyfikacji usługodawcy o konkretnych treściach znajdujących się na jego serwerach, które mogą mieć bezprawny charakter. Treściami takimi mogą być udostępnione w serwisie internetowym utwory lub przedmioty praw pokrewnych, jeśli użytkownik je publikujący nie jest do tego uprawniony, a także treści naruszające dobra osobiste lub wypełniające znamiona określonych przestępstw (np. zniesławienia). W tym modelu hostingodawca nie poniesie odpowiedzialności za przechowywane dane, jeśli udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności, niezwłocznie uniemożliwi dostęp do tych danych. W takiej sytuacji wyłączona jest również odpowiedzialność hostingodawcy wobec użytkownika za szkodę, która powstała lub mogła powstać w wyniku uniemożliwienia mu dostępu do tych danych.

Jeśli więc host provider ma wpływ na to, jakie treści zamieszczane są na jego serwerach przez korzystających z usługi, np. w ramach moderowania treści komentarzy na forum dyskusyjnym, jest to równoznaczne z wiedzą o ich bezprawnym charakterze. W takiej sytuacji jest on obowiązany samodzielnie usuwać takie treści, lub uniemożliwiać do nich dostęp, nawet bez uprzedniego zawiadomienia.

Należy jednak pamiętać, iż host provider będzie ponosił odpowiedzialność za udostępniane treści, nawet przy spełnieniu wszystkich powyższych warunków, jeśli przejął on kontrolę kapitałową nad zamieszczającym te treści usługobiorcą.

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

2.2. Powierzenie przetwarzania danych

W przypadku gdy korzystający z usługi hostingu przechowuje na zasobach udostępniającego infrastrukturę IT dane osobowe, konieczne jest uwzględnienie regulacji zawartych w Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 195, 677.), a także Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100 poz. 1024). W świetle przepisów tej ustawy w stosunku takim usługobiorca jest administratorem danych osobowych, natomiast hostingodawca staje się przetwarzającym dane (tzw. procesorem). Przetwarzaniem jest bowiem wykonywanie jakichkolwiek operacji na danych osobowych, w tym m.in. zbieranie, utrwalanie, przechowywanie i udostępnianie, zwłaszcza jeśli wykonuje się je w systemach informatycznych.

W przypadku udostępnienia host providerowi danych osobowych do przetwarzania w imieniu i na rzecz usługobiorcy, konieczne jest zawarcie umowy o powierzeniu przetwarzania danych osobowych. W razie braku dopełnienia tego obowiązku, administrator danych narusza przepisy, narażając się tym samym na sankcje w przypadku kontroli GIODO. Przy braku zawarcia umowy powierzenia, udostępnienie przez usługobiorcę do przetwarzania danych osobowych hostingodawcy traktowane jest jak udostępnienie ich osobom nieupoważnionym, co stanowi przestępstwo zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Taka sankcja nie grozi usługodawcy, jeśli nie udostępnia on dalej uzyskanych w ten sposób danych, jednak w jego interesie jest zawarcie z usługobiorcą takiej umowy. Oferując bowiem możliwość zawarcia umowy powierzenia przetwarzania danych w ramach świadczonej usługi, staje się on bardziej konkurencyjny, a w razie ewentualnej kontroli GIODO ma możliwości wykazania podstawy przetwarzania danych. Umowa powierzenia umożliwia także uregulowanie praw i obowiązków stron w razie zaistnienia incydentów nieautoryzowanego udostępnienia danych.

Umowa powierzenia powinna być zawarta na piśmie i może stanowić część umowy o świadczenie usługi hostingowej, bądź też stanowić odrębny dokument. Przepisy wymagają, aby w umowie powierzenia określić co najmniej cele oraz zakres przetwarzania, poza które przetwarzający nie może wykraczać. W praktyce w umowie takiej określa się ponadto wzajemne prawa i obowiązki powierzającego oraz procesora, standardy zabezpieczenia danych przez przetwarzającego i procedurę ich kontroli przez administratora, możliwość dokonania tzw. podpowierzenia, czy też zasady zwrotu danych.

