ZWIĄZEK BANKÓW POLSKICH

Bird & Bird

FORUM TECHNOLOGII BANKOWYCH

Cloud Computing w Sektorze Finansowym Regulacje i Standardy

pod redakcją Macieja Gawrońskiego

Listopad 2011

Wstęp Forum Technologii Bankowych Związku Banków Polskich

Opracowanie stanowi część raportu o cloud computingu Forum Technologii Bankowych Związku Banków Polskich. Obecnie obserwujemy w sektorze bankowym duże zainteresowanie rozwiązaniami typu cloud computing. Umożliwia ono szybki dostęp do najnowszych zasobów obejmujących oprogramowanie, aplikacje, platformę sprzętową, praktycznie z dnia na dzień, bez konieczności inwestowania w sprzęt oraz długotrwałego i kosztownego wdrażania.

Przy Forum Technologii Bankowych Związku Banków Polskich utworzono grupę ds. cloud computing. Głównym celem prac grupy jest przygotowanie raportu na temat zastosowania cloud Computingu w sektorze bankowym w Polsce i na świecie. W raporcie zostanie opisane zjawisko cloud computing całościowo, zakres modelu "przetwarzania w chmurze, aspekty prawne, możliwości wykorzystania, bariery i ograniczenia jak również korzyści.

Grupa planuje opracować i wydać raport do końca 2012r.

Poniżej część prawna raportu o cloud computingu Forum Technologii Bankowych Związku Banków Polskich pod redakcją Macieja Gawrońskiego.

Od Macieja Gawrońskiego

Mam nadzieję, że nasze opracowanie będzie pomocne jego czytelnikom. Staraliśmy się w sposób przejrzysty i wyczerpujący przedstawić regulacje, które należy uwzględnić rozważając korzystanie z usług IT w modelu cloud. Jesteśmy otwarci na wszelkie uwagi i dyskusje na ten temat i zapraszamy do kontaktu bezpośrednio ze mną pod adresem maciej.gawronski@twobirds.com.

Maciej Gawroński

Opracowanie dostępne również pod adresami internetowymi:

http://www.zbp.pl/site.php?s=MjIzODYxMA==

oraz

http://www.twobirds.com/English/Expertise/Pages/Poland.aspx

Cloud Computing w Sektorze Finansowym
Część Prawna

Spis treści

Wstęp do części prawnej

Przedstawiamy Państwu opracowanie starające się streścić regulacje krajowe znajdujące zastosowanie do przetwarzania chmurowego w bankowości a także w innych obszarach sektora finansowego. Opracowanie to stanowi pierwszą część raportu na temat cloud computingu zespołu roboczego Forum Technologii Bankowych Związku Banków Polskich.

Dotychczas nie ma w Polsce przepisów ani urzędowych interpretacji czy zaleceń odnoszących się bezpośrednio do przetwarzania chmurowego. Istnieją natomiast normy regulujące powierzanie przetwarzania informacji oraz outsourcing – powierzanie wykonywania czynności, które organizacja mogłaby realizować własnymi siłami. Stąd w tym dokumencie staramy się interpretować istniejące regulacje pod kątem tego, jakie tworzą uwarunkowania dla modelu cloud computingu.

Regulacje, które stosują się do przetwarzania chmurowego, to przede wszystkim przepisy o ochronie danych osobowych oraz przepisy dotyczące outsourcingu.

Ochrona danych. Z punktu widzenia ochrony danych osobowych co do zasady cloud computing stanowi powierzenie przetwarzania danych osobowych innemu podmiotowi. Regulacja ochrony danych osobowych ma charakter ogólny, stąd jest opisana w pierwszej kolejności.

Istnieje rozbieżność pomiędzy tradycyjnym, terytorialnym spojrzeniem na ochronę danych osobowych a modelem przetwarzania w chmurze. Organy ochrony danych osobowych wskazują na to, że w kontekście chmury uprawnienia właściciela informacji względem dostawcy chmury, w szczególności uprawnienia do nadzoru nad przetwarzaniem danych (w tym dawania wiążących wytycznych dostawcy chmury, czy możliwością audytu) są iluzoryczne. Rozwiązaniem może być nowe podejście do rozumienia tych uprawnień. Po pierwsze, prawo nadzoru nad danymi powinno być rozumiane w ten sposób, że właściciel informacji wybierając dostawcę chmury dokonuje wyboru sposobu przetwarzania danych w chmurze – ten wybór byłby oparty na tym, że właściciel informacji może skorzystać z usługi o określonych standardowych parametrach i może w każdym czasie z niej zrezygnować – nie może jednak modyfikować usługi czy dostosowywać jej do swoich indywidualnych potrzeb. Po drugie, nadzór i audyt mógłby być dokonywany za pośrednictwem odpowiednich certyfikowanych podmiotów trzecich. Kolejnym zagadnieniem jest wymóg, aby właściciel danych miał każdorazowo świadomości tego gdzie znajdują się dane a także, kto przetwarza dane je w imieniu ich właściciela. Z perspektywy praktycznej rozwiązaniem mogłoby być konkretne określenie podmiotów, które mogą przetwarzać dane, a także lokalizacji, w których dane mogą być przetwarzane. Jeśli byłoby to potrzebne w konkretnym przypadku, możliwe byłoby zlokalizowanie konkretnego miejsca przetwarzania danych oraz podmiotu przetwarzającego. Z perspektywy bezpieczeństwa danych nie ma natomiast potrzeby, aby właściciel danych permanentnie śledził dane lub miał wiedzę o ich położeniu w danej chwili.

Organy do spraw ochrony danych osobowych w różnych krajach europejskich mają różne podejście do przetwarzania chmurowego. Niektóre organy podchodzą do tego zagadnienia niezwykle restrykcyjnie inne w sposób przyjazny. Jednocześnie prawo o ochronie danych osobowych na poziomie unijnym nie zakazuje cloud computingu. Istniejące rozbieżności nawet pomiędzy poszczególnymi regulatorami w Unii Europejskiej wskazują, że świeże podejście do ochrony danych osobowych oraz do zjawiska przetwarzania chmurowego jest potrzebne. Prace nad takim świeżym spojrzeniem trwają już w Komisji Europejskiej.

Outsourcing w sektorze finansowym. Regulacje sektora finansowego dotyczące powierzania czynności za zewnątrz zwracają przede wszystkim uwagę na to, czy dana czynność lub proces, które mają być wydzielone na zewnątrz, są dla organizacji krytyczne. Za takie uważa się w szczególności czynności związane z dostępem do informacji prawnie chronionej ale także i inne, których zakłócenie naruszyłoby zdolność świadczenia przez instytucję finansową usług swoim klientom. W przypadku, gdy czynność jest krytyczna - regulacje opierają się na następujących założeniach: **(i) odpowiedzialność** – brak możliwości ograniczenia odpowiedzialności dostawcy za szkodę, **(ii) bezpieczeństwo informacji** – regulatorzy oczekują, aby instytucja finansowa znała i kontrolowała swoje ryzyko operacyjne **(iii) ciągłość działania –**

rozumiana jako jeden z aspektów bezpieczeństwa informacji; **(iv) monitorowanie ryzyka** – wiedza o tym, jakie jest rzeczywiste ryzyko związane z korzystaniem z usług podmiotu zewnętrznego. Przy tym, podobnie jak w przypadku ochrony danych osobowych, Unia Europejska z dużo większą nieufnością (a co za tym idzie z większym formalizmem) traktuje przetwarzanie danych poza terytorium Europejskiego Obszaru Gospodarczego.

Przyszłość. Ograniczenia i obawy wzmiankowane powyżej a opisane z większą dokładnością w dalszej części niniejszego opracowania wywierają wpływ na szybkość rozwoju modelu przetwarzania chmurowego. Jednak wydaje się, że przechodzenie do chmury będzie następować. Już w tej chwili duża część najpopularniejszych usług konsumenckich świadczona jest z wykorzystaniem chmur obliczeniowych. Wygoda dla konsumenta z tym związana powoduje, że procesu tego w obszarze B2C raczej nie da się zatrzymać. W obszarze B2B proces jest wolniejszy – bardziej kontrolowany administracyjnie oraz też z większą odpowiedzialnością potencjalnych klientów. Tym niemniej, zważywszy na możliwe korzyści ekonomiczne oraz nikłą różnicę od strony technologicznej względem obecnie stosowanych przez przedsiębiorstwa rozwiązań informatycznych, także i tu oczekiwać można ekspansji chmury.

Cloud Computing w Regulacjach dot. Ochrony Danych Osobowych

1. Cloud Computing w Regulacjach dot. Ochrony Danych Osobowych

Przepisy ochrony danych osobowych. Podstawowe przepisy, które regulują zagadnienie cloud computingu, choć bezpośrednio do niego się nie odwołują, to przepisy o ochronie danych osobowych. Takimi przepisami są w szczególności:

(i) ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.02.101.926) (dalej jako **„uodo"**), która jest implementacją

(ii) Dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (dalej jako **„Dyrektywa"**); oraz

(iii) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 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.04.100.1024) (dalej jako **„Rozporządzenie"**); oraz

(iv) poszczególne regulacje sektorowe wskazane w punktach 1.2. oraz 1.4. poniżej.

(v) Szczególne zasady ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczna reguluje Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz.U.02.144.1204) (dalej jako **„usude"**).

Podstawowe pojęcia. Według uodo **dane osobowe** to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, na podstawie których bezpośrednio lub pośrednio możliwe jest określenie tożsamości osoby (np. dane pracowników, klientów lub potencjalnych klientów, adres email, numer telefonu). Innymi słowy są to relacje pomiędzy szeregiem danych o osobie, które prowadzą do konkretnej osoby.