Istotnym obowiązkiem hostingodawcy, któremu powierzono przetwarzanie danych osobowych, jest zapewnienie odpowiednich środków technicznych i organizacyjnych zabezpieczających przetwarzane dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Środki te obejmują m.in. przyjęcie wymaganej dokumentacji, a w szczególności polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, a także nadanie upoważnień pracownikom

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

przetwarzającego wraz z prowadzeniem ich ewidencji. Obowiązku te mogą być realizowane przy pomocy powołanego przez przetwarzającego administratora bezpieczeństwa informacji. Co istotne, środki te powinny być wdrożone jeszcze przed faktycznym rozpoczęciem przetwarzania, a ich standard powinien odpowiadać co najmniej temu, jaki obowiązuje u samego administratora.

W przypadku niedopełnienia obowiązków ustawowych w zakresie powierzenia danych jak i prawidłowego ich zabezpieczenia, zasadniczo odpowiedzialność ponosi administrator danych, jednak nie wyłącza to odpowiedzialności przetwarzającego. W przypadku bowiem niedopełnienia obowiązków wynikających z umowy, będzie on ponosił odpowiedzialność kontraktową względem powierzającego, natomiast zaniechanie odpowiedniego zabezpieczenia przetwarzanych danych, naraża go na odpowiedzialność administracyjnoprawną w razie kontroli GIODO.

3. Polski rynek handlu i reklamy elektronicznej

W Polsce dynamicznie rozwija się rynek handlu elektronicznego. W efekcie znacznego rozwoju technologicznego w ostatnich latach, już ponad 76 proc. Polaków korzysta z internetu, z czego połowa z nich nabywa produkty i usługi online. Według raportu Gemius[3] szacunkowa wartość polskiego rynku e-commerce w roku 2015 mieściła się w przedziale 30-33 mld zł, notując przy tym 20-procentowy wzrost w stosunku do roku poprzedniego. Eksperci szacują, że wartość tego rynku powinna się podwoić w ciągu 4-5 lat, a do 2020 roku wynosić powinna ok. 63 mld zł. Stale rosnący jest też udział polskiego rynku e-commerce w całości obrotów handlowych, który wynosi obecnie 2,5-4 proc., a w ciągu najbliższych dwóch lat powinien wzrosnąć do 9 proc.

Wraz z rozwojem sektora e-commerce w Polsce, rośnie również udział wydatków na reklamę internetową, który w roku 2015 wyniósł 3,17 mld zł, co stanowi 20-procentowy wzrost w porównaniu z rokiem poprzednim.[4] Przewidywany jest także dalszy rozwój rynku marketingu internetowego, a w szczególności wzrost wydatków na kampanie reklamowe w sieciach content marketingowych oraz kontekstowych. Rośnie tym samym znaczenie reklamy internetowej, czego dowodem jest zwiększający się w polskich firmach udział budżetów marketingowych na kampanie promocyjne prowadzone w sieci.

Powyższe statystyki i prognozy wskazują na duży potencjał dalszego rozwoju sektora e-commerce i marketingu elektronicznego w Polsce, stwarzając korzystne perspektywy rozwoju dla działających w tej branży przedsiębiorców i inwestorów.

[3] https://www.gemius.pl/files/reports/E-commerce-w-Polsce-2015.pdf (dostęp 25 marca 2017 roku)
[4] http://iab.org.pl/aktualnosci/iabpwc-adex-reklama-online-na-fali-wznoszacej/ (dostęp: 25 marca 2017 roku)

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

4. Świadczenie usług drogą elektroniczną

Kluczowym aktem prawnym dla prowadzenia działalności handlowej oraz marketingu w Internecie jest wspomniana już ustawa o świadczeniu usług drogą elektroniczną. Poza regulacją odpowiedzialności hostingodawcy, ustawa ma zastosowanie do wszelkiego rodzaju usług świadczonych drogą elektroniczną. Obejmują one usługi, których wykonanie następuje przez wysyłanie i odbieranie danych za pomocą systemów teleinformatycznych na indywidualne żądanie klienta, bez jednoczesnej obecności stron, jeśli są one transmitowane za pośrednictwem sieci publicznych. Przykładami usług podlegających regulacji ustawy są np. usługa wyszukiwania treści w internecie, usługa poczty e-mail, czy też udostępnianie aplikacji mobilnych.

4.1. Obowiązki usługodawcy

W stosunku do przedsiębiorców świadczących usługi drogą elektroniczną ustawa przewiduje szereg obowiązków, takich jak konieczność przekazania klientowi określonych informacji identyfikujących przedsiębiorcę, czy tez informacji o szczególnych zagrożeniach związanych z korzystaniem z usługi świadczonej drogą elektroniczną. W przypadku usług, których przedmiotem są dane poufne klienta, np. usług bankowości internetowej, usługodawca ma ponadto obowiązek zabezpieczenia poufności i integralności przekazywanych danych, np. poprzez techniki kryptograficzne czy podpis elektroniczny. Techniki stosowanych zabezpieczeń powinny być dostosowane do rodzaju usługi oraz przekazywanych danych, a także ryzyka ich ujawnienia.

Jednym z istotniejszych obowiązków przedsiębiorcy świadczącego usługi drogą elektroniczną jest przyjęcie regulaminu świadczenia usług drogą elektroniczną, który powinien określać co najmniej rodzaj i warunki świadczonej usługi, warunki zawierania i rozwiązywania umowy, a także tryb postępowania reklamacyjnego. Regulamin taki powinien nieodpłatnie zostać udostępniony klientowi przed zawarciem umowy, np. poprzez umieszczenie go na stronie internetowej, z możliwością jego utrwalenia na urządzeniu elektronicznym klienta.

Witryna internetowa przedsiębiorcy świadczącego usługę może ponadto wykorzystywać tzw. pliki *cookies*, czyli niewielkie pliki tekstowe, które zapisywane są na urządzeniach elektronicznych wykorzystywanych przez klientów i umożliwiają prawidłowe działanie serwisu, ale także ich profilowanie pod kątem odpowiednich przekazów marketingowych. Zarówno ustawa o świadczeniu usług drogą elektroniczną, jak i ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. Z 2016 poz. 1489) nakładają w tym zakresie na właścicieli serwisów obowiązki, w tym przede wszystkim obowiązek należytego informowania użytkowników serwisu o wykorzystywaniu plików *cookies*, sposobie ich dziania oraz ich wyłączenia, a także obowiązek uzyskania zgody klienta.

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

4.2. Obowiązki w zakresie marketingu internetowego

Dla przedsiębiorców prowadzących marketing z wykorzystaniem środków komunikacji elektronicznej, a więc przykładowo na stronie internetowej lub przez pocztę elektroniczną, szczególnie istotne jest uwzględnienie wymagań jakie musi spełniać informacja handlowa. Chodzi tutaj o każdą informację przeznaczoną bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy. Informacja taka powinna być wyraźnie wyodrębniona od pozostałej treści, a także oznaczona jako komunikat marketingowy. Musi ponadto zawierać oznaczenie podmiotu od którego pochodzi, wraz z jego adresem elektronicznym, a także opis rodzaju działalności promocyjnej wraz z określeniem warunków koniecznych do skorzystania z niej.

Należy pamiętać, iż przed przesłaniem informacji handlowej za pośrednictwem środków komunikacji elektronicznej (np. e-mail, SMS) do oznaczonej osoby fizycznej lub poprzez telekomunikacyjne urządzenia końcowe (np. telefon, faks) do jakiegokolwiek podmiotu, konieczne jest uprzednie uzyskanie stosownych zgód na taką formę komunikacji. Zgody takie mogą być wyrażone w dowolnej formie, jednak istotne jest, aby nie były one dorozumiane i odbiorca miał świadomość na co wyraża zgodę oraz, że w każdym czasie może ją wycofać. Zgody te nie mogą więc zostać umieszczone w regulaminie, ale mogą być wyrażone poprzez zaznaczenie określonych *checkboxów.*

Nieprzestrzeganie regulacji dotyczących formy przekazu marketingowego, w tym stosowanie reklamy uciążliwej i naruszającej obowiązki informacyjne, może naruszać szereg przepisów. Działania takie mogą stanowić nadużywanie technicznych środków przekazu informacji, stanowiąc czyn nieuczciwej konkurencji. Mogą być także kwalifikowane jako agresywne praktyki rynkowe a także praktyki naruszające zbiorowe interesy konsumentów. W konsekwencji takich działań Urząd Ochrony Konkurencji i Konsumentów ma możliwość wszcząć postępowanie wobec przedsiębiorców stosujących takie praktyki, które może zakończyć się wymierzeniem kary w wysokości do 10 proc. obrotu osiągniętego w roku obrotowym poprzedzającym rok nałożenia kary.