Niejako „właściciel" danych osobowych – podmiot, który decyduje o celach i środkach przetwarzania danych osobowych, nazywany jest **administratorem danych osobowych**. Np. administratorem danych klientów banku jest bank.

Administrator może sam wykonywać operacje na danych osobowych lub przekazać je do wykonania podwykonawcy, tzw. **przetwarzającemu dane osobowe**. Przetwarzający (z ang. *processor*) jest to podmiot działający w imieniu i na rzecz administratora danych i upoważniony przez administratora danych do przetwarzania danych osobowych.

W cloud computingu mamy często do czynienia z sytuacją, w której administratorem danych jest odbiorca a przetwarzającym jest dostawca usług w chmurze. Możliwe są także inne konfiguracje.

Przetwarzanie danych osobowych regulowane uodo ujęte jest bardzo szeroko, gdyż obejmuje jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Zakres zastosowania przepisów ochrony danych. W świetle Dyrektywy i Opinii 8/2010 Grupy roboczej art. 29[1] w sprawie prawa właściwego z dnia 16 grudnia 2010 r. („**Opinia**") należy przyjąć, że uodo

[1] Grupa robocza art. 29 jest to niezależny europejski organ doradczy w zakresie ochrony danych i prywatności, składającego się z organów ochrony danych osobowych z poszczególnych państw członkowskich.

stosuje się do administratorów danych (np. odbiorców chmury) **(i)** mających siedzibę na terytorium Polski lub prowadzących stałą i wyodrębnioną działalność w Polsce (np. w formie oddziału) albo **(ii)** mających siedzibę poza Europejskim Obszarem Gospodarczym (dalej jako **„EOG"**), ale wykorzystujących do przetwarzania danych osobowych środki techniczne znajdujące się na terytorium Polski (pod warunkiem, że środki te nie służą wyłącznie do przekazywania danych osobowych). Za środki techniczne administratora danych spoza EOG uważa się m.in. serwery administratora danych zlokalizowane w EOG ale także środki techniczne przetwarzającego dane w EOG, któremu administrator danych spoza EOG powierzył przetwarzanie danych osobowych. Według nowatorskiego poglądu wyrażonego w Opinii 8/2010 Grupy roboczej art. 29[2] w sprawie prawa właściwego z dnia 16 grudnia 2010 r. za środki techniczne wykorzystane przez administratora danych do przetwarzania danych a znajdujące się w Polsce, które spowodują stosowanie prawa polskiego, można uznać również pliki tekstowe cookies umieszczone na urządzeniu końcowym użytkownika znajdującego się w Polsce (np. w komputerze, tablecie lub smartfonie) w celu przechowywania danych osobowych.

Do przetwarzającego dane z siedzibą w Polsce zastosowanie będzie mieć uodo w zakresie rozdziału 5, to jest środków zabezpieczających zbiory danych osobowych.

Według Dyrektywy, Opinii, gdy administrator danych i przetwarzający dane znajdują się w różnych Państwach EOG, relacją między administratorem danych i przetwarzającym rządzi prawo ochrony danych osobowych państwa siedziby administratora danych. Dodatkowo do przetwarzającego dane stosują się zasady zabezpieczenia danych osobowych określone w państwie siedziby przetwarzającego.

Zatem uodo ma zastosowanie także do przetwarzających w sytuacjach (i) i (ii), przy czym w zakresie ograniczonym, to jest tylko w odniesieniu do środków zabezpieczających dane osobowe.

Zasięg obowiązywania uodo może być więc bardzo szeroki. Podobnie szeroki może być zakres zastosowania innych ustaw europejskich opartych na Dyrektywie.

„Wieloreżimowa zgodność" chmury. W teorii Dyrektywa ma wyznaczać jednolity poziom ochrony danych osobowych w EOG i nakładać podobny poziom obowiązków na podmioty przetwarzające dane – w praktyce rozbieżności pomiędzy poszczególnymi systemami prawnymi w krajach EOG są znaczne.

Formalnie do przetwarzającego dane stosują się zasady zabezpieczenia danych osobowych miejsca jego siedziby.

W praktyce jednak przetwarzający dane zobowiązany jest często do wykonania nie tylko ciążących na nim jako przetwarzającym dane obowiązków zabezpieczenia danych osobowych (które to obowiązki podlegają prawu jego siedziby), a także, w wykonaniu umowy powierzenia przetwarzania danych, zobowiązany jest wykonać obowiązki administratora danych, w tym w zakresie zabezpieczenia danych osobowych.

W takim wypadku, pomimo wskazanego powyżej stanowiska wyrażonego w Opinii odnośnie stosowania do obowiązków zabezpieczenia danych osobowych prawa państwa siedziby przetwarzającego, w praktyce wystąpi sytuacja, w której przetwarzający dane osobowe będzie zobowiązany do kumulatywnego stosowania środków zabezpieczających wskazanych zarówno w prawie państwa swojej siedziby jak i siedziby administratora danych.

W szczególności, administratorzy danych (odbiorcy chmury) z Polski oczekiwać powinni od dostawców chmury zlokalizowanych w innych krajach EOG spełnienia obowiązków określonych przez uodo, w tym w zakresie zabezpieczenia danych osobowych. W teorii sposób zabezpieczenia danych osobowych gwarantowany przez systemy prawne innych państw EOG powinien być wystarczający. Jednak ze względu na obowiązki ciążące na odbiorcach chmury z Polski (np. obowiązek zapewnienia funkcjonalności systemu IT, dzięki której system rejestruje kto, kiedy ma dostęp do danych i kto, kiedy i w jakim zakresie je

[2] Grupa robocza art. 29 jest to niezależny europejski organ doradczy w zakresie ochrony danych i prywatności, składającego się z organów ochrony danych osobowych z poszczególnych państw członkowskich.

modyfikuje) często konieczne będzie, aby dostawca chmury zapewniał zgodność chmury z polskimi wymaganiami ochrony danych osobowych.

Analogicznie, przetwarzający dane (dostawca chmury) mający siedzibę w Polsce lub wykorzystujący środki techniczne do przetwarzania danych osobowych w Polsce, który kieruje swoje usługi do administratorów danych (odbiorców chmury) mających siedzibę w różnych państwach EOG, może być zmuszony dostosować warunki przetwarzania danych osobowych do wymogów wszystkich tych państw członkowskich.

1.1 Obowiązki administratora danych a cloud computing

Aby przetwarzanie danych osobowych było zgodne z prawem, administrator danych (odbiorca chmury) musi dopełnić szeregu obowiązków wynikających z uodo oraz Rozporządzenia, m.in. (i) zapewnić szczególną staranność przetwarzania danych, (to jest zapewnić, że dane przetwarzane są w konkretnym, określonym celu, a także że są merytorycznie poprawne (dokładne, kompletne i aktualne) i adekwatne do celu przetwarzania, a także przetwarzane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania), (ii) przetwarzać dane osobowe na podstawie konkretnych przesłanek legalizujących, (iii) zapewnić odpowiednie informacje osobie, której dane dotyczą, (iv) zarejestrować zbiór danych, (v) odpowiednio zabezpieczyć dane osobowe.

Obowiązki te mogą być wykonane bezpośrednio przez administratora danych lub, jak wspomniano powyżej, administrator danych może powierzyć wykonanie części obowiązków przetwarzającemu (np. obowiązek udzielenia odpowiednich informacji osobom, których dane dotyczą).

Na administratorze danych ciąży odpowiedzialność za przetwarzanie danych zgodnie z prawem, w tym spełnienie wszystkich obowiązków ustawowych / nadzór nad tym, aby wszystkie obowiązki były spełnione. Dlatego administrator danych powinien mieć nieustanną kontrolę nad warunkami, w jakich przetwarzane są dane osobowe. W tym kontrolę nad tym do jakich podmiotów trafiają przez niego administrowane dane osobowe, gdzie i w jaki sposób będą one przetwarzane oraz czy będą one odpowiednio zabezpieczone.

1.2 Obowiązek zabezpieczenia danych osobowych w uodo

Szczególnie kłopotliwy przy przetwarzaniu danych osobowych w chmurze (w szczególności jeśli dane osobowe przetwarzać będzie dostawca poza Polską) może okazać się obowiązek zabezpieczenia danych osobowych w zgodzie z uodo i Rozporządzeniem.

Polskie przepisy są jednymi z nielicznych w EOG tak szczegółowo opisującymi odpowiednie techniczne i organizacyjne środki zabezpieczenia, które muszą być stosowane, aby odpowiednio chronić dane osobowe.

Tytułem przykładu wskazać można, że polski administrator danych (przetwarzający) powinien dysponować i wdrożyć w swojej organizacji pisemną politykę bezpieczeństwa i instrukcję zarządzanie systemem informatycznym oraz ewidencję użytkowników systemu IT. Dokumenty te powinny określać, między innymi miejsca, w których dane są przetwarzane (tj. miejsca w których fizycznie następuje przetwarzanie danych osobowych), funkcjonalność systemu informatycznego (m.in. to czy system zapewnia odnotowywanie informacji, kto i kiedy wprowadził dane osobowe do systemu, a także kiedy je modyfikował, oraz komu i kiedy przekazał).

Jeśli dane osobowe zostały powierzone lub przekazane podmiotom trzecim do „chmury", kłopotliwe może być zidentyfikowanie w polityce bezpieczeństwa miejsc, w których administrowane przez niego dane się znajdują. Należałoby, jak się wydaje, wskazać wszystkie lokalizacje centrów danych należących do chmury. Dodatkowo administrator danych musi spełniać wymogi względem funkcjonalności systemu IT - np. wymaga się sporządzenia czytelnych raportów, w których należy wskazać źródło danych, informacji o sprzeciwie, udostępnieniach danych wraz z datą i zakresem udostępnienia.