Ponieważ marketing internetowy często będzie wiązał się z przetwarzaniem danych osobowych, konieczne jest również uwzględnienie wymogów przewidzianych w ustawie o ochronie danych osobowych. Świadczący usługę może bez zgody klienta przetwarzać udostępnione dane w celu marketingu własnych produktów i usług, przy czym klient może wyrazić sprzeciw wobec takiego sposobu wykorzystania jego danych. Natomiast udostępnienie danych w tym celu innym przedsiębiorcom, bądź prowadzenie marketingu ich działalności będzie zawsze wymagało wyraźnej zgody klienta, przy czym jest to zgoda odrębna i niezależna od wcześniej omówionych zgód na komunikację elektroniczną i telekomunikacyjną. Prowadzenie zbioru danych osobowych przetwarzanych w celach marketingowych wiąże się również z szeregiem innych obowiązków sprecyzowanych w tej ustawie, w tym obowiązkiem zgłoszenia go do GIODO, a także wdrożenia stosownych środków technicznych i organizacyjnych mających na celu zabezpieczenie poufności oraz integralności przetwarzanych danych.

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

5. Polski rynek fintech

Mianem fintech określa się wszelkiego rodzaju nowoczesne rozwiązania technologiczne wykorzystywane w działalności finansowej, umożliwiające zwiększenie efektywności i dostępności świadczonych usług. Używa go się także do określenia sektora gospodarki, w którym podmioty świadczące usługi finansowe wprowadzają produkty finansowe i modele biznesowe oparte technologicznych innowacjach.

Według raportu firmy Deloitte „CEE FinTech Report"[5] wartość globalnego rynku fintech szacuje się na ponad 19 mld dolarów, natomiast do 2020 r. tempo wzrostu inwestycji w tej branży będzie wynosiło 55 proc. rocznie. Sam rynek technologii wspierających usługi finansowe w Europy Środkowo-Wschodniej wyceniany jest na 2,2 miliarda euro, z czego 860 milionów przypada na Polskę.

Polski sektor fintech wyróżnia przede wszystkim konkurencyjność oraz innowacyjność sektora finansowego, współpraca między bankami a nowymi startupami z branży, wysokiej klasy zasoby ludzkie, niewielkie koszty, wielkość rynku oraz dostęp do rynków innych krajów, duże zainteresowanie inwestorów zagranicznych, a także wsparcie ze strony specjalnych stref ekonomicznych.[6] Polskę wyróżnia ponadto otwartość społeczeństwa na zmiany technologiczne oraz coraz powszechniejsze wykorzystywanie nowoczesnych możliwości w płatnościach mobilnych, w tym także bezstykowych.

O dużym potencjale polskiego rynku fintech świadczy również dynamiczny rozwój rodzimych startupów świadczących innowacyjne usługi finansowe. Takich firm na rynku działa obecnie ponad sto, z czego większość oferuje płatności elektroniczne oraz platformy finansowe. Wśród pozostałych usług znajdują się pożyczki on-line, dostęp do transakcji walutowych i kryptowalut czy inwestycji.

6. Dyrektywa PSD2

Na szczególną uwagę w tym kontekście zasługuje dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366, tzw. Dyrektywa PSD2, która w znaczącym stopniu wpłynie na kształt europejskiego sektora finansowego, otwierając jednocześnie wiele nowych szans dla innowacyjnych modeli biznesowych z obszaru fintech. Dyrektywa zastąpiła wcześniej obowiązującą dyrektywę 2007/64/WE z dnia 13 listopada 2007 r. (PSD1), rozszerzając przy tym ramy prawne dotyczące świadczenia nowoczesnych usług płatniczych, a także uzupełniając istniejące regulacje. Obecnie przepisy dyrektywy są wdrażane przez państwa członkowskie, poprzez dokonywanie stosowny zmian w krajowych regulacjach, a ostateczny termin implementacji dyrektywy przypada na 13 stycznia 2018 roku. Wprowadzone zmiany

[5] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/central-europe/ce-fintech-in-cee-region-2016.pdf (dostęp: 25 marca 2017 roku)
[6] http://fintechpoland.com/wp-content/uploads/2016/12/FinTech_w_Polsce_bariery_i_szanse_rozwoju.pdf (dostęp: 25 marca 2017 roku)

Kancelaria APLAW Artur Piechocki
ul. Solec 22
00-410, Warszawa
T:+48 606 294 306
E: artur.piechocki@aplaw.pl
www.aplaw.pl

z pewnością będą miały znaczący wpływ na rynek nowoczesnych usług płatniczych, a tym samym na działalność instytucji płatniczych, banków, niezależnych operatorów bankomatów, czy też innych dostawców usług płatniczych, oferujących płatności mobilne.