Kiedy administrator danych osobowych przekazuje dane osobowe do dostawcy chmury, którego centrum działalności zlokalizowane jest w Polsce, spełnienie powyższych obowiązków nie powinno być problemem, gdyż dostawca chmury jest zobowiązany przez uodo i Rozporządzenie do ich stosowania we własnej organizacji.

Kiedy administrator danych (odbiorca chmury) przekazuje dane dostawcy chmury poza Polską, powinien szczególnie zadbać o to, żeby dostawca chmury odpowiednio zabezpieczył dane.

1.3 Cloud computing jako powierzenie przetwarzania danych osobowych

W literaturze pojawiło się pytanie, czy chmura obliczeniowa będzie powierzeniem przetwarzania danych osobowych. Pytanie to postawiono w kontekście cloud computingu polegającego wyłączne na udostępnianiu infrastruktury w celu przechowywania danych, czyli hostingu.

Zdaniem Grupy roboczej art. 29 wyrażonym w Opinii 1/2010 z dnia 16 lutego 2010 r. w sprawie pojęć „administrator danych" i „przetwarzający", hosting co do zasady stanowić będzie powierzenie przetwarzania danych osobowych do przetwarzającego dane.

Część doktryny kwestionuje taką kwalifikację chmury, w sytuacji, gdy dostawca chmury nie ma dostępu do danych, gdyż np. są one zaszyfrowane przez odbiorcę chmury. Wydaje się jednak, że tak długo jak przechowywanie danych osobowych będzie jedną z operacji, która stanowi przetwarzanie danych osobowych w rozumieniu uodo, to zlecenie innemu podmiotowi (dostawcy chmury) już choćby operacji przechowywania danych osobowych odbiorcy chmury będzie w istocie stanowiło powierzenie przetwarzania danych osobowych.

Ciekawy pogląd wyraził Generalny Inspektor Danych Osobowych (dalej jako "GIODO")[3] na stronie https://edugiodo.giodo.gov.pl/file.php/1/INF1/INF_R05.html. Mówi on, że „gdy mamy do czynienia z powierzeniem przetwarzania danych, w rozumieniu art. 31 uodo, co oznacza, że podmiot udostępniający infrastrukturę informatyczną posiada wiedzę co do charakteru przetwarzanych danych, wówczas podlega jej przepisom w zakresie art. 36–39 (zabezpieczenia danych osobowych), pomimo iż nie jest administratorem danych osobowych. Natomiast, jeżeli podmiot udostępniający system nie posiada wiedzy co do charakteru przetwarzanych danych, to podlega przepisom art. 12–15 usude".

W praktyce jednak najczęściej zasłonięcie się przez dostawcę infrastruktury brakiem wiedzy o charakterze przetwarzanych danych nie będzie wiarygodne.

1.4 Umowa o powierzenie przetwarzania danych osobowych

Lekarstwem na większość powyższych problemów związanych z zapewnieniem odpowiedniej kontroli na zasadami przetwarzania i zabezpieczenia danych osobowych może być właściwie sporządzona umowa gwarantująca stałe utrzymanie odpowiedniego sposobu przetwarzania danych osobowych.

W przypadku chmury prywatnej czy hybrydowej odbiorca chmury ma szansę indywidualnego ukształtowania postanowień umownych w sposób zapewniający odpowiednie zabezpieczenie procesów przetwarzania danych w chmurze. W przypadku chmury publicznej odbiorca chmury będzie miał mniejszą lub żadną możliwość negocjowania umowy i wpływu na jej kształt, zatem odpowiedzialnością dostawcy chmury będzie wypracowanie takiej umowy, aby instytucja zaufania publicznego, jaką jest bank (a także inne instytucje finansowe), miała możliwość zaakceptowania zaproponowanych warunków.

Uodo nakazuje, aby powierzenie przetwarzania danych osobowych przetwarzającemu przez administratora danych nastąpiło na podstawie umowy o powierzenie przetwarzania danych osobowych. Przepis uodo

[3] https://edugiodo.giodo.gov.pl/file.php/1/INF1/INF_R05.html w dacie 6 października 2011

stanowi, że umowa taka powinna być zawarta w formie pisemnej. Brak formy pisemnej może rodzić negatywne konsekwencje dla administratora danych na gruncie prawa administracyjnego, GIODO może wydać decyzję nakazująca zawarcie takiej umowy w formie pisemnej. Teoretycznie może też skutkować odpowiedzialnością karną za nienależyte zabezpieczenie danych osobowych.

Umowa o powierzenie przetwarzania danych osobowych powinna przynajmniej minimalnie określać cel i zakres przetwarzania danych osobowych. Jak wskazano powyżej, administrator danych - odbiorca usług w „chmurze" - odpowiada (przed GIODO i osobą, której dane dotyczą) za spełnienie wszystkich ciążących na nim obowiązków, nawet jeśli powierzył przetwarzanie danych osobowych przetwarzającemu.

Przetwarzający z kolei odpowiada przed GIODO za zabezpieczenie danych osobowych w zakresie powierzonych mu danych osobowych tak jak administrator danych. Przetwarzający odpowiada względem administratora danych za zgodność przetwarzania z zawartą umową.

W Polsce właściwie wystarczające jest powołanie się w umowie o powierzeniu danych osobowych na przepisy uodo i Rozporządzenie, gdyż zapewniają one wystarczający poziom zabezpieczenia. Natomiast powierzając dane osobowe dostawcy chmury w innym państwie EOG (szczególnie jeśli prowadzi on działalność w systemie prawnym który nie zapewnia szczegółowych regulacji ustawowych odnośnie zabezpieczenia danych) właśnie regulacja umowna zabezpieczenia danych będzie ogrywała podstawową rolę.

Konieczne jest zatem staranne umowne doprecyzowanie obowiązków przetwarzającego, a także uprawnień kontrolnych administratora danych, uregulowanie sposobu zwrotu czy zniszczenia danych osobowych na wypadek rozwiązania umowy czy określenie miejsc przetwarzania danych. W ten sposób administrator danych może uzyskać umowną gwarancję, że dane osobowe w chmurze będą właściwie zabezpieczone.

1.5 Podpowierzenie danych osobowych

Dostawca chmury, który chciałby część usługi świadczonej w chmurze podzlecić innemu wykonawcy (na przykład spółce z grupy) powinien pamiętać o implikacjach takiego podzlecenia z pespektywy danych osobowych. Podzlecenie jest to podpowierzenie przetwarzania danych osobowych (ang. *subprocessing*). Podpowierzenie przetwarzania danych osobowych, inaczej niż powierzenie przetwarzania danych, nie jest wprost uregulowane w uodo.

Zdaniem GIODO, podpowierzenie będzie zgodne z prawem gdy (i) administrator danych zawrze umowę powierzenia bezpośrednio z podpowierzającym, lub (ii) umowa pomiędzy administratorem danych i przetwarzającym dane będzie zawierać wyraźnie upoważnienie do podpowierzania przetwarzania danych osobowych.

Oznacza to, że (i) dostawca chmury powinien zawrzeć klauzulę podpowierzenia danych osobowych w umowie o powierzeniu danych osobowych z odbiorcą chmury lub (ii) odbiorca chmury powinien zawrzeć umowę bezpośrednio z podprzetwarzającym.

Ta pierwsza ewentualność wydaje się bardziej optymalna z perspektywy praktycznej, aczkolwiek podprzetwarzający powinien być określony. Blankietowe wskazanie podprzetwarzającego może być niewystarczające.

Przyjmuje się, że wymogi dotyczące umowy powierzenia danych osobowych wskazane przez Ustawę, tj. obowiązek zawarcia umowy w formie pisemnej, wskazania celu i zakresu przetwarzania danych, zabezpieczenia danych osobowych przez podprzetwarzającego stosują się także do umowy/klauzuli podpowierzenia.

1.6 Eksport danych osobowych

Eksportem danych osobowych określa się żargonowo przekazanie danych osobowych poza Polskę. Oczywiście, w kontekście Internetu, instytucje prawne oraz koncepcje oparte na Dyrektywie z 1995 r. (która powstała przed erą Internetu) nie w pełni odpowiadają obecnej rzeczywistości i z konieczności wymuszają sztuczne podziały terytorialne.

Pamiętając o tym założeniu, kluczowym czynnikiem, jaki należy badać przy eksporcie danych, jest zlokalizowanie chmury, tj. ustalenie czy chmura znajduje się na terytorium EOG czy też poza tym obszarem.

EOG. Eksport danych w ramach EOG (jako zapewniający na podstawie Dyrektywy ten sam poziom ochrony) nie wymaga spełnienia dodatkowych wymagań. Zatem umieszczenie danych osobowych w chmurze położonej na terenie EOG jest traktowane jak skorzystanie z usług polskiej chmury.

Poza EOG. Eksport danych do kraju trzeciego poza EOG nie wymaga spełnienia dodatkowych obowiązków, jeśli prawo tego kraju zapewnia adekwatną ochronę danych osobowych. Jeżeli eksport danych osobowych ma nastąpić do kraju trzeciego niezapewniającego adekwatnej ochrony danych osobowych, konieczne jest spełnienie dodatkowych wymagań.

Komisja Europejska, w drodze decyzji, wskazała jak na razie tylko 10 państw (w tym np. Kanadę, Australię, Izrael) na około 190 istniejących, które spełniają wymagania adekwatnej ochrony i tym samym eksport danych do tych państw nie musi być obwarowany szczególnymi wymogami.

Także Stany Zjednoczone, co do zasady, nie zapewniają adekwatnego poziomu ochrony. Jednakże niektóre amerykańskie podmioty gospodarcze, które uzyskały certyfikat programu *Safe Harbour* („Bezpieczna przystań") przez uczestnictwo w nim gwarantują odpowiedni poziom ochrony danych osobowych. Należy jednak pamiętać, że podmioty amerykańskie mają możliwość selektywnego przystępowania do programu *Safe Harbour*, np. tylko w odniesieniu do własnych danych pracowniczych.

Tym samym, jeśli chmura będzie zlokalizowana także w państwie spoza EOG zapewniającym adekwatny poziom ochrony lub jeśli dostawca chmury przystąpił do programu *Safe Harbour* –będzie to chroniło odbiorcę chmury przed dodatkowymi obowiązkami.

Zgoda GIODO na eksport danych. Teoretycznie zgodnie z uodo i wytycznymi GIODO eksporter danych powinien dokonać samodzielnej oceny, czy państwo, do którego zamierza eksportować dane zapewnia adekwatną ochronę danych osobowych.

W praktyce, ocena taka byłaby niezmiernie trudna, gdyż wymagałaby uwzględnienia wszystkich okoliczności transferu danych, w tym znajomości prawa innego państwa i praktyki jego stosowania. Dodatkowo ocena powinna uwzględniać wpływ na adekwatności zamierzonego eksportu charakteru danych, celu i czasu trwania zamierzonego eksportu danych, a także kraju pochodzenia i kraju ostatecznego przeznaczenia danych. Eksporter danych będzie też ponosił ryzyko niewłaściwej oceny adekwatności innego systemu prawnego (w postaci odpowiedzialności administracyjnej a nawet karnej).

Dlatego, w praktyce przyjmuje się, że wyłącznie eksport danych do państw trzecich uznanych przez Komisję Europejską za zapewniające adekwatny poziom ochrony lub należący do *Safe Harbour* nie wymaga spełnienia dodatkowych obowiązków.

Aby uzyskać zgodę GIODO, eksporter danych musi zapewnić, że importer danych zagwarantuje odpowiednie zabezpieczenie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. Najczęściej taką gwarancją będzie odpowiednia umowa pomiędzy eksporterem a importerem danych.

Komisja Europejska opracowała dwa mechanizmy zapewnienia adekwatnej ochrony danych tj.

(i) standardowe klauzule umowne (zestaw odpowiednich wzorcowych postanowień umownych);

(ii) wiążące reguły korporacyjne (możliwość przyjęcia zasad ochrony danych obowiązujących spółki danej korporacji – w wyniku przyjęcia tych reguł i ich zatwierdzenia przez odpowiednie organy ochrony danych osobowych – w Polsce GIODO – korporacja jest traktowana jako bezpieczny obszar przetwarzania danych, w którym dane osobowe są chronione na poziomie wymaganym w Unii Europejskiej) oraz

Z perspektywy praktycznej - zgoda GIODO jest udzielona na konkretny eksport danych, w zakresie wskazanym we wniosku – dookreślone muszą być kategorie danych, które mają być przekazane, osoby, których dane dotyczą, oraz cel w którym dane będą przetwarzane po przekazaniu. GIODO nie udziela generalnej zgody na eksport wszystkich kategorii danych, bez ich dookreślenia. Zatem, jeśli eksporter danych chciałby rozszerzyć zakres eksportowanych danych (np. w związku z rozszerzeniem oferty dostawcy chmury) musi ponownie wystąpić do GIODO o zgodę.

Inne podstawy eksportu danych. Hipotetycznie, eksport danych do państwa nie zapewniającego adekwatnego poziomu ochrony może być także dokonany bez zgody GIODO na podstawie jednego z wyjątków np. (i) za pisemną zgodą osoby, której dane dotyczą (forma pisemna nie jest spełniona, jeśli zgoda jest wyrażona przez Internet) (ii) gdy jest to niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie (iii) dane są ogólnie dostępne. Jednak przesłanki te musiałyby się odnosić do wszystkich eksportowanych danych, a wiec musiałaby się odnosić do wszystkich danych i każdej z osób, której dane miałyby być umieszczone w chmurze. W praktyce mało prawdopodobne jest powołanie się na którąkolwiek z przesłanek względem wszystkich danych osobowych (a więc i wszystkich podmiotów danych), które miałyby znaleźć się w chmurze.

Tytułem przykładu, zastanówmy się nad odbiorcą chmury, który chciałby oprzeć przekazanie danych osobowych do chmury znajdującej się poza EOG na podstawie zgody osób, których dane dotyczą (abstrahując od konieczności uzyskania zgody na piśmie, która w kontekście podmiotów działających na podstawie prawa bankowego mogłaby potencjalnie być ważnie uzyskana w formie elektronicznej ze względu na art. 7 prawa bankowego).

Zgoda, aby była ważna, musi być dobrowolna. Ponadto, osoba której dane dotycz,ą w każdej chwili może odwołać swoja zgodę (ze skutkiem na przyszłość). To oznacza, że jeśli choć jedna osoba nie wyrazi zgody na eksport danych do kraju poza EOG lub taką zgodę odwoła, odbiorca chmury byłby zmuszony wycofać dane tej osoby z chmury i przetwarzać je na terytorium EOG lub uzyskać zgodę GIODO na eksport tych danych.

Model eksportu danych osobowych na podstawie zgody osoby, której dane dotyczą, ze swej istoty nie będzie kompletny tj. nie będzie dotyczył wszystkich osób, których dane znajdują się w danym zbiorze danych. Nie nadaje się on zatem do zapewnia legalność eksportu danych osobowych zawartych w całym, kompletnym zbiorze danych.

W związku z powyższym wyjątki od konieczności uzyskania zgody GIODO na eksport danych mają marginalne znaczenie przy przekazaniu danych do chmury.

1.7 Sankcje

Za nieprzestrzeganie przepisów dotyczących ochrony danych osobowych w szczególności przy przetwarzaniu danych osobowych w chmurze lub powierzeniu ich do chmury mogą grozić sankcje (i) administracyjne, (ii) karne, lub (iii) cywilne.

GIODO może na podstawie decyzji administracyjnej zażądać przywrócenia stanu zgodnego z prawem np. poprzez zastosowania dodatkowych środków zabezpieczenia zgromadzonych danych osobowych, wstrzymanie przekazania danych od państwa trzeciego. W przypadku gdy podmiot naruszający nie wykonuje decyzji, GIODO może nałożyć grzywnę w celu przymuszenia podmiotu do wykonania decyzji - jednorazowo do 50 tys. zł, zaś łącznie do 200 tys. zł.

Konsekwencją szeregu naruszeń uodo jest także odpowiedzialność karna. Przykładowo, w sytuacji, gdy osoba administrująca danymi choćby nieumyślne naruszy obowiązek zabezpieczenia danych w chmurze, dopuszcza się przestępstwa według przepisów uodo, zagrożonego karą grzywny, ograniczenia wolności albo pozbawienia wolności do 2 lat.

Prywatność i dane osobowe są objęte także ochroną cywilnoprawną. Nieposzanowanie zasad ochrony danych osobowych może skutkować naruszeniem dóbr osobistych osoby, której dane dotyczą. Osoba taka może żądać zaniechanie naruszenia i usunięcia jego skutków, zapłaty kwoty pieniężnej tytułem zadośćuczynienia za doznaną krzywdę, lub odszkodowania za wyrządzoną szkodę.

1.8 Podsumowanie

Model przetwarzania danych osobowych w chmurze mieści się w obecnym modelu ochrony danych osobowych.

Przetwarzanie danych w chmurze będzie legalne, o ile odbiorca chmury spełni wszystkie ciążące na nim obowiązki z zakresu ochrony danych osobowych. Z perspektywy praktycznej oznacza to, że dostawca chmury musi zapewnić odbiorcy chmury (który odpowiada za dane osobowe przetwarzane w chmurze), że przetwarzanie danych osobowych w chmurze nastąpi zgodnie z zasadami wiążącymi odbiorcę chmury.

Kluczowym zagadnieniem jest odpowiednia umowa pomiędzy odbiorcą i dostawcą chmury. Powinna ona gwarantować odpowiednie zasady przetwarzania danych osobowych oraz mechanizm weryfikacji tych zasad.

Dodatkowo, jeśli lokalizacja chmury miałaby wykraczać poza Europejski Obszar Gospodarczy, konieczne jest zapewnienie podstawy prawnej (najczęściej zgody GIODO) na eksport danych do dostawcy chmury.

Zważywszy na wielopodmiotowy oraz wielonarodowy charakter przetwarzania chmurowego, dogodnym sposobem wykazania zgodności chmury z europejskim reżimem ochrony danych osobowych mogą okazać się wspomniane wyżej wiążące reguły korporacyjne.

Komisja Europejska chcąc wyjść na przeciw trudnościom lub wątpliwościom związanym z przetwarzaniem danych w chmurze oraz zapewnić odpowiednią ochronę danych przetwarzanych w chmurze poza EOG przygotowuje obecnie strategię dotyczącą cloud computingu. Strategia ta może wpłynąć na wykładnię przepisów dotyczących danych osobowych w chmurze oraz na dalsze zmiany legislacyjne w tym zakresie.