Dyrektywa będzie miała szersze zastosowanie niż dotychczasowa PSD1, która regulowała płatności ramach rynku unijnego. Nowe przepisy będą regulowały każdą transakcję, bez względu na ich walutę, jeśli co najmniej jeden z dostawców usługi płatniczej uczestniczących w transakcji posiada siedzibę na terenie Europejskiego Obszaru Gospodarczego (EOG).

Jedną z istotniejszych zmian wprowadzonych dyrektywą jest rozszerzenie katalogu dostawców usług płatniczych (tzw. TPP) o podmioty świadczące usługę inicjowania płatności oraz podmioty zapewniające dostęp do informacji o rachunku. W ramach pierwszej usługi dostawca uzyska dostęp do rachunku bankowego płatnika, a następnie będzie mógł zainicjować płatność. Dostawca usługi dostępu do rachunku będzie mógł natomiast przedstawić płatnikowi informacje o posiadanych przez niego rachunkach płatniczych. W wyniku realizacji powyższych usług nie będzie dochodziło do faktycznych przesunięć środków pieniężnych płatnika, a przez to dostawcy nie będą wchodzili w ich posiadanie. Pomimo tego dostawca usługi inicjowania płatności nadal będzie zobowiązany do zapewnienia poufności danych, nieprzetrzymywania ich oraz weryfikacji tożsamości płatnika, a także do niemodyfikowania cech transakcji. Świadczenie więc tego rodzaju usługi będzie wymagało zezwolenia, natomiast jedynie rejestracji będzie wymagała działalność zapewnienia dostępu do rachunku.

Z pozostałych zmian na szczególną uwagę zasługują nowe zasady odpowiedzialności w przypadkach incydentów nieautoryzowanych transakcji. Dyrektywa wprowadza wymóg zastosowania tzw. silnego uwierzytelniania, a więc wyższego standardu weryfikacji tożsamości płatnika, przy wykonywaniu określonych operacji płatniczych (np. przy inicjacji elektronicznej transakcji, czy też uzyskiwania dostępu on-line do rachunku). Jeśli tego rodzaju zabezpieczenie nie zostanie wprowadzone przez dostawcę usługi płatniczej, a płatnik będzie działał w dobrej wierze, w razie wystąpienia incydentu, to dostawca będzie odpowiedzialny za powstałą szkodę, a tym samym zobowiązany do zwrotu płatnikowi utraconej kwoty. Płatnik zawsze będzie miał możliwość dochodzenia roszczeń od dostawcy prowadzącego rachunek bankowy, który z kolei będzie mógł domagać się stosownej kompensaty od zewnętrznego dostawcy odpowiedzialnego za nieautoryzowaną transakcję.

www.aplaw.pl

APLaw jest polską kancelarią butikową specjalizującą się w prawie własności intelektualnej oraz nowych technologii.

APLaw została założona w 2010 r. przez radcę prawnego Artura Piechockiego, który przez wiele lat pełniąc rolę doradcy ds. prawnych i polityki domenowej rejestru PL w Naukowej i Akademickiej Sieci Komputerowej (NASK), reprezentował Rejestr w Polsce i w organizacjach międzynarodowych.

Artur Piechocki jest współzałożycielem oraz członkiem rady Sądu Polubownego ds. Domen Internetowych przy Polskiej Izbie Informatyki i Telekomunikacji (PIIT), oraz współtwórcą orzecznictwa domenowego w Sądzie Arbitrażowym przy Krajowej Izbie Gospodarczej (KIG). Ponadto, jest ekspertem Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency – ENISA) w zakresie doradztwa regulacyjnego, ochrony prywatności i danych osobowych. Współpracuje również z Internet Corporation for Assigned Names and Numbers (ICANN) oraz Światową Organizacją Własności Intelektualnej (WIPO), a w przeszłości Council of European National Top Level Domain Registries (CENTR). Był także uczestnikiem spotkań Międzynarodowej Unii Telekomunikacyjnej (ITU), a obecnie jest współpracownikiem Fundacji Bezpieczna Cyberprzestrzeń.

Kluczowe obszary doradztwa prawnego:

- prawo technologii informacyjnych i komunikacyjnych (ICT)
- ochrona prywatności i danych osobowych
- prawo własności intelektualnej
- prawo własności przemysłowej
- prawo mediów
- gry komputerowe
- prawo konkurencji i ochrona konsumentów
- usługi dla inwestorów zagranicznych