Outsourcing w Sektorze Finansowym

2. Outsourcing w Sektorze Finansowym

Normy, a idąc za nimi regulacje dotyczące powierzania czynności na zewnątrz zwracają przede wszystkim uwagę na to, czy dana czynność lub proces, które mają być wydzielone na zewnątrz, są dla organizacji krytyczne (tzn. czy problem z realizacją takiej czynności lub procesu uniemożliwia lub istotnie utrudnia wykonywanie przez organizację swojej podstawowej działalności).

Regulacje skupiają się zasadniczo na czynnościach lub procesach krytycznych dla organizacji, pozostawiając czynności niekrytyczne poza obszarem regulowanym przez prawo administracyjne, a więc w domenie prawa cywilnego i zasady swobody kontraktowania. Ocenę istotności (wydzielanej) czynności dla organizacji regulacje pozostawiają sferze praktyki z jednym znaczącym wyjątkiem – czynności związane z dostępem do informacji prawnie chronionych są uznawane za czynności krytyczne / podlegające regulacjom. Zgodnie tą logiką reglamentacja dotyczy czynności powodujących dostęp do danych (informacji) objętych prawem nałożonym obowiązkiem zachowania w tajemnicy oraz innych czynności, które dla organizacji są krytyczne.

W przypadku czynności i procesów krytycznych, regulacje na ogół opierają się na następujących założeniach:

(i) **Odpowiedzialność.** *Ktoś, kto może coś zniszczyć, ma nad tym władzę* (Paul Atryda, Diuna, Frank Herbert). *Z wielką władzą wiąże się wielka odpowiedzialność* (Wujek Ben, Spiderman). Jak się wydaje polski ustawodawca wyznaje obie te zasady. W konsekwencji, regulując outsourcing, na ogół nie zezwala na to, aby dostawca usługi krytycznej mógł ograniczyć swoją odpowiedzialność za szkody wyrządzone nienależytym jej wykonaniem.

(ii) **Bezpieczeństwo informacji.** Regulatorzy europejscy, w tym polski, oczekują, aby instytucja finansowa znała i kontrolowała swoje ryzyko operacyjne, w tym w szczególności, aby zapewniała bezpieczeństwo informacji prawnie chronionej. Warunkiem zapewnienia bezpieczeństwa i świadomego zarządzania ryzykiem jest znajomość ryzyka. Przy procesach wewnętrznych wychodzi się z założenia, że ryzyko jest znane. Organizacja i jej kadra zarządzająca obcuje na co dzień z poszczególnymi czynnikami ryzyka – procesami, personelem, infrastrukturą. Konieczność zinstytucjonalizowania procesu monitorowania ryzyka pojawia się, gdy tracimy z oczu proces – czyli w przypadkach przekazania go na zewnątrz. Opierając się na tej obserwacji, ustawodawca i regulatorzy oczekują od organizacji, że nawet w przypadku przekazania na zewnątrz danej czynności, organizacja będzie w dalszym ciągu faktycznie monitorować ryzyko z tym związane, nie poprzestając na sferze zobowiązań prawnych czyli zapewnień.

W zakresie zapewnienia bezpieczeństwa, co wyjaśnione zostało w dalszej części niniejszego opracowania, pojawia się pytanie czy rzeczywiście przetwarzanie chmurowe zapewnia mniejsze bezpieczeństwo informacji niż outsourcing lub wręcz insourcing. Wydaje się, że odpowiedź na na tak postawione pytanie wydaje się brzmi – nie. Co do zasady przetwarzanie chmurowe nie generuje większego ryzyka dla bezpieczeństwa informacji niż outsourcing czy utrzymywanie procesu wewnątrz. W przypadku cloud computingu stosują się te same metody bezpieczeństwa i separacji danych jak w przypadku outsourcingu/insourcingu. Być może jedną z zalet jest ponadto (z punktu widzenia bezpieczeństwa danych) odseparowanie fizyczne, bowiem największym zagrożeniem dla organizacji są zawsze działania jej pracowników.

Jednak, odpowiedź na pytanie, czy konkretny dostawca chmury w ramach konkretnego rozwiązania zapewnia oczekiwany przez nas poziom bezpieczeństwa informacji, zależy od sytuacji rzeczywistej, co do której odbiorca chmury powinien się należycie upewnić.

(iii) **Ciągłość działania.** Ciągłość działania jest jednym z aspektów bezpieczeństwa informacji – bezpieczeństwa w aspekcie dostępności informacji. Regulatorzy oczekują zapewnienia ciągłości działania z tych samych względów, które zostały opisane w obu poprzednich punktach.

(iv) **Monitorowanie ryzyka**. Wiedza o tym, jakie jest rzeczywiste ryzyko związane z korzystaniem z usług podmiotu zewnętrznego.

Niewykluczone, że w modelu cloud computingu efekt skali może ułatwiać zapewnienie ciągłości działania. Dostawcy powinno zależeć bardziej na zapewnieniu ciągłości działania swojej usługi, gdy obsługuje on tą samą infrastrukturą wiele podmiotów. Równocześnie zważywszy na wielkość infrastruktury podstawowej koszt ewentualnych napraw czy koniecznej redundancji może okazać się relatywnie mniejszy względem rozwiązań o mniejszej skali przy zapewnieniu tego samego poziomu niezawodności.

Outsourcing Bankowy

3. Outsourcing Bankowy

Prawo bankowe, podobnie jak inne obecnie obowiązujące przepisy, nie reguluje wprost cloud computingu. Do przetwarzania chmurowego będą jednak miały zastosowanie wymogi prawne dla tzw. outsourcingu w działalności bankowej, które określa Ustawa z 29 sierpnia 1997 r. Prawo Bankowe (Dz.U.02.72.665) (dalej jako **„Prawo bankowe”**), w szczególności w art. 6a-6d.

Banki mogą powierzać wykonywanie różnych czynności prawnych lub faktycznych innemu przedsiębiorcy. Powierzenie przetwarzania danych, którego rodzajem jest cloud computing, jest czynnością faktyczną w rozumieniu Prawa bankowego. Stąd dalsza analiza koncentrować się będzie na reglamentacji powierzania przez banki podmiotom trzecim przetwarzania danych (outsourcing rodzaju usług informatycznych).

Ustawodawca nałożył na banki szereg obowiązków związanych ze zleceniem na zewnątrz czynności faktycznych związanych z działalnością bankową.

Usługi informatyczne podlegające reżimowi outsourcingu bankowego.

Reglamentacji podlegają czynności faktyczne „związane z działalnością bankową”, a więc związane z czynnościami bankowymi (art. 5 Prawa bankowego) oraz innymi czynnościami, które podejmuje bank w ramach swojej działalności i w granicach uprawnień do podejmowania działalności określonych Prawem bankowym (art. 6 ust. 1 Prawa bankowego) lub innymi ustawami (np. ustawą o pośrednictwie ubezpieczeniowym).

Zgodnie ze stanowiskiem GINB (pismo z 21 grudnia 2004 r., NB-BPN-I-022-70/04) za czynności związane z działalnością bankową można uznać tylko takie, które pozostają w bezpośrednim i funkcjonalnym związku z taką działalnością, a więc czynności cząstkowe (składowe) czynności wskazanych w art. 5 i 6 ust. 1 Prawa bankowego lub takie, bez których podjęcia nie jest możliwe (ze względu na istotę lub charakter danej czynności bankowej lub czynności z art. 6 ust. 1 Prawa bankowego) wykonanie umowy, której przedmiotem są czynności wymienione w art. 5 i 6 ust. 1 ustawy.

Przenosząc to stanowisko na grunt technologii informatycznych, GINB zalicza do czynności faktycznych związanych z działalnością bankową takie czynności, z którymi wiąże się dostęp do informacji „wrażliwych” związanych z działalnością bankową banku powierzającego, w szczególności danych objętych tajemnicą bankową. Istotnym i faktycznie determinującym czynnikiem jest przy tym także cel wykonywanych na rzecz banku czynności. Za pozostające „w związku” z działalnością bankową uznaje się także te czynności, których znaczenie jest fundamentalne dla zapewnienia ciągłego i niezakłóconego działania systemów informatycznych służących bezpośrednio do wykonywania działalności bankowej (np. systemy obsługi bankowości internetowej, systemy służące do rejestracji operacji bankowych).

Zdaniem regulatora nie są natomiast objęte ustawowym reżimem outsourcingu bankowego czynności dotyczące systemów informatycznych nie wykorzystywanych bezpośrednio do czynności działalności bankowej (czyli w szczególności sfera procesów wewnętrznych takich jak np. zarządzanie zasobami ludzkimi, wewnętrzna administracja materiałami, logistyka, zarządzanie zakupami), nabywanie sprzętu, nabywanie i instalacja oprogramowania, tworzenie, rozwój i modyfikacja licencjonowanego oprogramowania, serwis sprzętu komputerowego czy standardowego oprogramowania operacyjnego/systemowego.

Rozróżnienie, czy dana czynność faktyczna lub proces biznesowy są związane (specyficznie) z działalnością bankową czy też nie (podział na czynności krytyczne i niekrytyczne), ma więc istotne znaczenie dla określenia wymogów warunkujących dopuszczalność przeniesienia powiązanego z taką czynnością lub procesem przetwarzania danych.

3.1 Treść reglamentacji outsourcingu bankowego.

Cały proces outsourcingu bankowego poddano aktywnej kontroli Komisji Nadzoru Finansowego (dalej jako „**KNF**"). W ramach swoich uprawnień KNF (wcześniej jej poprzednik – Komisja Nadzoru Bankowego poprzez Główny Inspektorat Nadzoru Bankowego („**GINB**") uczestniczy także w tworzeniu standardów w zakresie realizacji wymogów ustawowych, wydając przepisy wykonawcze (Uchwała nr 379/2008 Komisji Nadzoru Finansowego z dnia 17 grudnia 2008 r. w sprawie określenia wykazu dokumentów dotyczących działalności przedsiębiorcy zagranicznego, który ma wykonywać powierzone przez bank czynności określone w art. 6a ust. 1 ustawy – Prawo bankowe (dalej „**Uchwała**")), ale także rekomendacje, interpretacje i zalecenia dotyczące stosowania przepisów związanych z outsourcingiem bankowym, które w praktyce tworzą wraz z samą regulacją ustawową nierozłączną całość regulacyjną dla sektora bankowego. Dlatego niektóre wnioski czy informacje przedstawione poniżej uwzględniają stanowisko KNF (GINB), czy przepisy wydane przez KNF, dla pełnego przedstawienia istoty zagadnienia.

3.2 Wymogi formalne

Aby móc powierzyć do chmury (ogólnie na zewnątrz) procesy informatyczne o krytycznym znaczeniu (w szczególności przetwarzanie danych klientowskich) Bank musi dopilnować spełnienia następujących wymogów:

1) bank i dostawca chmury muszą posiadać plany ciągłości działania (z ang. *BCDR = business continuity + disaster recovery*) obejmujące przekazany proces / czynności

2) bank musi przeprowadzić analizę wpływu przekazania na działalność banku pod kątem wpływu na: (i) zgodność z prawem; (ii) ostrożne i stabilne zarządzanie bankiem; (iii) skuteczność kontroli wewnętrznej; (iv) możliwość audytu banku; (v) bezpieczeństwo informacji (ochronę tajemnicy) – przekazanie jest możliwe, jeśli analiza wpływu nie wykaże negatywnych konsekwencji przekazania czynności na zewnątrz

3) bank ujmuje ryzyko przekazania czynności w systemie zarządzania ryzykiem

4) bank prowadzi ewidencję umów o powierzeniu czynności na zewnątrz; nadto

jeśli dostawca usług lub poddostawca ma siedzibę poza terytorium Europejskiego Obszaru Gospodarczego lub powierzone czynności mają być wykonywane poza EOG

5) bank musi uzyskać zezwolenie KNF na zawarcie umowy.

Powierzenie przez bank wykonywania czynności może nastąpić na podstawie umowy zawartej na piśmie. W umowie z dostawcą usług bank powinien ująć:

1) konieczność posiadania przez dostawcę planu ciągłości działania;

2) zobowiązanie dostawcy do przedstawienia opisu rozwiązań technicznych stosowanych przy świadczeniu usług, zapewniających bezpieczeństwo informacji i sprawną realizację usług;

3) zobowiązanie do realizacji usług na terenie EOG lub uzależnienie wejścia w życie umowy od zgody KNF na realizację usług lub dostawcę spoza EOG;

4) warunki podzlecania przez dostawcę czynności (podoutsourcingu/podpowierzenia), w tym (i) obowiązek uzyskania zgody banku na stałe podpowierzenie, (ii) obowiązek uzależnienia podpowierzenia poza EOG lub podmiotowi spoza EOG od zgody KNF, (iii) obowiązek dalszego „przeniesienia" na poddostawcę istotnych obowiązków dostawcy (w tym w szczególności tych, które są konsekwencją przepisów);

5) brak ograniczeń odpowiedzialności;

6) zasady monitorowania sposobu wykonywania umowy i ryzyka związanego z jej przedmiotem;

7) sposób współpracy z kontrolą wewnętrzną i audytorem banku;

8) zobowiązanie dostawcy do poddania się kontroli KNF oraz uprawnienia dostępu KNF do informacji o umowie i jej wykonywaniu;

9) prawo banku do zmiany umowy wskutek decyzji lub zaleceń KNF;

10) zobowiązanie dostawcy do przedstawiania dokumentów założycielskich i rejestracyjnych dostawcy.

Zakaz ograniczeń odpowiedzialności. Obowiązuje zakaz ograniczania odpowiedzialności dostawcy usług wobec banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej – art. 6b ust. 1 Prawa bankowego. Zakaz ograniczania odpowiedzialności dostawcy skorelowany jest z ustawowym zakazem wyłączania lub ograniczania odpowiedzialności banku wobec swoich klientów za szkody wyrządzone wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej przez dostawcę.

Kwestia odpowiedzialności ma szczególnie istotne znaczenie dla przetwarzania chmurowego. Usługa przetwarzania chmurowego wyrosła w obszarze usług konsumenckich, gdzie finansowa odpowiedzialność dostawcy usługi była praktycznie wyłączona. Polska regulacja outsourcingu bankowego stoi na przeciwległym biegunie – pełnej odpowiedzialności dostawcy. Wymóg ten wywołuje w dalszym ciągu duże kontrowersje po stronie dostawców (zwłaszcza zagranicznych), w szczególności z sektora usług informatycznych, w którym praktyka stosowania ograniczeń odpowiedzialności jest powszechna. Jednak wraz z pojawieniem się biznesowej oferty cloud computingu w sektorze finansowym trudno spodziewać się, aby polski ustawodawca łatwo zmienił swoje nastawienie.

Podoutsourcing. Do niedawna w świetle interpretacji Komisji Nadzoru Finansowego, podoutsourcing był niedozwolony. Obecnie formalnie uznano możliwość podzlecania czynności objętych umową outsourcingową. Podoutsourcing nie może obejmować całości świadczeń objętych umową (aby uniknąć konstrukcji tzw. „wydmuszki") a nadto (i) bądź powinien być przewidziany w umowie outsourcingowej oraz bank powinien wyrazić na konkretne podzlecenie zgodę na piśmie; (ii) bądź może nastąpić incydentalnie dla odwrócenia skutków katastrofy lub innego przypadku siły wyższej. Do podoutsourcingu stosują się te same wymagania co do outsourcingu bezpośredniego (np. zakaz ograniczeń odpowiedzialności, plany ciągłości działania, zapewnienie możliwości efektywnej kontroli KNF, wymóg zgody KNF na wyjście z EOG). Również przepisy dot. tajemnicy bankowej zostały znowelizowane w sposób dostosowujący je do instytucji podoutsourcingu.

Podobnie jak podpowierzenie przetwarzania danych, zagadnienie podoutsourcingu ma istotne znaczenie dla cloud computingu. Świadczeniem głównym przy przetwarzaniu chmurowym jest „chmura" i jej zasoby. Chmurowe zasoby przetwarzania danych są zaś na ogół własnością prawną jak i pod kontrolą faktyczną różnych podmiotów. W naszej ocenie nie przeszkadza to co do zasady zastosowaniu struktury umowa główna / umowy podoutsourcingowe. Jednak właściwą ocenę zarówno strony umowy o przetwarzanie chmurowe jak i regulator będą musiały przeprowadzać na podstawie okoliczności konkretnego przypadku. Praktyka wypracuje na pewno uznawane struktury i postanowienia. Możliwe będzie także stosowanie struktur transakcji wypracowanych przez sektor bankowy pod rządami poprzedniej regulacji – umożliwiające zawarcie umów outsourcingowych z „wielopodmiotowym" dostawcą usług bankowych, gdzie faktycznie usługi większości z usługodawców mają charakter pomocniczy, czy wspierający (uzupełniający) usługi głównego dostawcy. Do typowych takich struktur należą: konsorcjum dostawców, spółka celowa dostawcy i jego podwykonawców, umowa lokalna w celu wykonania postanowień umowy globalnej zawartej przez spółki-matki (dostawca występuje jako podmiot wiodący z podwykonawcami).

Nadzór KNF i banku nad powierzonymi czynnościami. Zgodnie z Prawem bankowym i dodatkowo wytycznymi KNF (GINB), bank powinien zapewnić sobie oraz KNF, na poziomie umowy z dostawcą usług, między innymi prawo do kontrolowania pomieszczeń, gdzie wykonywane są usługi,

dokumentacji usługodawcy, w tym dokumentów finansowych (także przez biegłego rewidenta banku) i innych związanych ze świadczonymi usługami w zakresie, w jakim jest to niezbędne do oceny jakości usług, sytuacji prawnej i finansowej usługodawcy i jego zdolności do świadczenia usług w sposób należyty i nieprzerwany.

Prawo kontroli fizycznej jest również zagadnieniem istotnym z punktu widzenia przetwarzania chmurowego. Zważywszy, że korzystanie z chmury ma między innymi na celu efektywne wykorzystanie zasobów informatycznych, a także na to, że dane odbiorcy usługi mogą znajdować się w każdej lokalizacji chmury, samodzielna realizacja ewentualnego prawa kontroli przez każdego z klientów, mogłaby znacząco utrudnić działalność dostawcy chmury, a także może wpłynąć na obniżenie bezpieczeństwa. Zarówno względy ekonomiczne, jak i względy jakości procesu wskazywałyby w naszej opinii na sensowność przeprowadzania cyklicznych audytów bezpieczeństwa przez niezależny podmiot trzeci z prawem bezpośredniej kontroli przez klienta w sytuacjach szczególnych.

Plany ciągłości działania. Kwestia rzeczywistego zapewnienia faktycznej i prawnej ciągłości działania wydaje się szczególnie ważna w przypadku procesu umieszczonego w chmurze. Zagadnienie niezawodności chmury oraz możliwości migracji obsługiwanego przez chmurę procesu do innego środowiska musi być zweryfikowana przed podjęciem decyzji o „wejściu chmurę" a następnie monitorowana.

Ochrona informacji/tajemnicy. Zapewnienie bezpieczeństwa informacji w chmurze jest zagadnieniem istotnym. Ocenę możliwości i praktycznej realizacji tego zapewnić mogą specjaliści merytoryczni. Istotnym zwiększeniem transparentności tej kwestii będzie zastosowanie odpowiednich standardów i poddanie się audytom niezależnych instytucji przez dostawców chmury. Wyrażane są niekiedy ogólne obawy o bezpieczeństwo danych w chmurze – a w szczególności o ich zabezpieczenie przed nieuprawnionym dostępem np. innych użytkowników chmury. Wydaje się jednak, że w praktyce zapewnienie bezpieczeństwa danych w chmurze nie różni się istotnie np. od zapewnienia bezpieczeństwa danych w infrastrukturze dostawcy usług outsourcingowych.

3.3 Sankcje

KNF w drodze decyzji może nakazać bankowi podjęcie działań, które mają na celu zmianę lub nawet rozwiązanie umowy outsourcingowej (podoutsourcingowej) (art. 6c ust. 5 Prawa bankowego). Taka sytuacja może mieć miejsce, gdy:

1) wykonanie umowy zagraża ostrożnemu i stabilnemu systemowi zarządzania bankiem; lub

2) przedsiębiorca lub przedsiębiorca zagraniczny będący stroną umowy stracił wymagane uprawnienia niezbędne do wykonania tej umowy.

Nadto należy pamiętać, że wniesienie przez bank skargi na decyzję KNF nie wstrzymuje wykonania takiej decyzji (art. 6c ust. 5 Prawa bankowego). Upływ wyznaczonego przez KNF terminu i nie zrealizowanie nałożonych obowiązków może spowodować, że KNF (bez uprzedniego upomnienia) zastosuje środki przewidziane w art. 138 ust. 3 Prawa bankowego (m.in. (i) wystąpienie z wnioskiem o odwołanie prezesa banku, (ii) kara finansowa do 1.000.000 zł).

3.4 Podsumowanie

Korzystanie przez banki z usług informatycznych w modelu przetwarzania chmurowego należy weryfikować pod kątem wymogów ustawowych dotyczących outsourcingu w działalności bankowej.

Gdy usługi te będą dotyczyły wykonywania czynności pozostających w funkcjonalnym związku z prowadzoną przez bank działalnością bankową (bezpośrednie zastosowanie chmury w wykonywaniu działalności bankowej), lub będą powodowały dostęp usługodawcy do tajemnicy bankowej, będą one objęte reżimem regulacji outsourcingowych, ze wszystkimi konsekwencjami dla czynności przygotowawczych po stronie banku, warunków kontraktowych ich świadczenia jak i ewentualnych obowiązków względem KNF (ograniczonych po ostatniej nowelizacji Prawa bankowego głównie do uzyskania zezwolenia na outsourcing poza EOG).

Wydaje się, że najistotniejszym zagadnieniem dla rozwoju modelu przetwarzania chmurowego w polskim systemie bankowym jest obowiązujący zakaz ograniczania odpowiedzialności dostawcy usług outsourcingowych. Zakaz ten z punktu widzenia standardów kontraktowych w informatyce wydaje się rygorem trudnym do zaakceptowania usługodawcom informatycznym, szczególnie międzynarodowym, i chyba najsurowszym w Europie. Okazuje się w praktyce, że są organizacje gotowe na akceptację formalnie nieograniczonej odpowiedzialności. Jednak pozostaje pytanie, czy taki rygor będzie do zaakceptowania przez dostawców chmury biznesowej i czy taki rygor jest potrzebny z punktu widzenia zapewnienia bezpieczeństwa informacji i procesów banku. Liczymy, że dojdzie do eksperckiej dyskusji na ten temat, z udziałem przedstawicieli wszystkich zainteresowanych stron, w tym regulatora czyli Komisji Nadzoru Finansowego.

Rekomendacje Komisji Nadzoru Finansowego

4. Rekomendacje Komisji Nadzoru Finansowego

Spośród wydanych przez Komisję Nadzoru Finansowego rekomendacji, do zagadnień związanych z przetwarzaniem chmurowym odnoszą się Rekomendacja D z 2002 r. (tekst zaktualizowany) dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki a także Rekomendacja M z 2004 r. dotycząca zarządzania ryzykiem operacyjnym w bankach.

Oba dokumenty zawierają zasadniczo pragmatyczne i zgodne z dobrymi standardami branży informatycznej zalecenia zbliżone do wyżej opisanych wymagań, które Prawo bankowe nakłada na banki w przypadku outsourcingu bankowego (np. konieczność systemowego i przemyślanego podejścia do rozwiązań informatycznych stosowanych przez bank – posiadania strategii informatycznej, posiadania strategii ciągłości działania, analizy i monitorowania ryzyka operacyjnego).

Standardy Branżowe

5. Standardy Branżowe

Cloud computing jest nowym zjawiskiem biznesowym w technologiach informatycznych. Stąd czasem rodzi nieufność, pojawiają się pytania o poziom bezpieczeństwa w chmurze.

Jak się wydaje, z punktu widzenia technologicznego rozwiązania chmurowe różnią się od dotychczas stosowanych rozwiązań informatycznych głównie skalą oraz równoległym wykorzystaniem zasobów chmury przez różnych użytkowników (tzw. chmura prywatna jest uznawana co do zasady za „zwykły" outsourcing). Z powyższego wynika, że problemy technologiczne, w szczególności dotyczące bezpieczeństwa informacji (poufności, integralności, dostępności, rozliczalności) nie różnią się od problemów informatyki „niechmurowej".

Zważywszy na powyższe, szczególną rolę w ocenie merytorycznej usługi przetwarzania chmurowego mogą spełniać dostępne standardy branżowe. Równocześnie, zważywszy na te same obawy i punkty zainteresowań poszczególnych użytkowników i potencjalnych użytkowników chmury, dostawca chmury powinien być zainteresowany zarówno stosowaniem uznanych standardów jak i uwierzytelnieniem swojej usługi poprzez jej certyfikację i weryfikację przez niezależnych specjalistów.

Poniżej wskazujemy znane autorom raportu standardy międzynarodowe, pod kątem których można oceniać rozwiązania technologiczne i organizacyjne oferowane w ramach usług cloud computingu.

5.1 Normy ISO

PN-ISO/IEC 20000-1:2007 Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja

PN-ISO/IEC 20000-2:2007 Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania

ISO/IEC 20000-3:2009 Information technology -- Service management -- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1

PN-ISO/IEC 27005:2008 Technika informatyczna, Techniki bezpieczeństwa, Zarządzanie ryzykiem w bezpieczeństwie informacji.

ISO/IEC 27001:2007 Technika informatyczna, Techniki bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji, Wymagania.

Normy powyższe mogą służyć do opracowania zasad dostarczania usługi (zarządzania ciągłością działania, zapewnienia bezpieczeństwa, optymalizacji) przez dostawcę chmury, a także do oceny przez bank rozwiązań w zakresie ciągłości działania opracowanych i przedstawionych bankowi przez dostawcę chmury. W zakresie ISO 20000 i 27001 organizacje mogą uzyskać certyfikację.

ISO/IEC 31000:2009 – Zarządzanie ryzykiem – Zasady i wskazówki, oraz ISO/IEC 31010:2009 – Zarządzanie ryzykiem, Techniki oceny ryzyka. Normy, zgodnie z ich tytułami, zawierają zasady, wskazówki i metody oceny różnych ryzyk i mogą być przydatne na etapie analizy wpływu przekazania przetwarzania do chmury jak i w dalszej ocenie ryzyka. Normy mają charakter ogólny – nie są specyficznie adresowane do ryzyk „informatycznych".

5.2 Normy British Standards Institution

BS 25777:2008 Zarządzanie ciągłością w informatyce i telekomunikacji – Kodeks dobrych praktyk. Podobnie jak wyżej wspomniane normy ISO, ten kodeks dobrych praktyk w zakresie ciągłości zarządzania informatyką i telekomunikacją może służyć do opracowania zasad zarządzania ciągłością działania przez

dostawcę chmury jak i przez bank, a także do oceny przez bank rozwiązań w zakresie ciągłości działania opracowanych i przedstawionych bankowi przez dostawcę chmury.

Także, BS 25999-1:2006 Zarządzanie ciągłością działania Część 1. Praktyczne zasady oraz BS 25999-2:2007 Zarządzanie ciągłością działania Część 2. Specyfikacja.

5.3 Standard SAS70 oraz Standard SSAE16

Zarówno Standard SAS70 jak i obecnie obowiązujący Standard SSAE16 zostały stworzone przez amerykańską organizację American Institute of Certifed Public Accountans (AICPA) do oceny (audytu) działania firm usługowych czyli dostawców usług outsourcingowych.

Obecnie standard SAS70 został zastąpiony przez AICIPA dwoma nowymi standardami: (i) standardem w zakresie raportowania SSAE16 (Statement on Standards for Attestation Engagement No. 16') (ii) standardem w zakresie audytu dla klientów (SAS Audit Considerations Relating to Entity using a Service Organization).

SAS70 był standardem w zakresie audytu zaprojektowanym, aby niezależny audytor mógł dokonać oceny i wydać opinię na temat istnienia, ale nie treści i głównych elementów, systemu kontroli dostawcy usługi. Jednakże fakt, iż dostawca usługi był w stanie wylegitymować się i przedstawić klientowi raport audytorski zgodny z SAS70 nie sprawiał, iż klient miał wiedzę nt. aktualnej kontroli zabezpieczeń stosowanej przez dostawcę usługi.

AICPA postanowiła podzielić standard SAS70 na dwa standardy: (i) jeden w zakresie standardów, które mają zastosowanie do dostawców usług (SSAE16) oraz (ii) drugi mający zastosowanie do sprawozdań finansowych klientów korzystających z usług dostawców zewnętrznych (Audit Consideration Relating to an Entity Using a Service Organisation). Kluczowe znaczenie dla usług IT ma więc standard SSAE16.

Standard SSAE16 wprowadza dwa rodzaje raportów audytora dostawcy usługi:

- **Typ 1** – dotyczy usługi dostawcy w zakresie dokładnego opisu zabezpieczeń określonych danych wraz z opinią audytora, czy dany opis jest zaprezentowany uczciwe oraz odpowiedni dla osiągnięcia deklarowanych celów

- **Typ 2** – zawierający ten sam zakres raportu co Type 1 oraz dodatkowo opinię audytora czy systemy zabezpieczeń dostawcy usług działały sprawnie przynajmniej w minimalnym okresie ostatnich 6 miesięcy.

Wydaje się, że zapoznanie się przez odbiorcę chmury (jego dział audytu wewnętrznego czy audytorów zewnętrznych) z raportem SSAE16 T2 może dać mu wiedzę na temat zakresu zabezpieczeń danych stosowanych przez dostawcę chmury jak i ich działania w praktyce.

5.4 ITIL 2011

ITIL to zestaw dobrych praktyk zarządzania usługami IT. Normy ITIL były pierwotnie rządowym standardem Wielkiej Brytanii. Normy ITIL stały się podstawą opracowania standardu ISO 20000, stąd ich stosowanie może ułatwić wdrożenie i certyfikowanie tego standardu.

29 lipca 2011 został opublikowany nowy zestaw norm ITIL zawierający szczątkowe odniesienia do cloud computingu. ITIL 2011 m.in. dostarcza: (i) definicję struktury usług w chmurze, (ii) opis strategii świadczenia takich usług, (iii) zagadnienia wdrażania różnego rodzaju usług do środowiska chmurowego – jednak bez propozycji konkretnych ani kompleksowych rozwiązań.

Inne Regulacje Sektora Finansowego

6. Inne Regulacje Sektora Finansowego

6.1 Cloud Computing w regulacjach dot. sektora funduszy inwestycyjnych

Podobnie jak w przypadku sektora bankowego, także w odniesieniu do sektora funduszy inwestycyjnych regulacje ustawowe dopuszczają powierzenie przez towarzystwo, czy też bezpośrednio fundusz, wykonywania niektórych czynności związanych z funkcjonowaniem funduszu inwestycyjnego podmiotom zewnętrznym.

Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych (Dz.U.04.146.1546 ze zmianami) (dalej jako **„ufi"**) wprost wspomina o podmiotach wyspecjalizowanych, takich jak depozytariusz (w zakresie prowadzenia rejestru aktywów funduszu inwestycyjnego) czy agent transferowy (w zakresie prowadzenia rejestru uczestników funduszu). Ustawa milczy o innych czynnościach, jakie towarzystwo czy fundusz inwestycyjny może zlecać podmiotom zewnętrznym w ramach outsourcingu. Analiza przepisów ustawy wskazuje jednak, że przewiduje ona możliwość zlecania również innych czynności niezbędnych do sprawnego i niezakłóconego działania funduszu. W ramach takiej działalności mieści się np. reklama, marketing, prowadzenie ksiąg rachunkowych czy też usługi informatyczne.

Podobnie jak w przypadku Prawa bankowego, również w zakresie sektora funduszy inwestycyjnych istnieją szczegółowe regulacje dotyczące zachowania tajemnicy. Regulacje te mogą mieć wpływ na warunki świadczenia usług informatycznych, a więc i cloud computingu, w przypadku gdyby w ramach świadczonych usług dostawca usługi przetwarzania chmurowego miałby możliwość dostępu do danych objętych tajemnicą zawodową na mocy ustawy o funduszach inwestycyjnych.

Tajemnica zawodowa uregulowana jest w art. 280 – 284 ufi. Zgodnie z art. 280 ust. 2 tajemnicą zawodową jest „tajemnica obejmująca informację uzyskaną w związku z podejmowanymi czynnościami służbowymi w ramach zatrudnienia, stosunku zlecenia lub innego stosunku prawnego o podobnym charakterze, dotyczącą chronionych prawem interesów podmiotów dokonujących czynności związanych z działalnością funduszu inwestycyjnego lub zbiorczego portfela papierów wartościowych, w szczególności z lokatami oraz rejestrem uczestników funduszu lub zbiorczego portfela papierów wartościowych, lub innych czynności w ramach regulowanej ustawą działalności objętej nadzorem Komisji lub zagranicznego organu nadzoru, jak również dotyczącą czynności podejmowanych w ramach wykonywania tego nadzoru."

Tajemnica zawodowa w ufi ujęta jest więc szeroko, obejmując swym zakresem wszelkie informacje uzyskane w związku z czynnościami dotyczącymi szeroko pojętej działalności funduszy inwestycyjnych, a dotyczące „chronionych prawem interesów podmiotów dokonujących czynności związanych z działalnością funduszu lub zbiorczego portfela papierów wartościowych". Będą to więc zarówno informacje dotyczące danego funduszu inwestycyjnego, zarządzającego nim towarzystwa, jak i innych podmiotów za pośrednictwem których fundusz wykonuje swoją działalność (w tym informacje dotyczące treści wiążących strony stosunków prawnych, czy informacje stanowiące tajemnicę przedsiębiorstwa), jak również informacje dotyczące klientów funduszu (uczestników oraz potencjalnych uczestników) lub zbiorczego portfela papierów wartościowych (w tym zarówno dane osobowe, jak i wszelkie informacje stricte inwestycyjne, dotyczące transakcji).

Katalog podmiotów zobowiązanych do zachowania tajemnicy zawodowej przewiduje art. 280 ust. 1 ufi. Zgodnie z art. 280 ust. 1 pkt 1 lit. f ufi do zachowania tajemnicy zawodowej zobowiązane są między innymi osoby wchodzące w skład organów oraz pracownicy podmiotów pozostających z towarzystwem lub funduszem w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze. Mogą to być na przykład podmioty świadczące usługi informatyczne, w tym również w ramach cloud computingu.

Z punktu widzenia umowy o przetwarzanie chmurowe istotny jest przepis art. 284 ust. 2 ufi, zgodnie z którym osoby zobowiązane do zachowania tajemnicy zawodowej ponoszą odpowiedzialność za szkody wynikające z ujawnienia takiej informacji i wykorzystania jej niezgodnie z przeznaczeniem. Przepis ten wprowadza zatem ustawową nieograniczoną odpowiedzialność osób wchodzących w skład organów i

pracowników outsourcera za ujawnienie informacji stanowiącej tajemnicę zawodową lub jej nieuprawnione wykorzystanie. Wskazać jednocześnie należy, że ufi nie daje wprost odpowiedzi na pytanie o zakres ewentualnej szkody oraz „osoby poszkodowanego". Należy przyjąć, z uwagi na szeroką ustawową definicję samej tajemnicy zawodowej, iż odpowiedzialność, o której mowa w tym przepisie, będzie obejmować wszelkie szkody poniesione przez „podmioty dokonujące czynności związanych z działalnością funduszu lub zbiorczego portfela papierów wartościowych" (przykładowy katalog wskazano powyżej), których dotyczyły informacje objęte ujawnioną tajemnicą zawodową.

Podsumowanie. Mając na względzie omówione powyżej regulacje dotyczące tajemnicy zawodowej, należy stwierdzić, iż świadczenie na rzecz podmiotów z sektora funduszy inwestycyjnych usług z zakresu technologii informatycznych z wykorzystaniem modelu chmury jest dopuszczalne. Z uwagi na zakres pojęciowy, jaki ufi nadaje tajemnicy zawodowej, niezależnie od zakresu powierzonych czynności (kategorii usług w chmurze świadczonych na rzecz towarzystwa czy funduszu), podmioty, na których rzecz powierzenie nastąpiło lub raczej wobec brzmienia art. 280 ufi – pracownicy oraz osoby pozostające z tymi podmiotami w stosunku zlecenia lub innym stosunku cywilnoprawnym o podobnym charakterze, są zobowiązani do zachowania tajemnicy zawodowej, ze wszystkimi tego konsekwencjami (omówionymi powyżej). W praktyce zatem korzystanie przez TFI lub fundusze inwestycyjne z usług „chmury obliczeniowej" będzie wiązało się z koniecznością odpowiedniego uregulowania kwestii poufności informacji, do których w ramach świadczonych usług może mieć dostęp usługodawca, a także z odpowiedzialnością osób bezpośrednio wykonujących usługi, na zasadach przewidzianych w ustawie.

6.2 Cloud Computing w regulacjach dot. sektora funduszy emerytalnych

Regulacje sektora funduszy emerytalnych są analogiczne do opisanych powyżej regulacji dotyczących sektora funduszy inwestycyjnych. Podobnie jak ufi, ustawa z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (dalej jako „**uoiffe**") dopuszcza powierzenie przez towarzystwo wykonywania niektórych czynności związanych z funkcjonowaniem funduszu inwestycyjnego podmiotom zewnętrznym. Także uoiffe wskazuje w tym zakresie jedynie podmioty wyspecjalizowane (bank depozytariusz, czy agent transferowy czy akwizytorzy), o innych podmiotach i czynnościach milcząc. Analiza przepisów uoiffe umożliwia jednak zasadne stwierdzenie, iż istnieje możliwość powierzenia innych czynności niezbędnych do sprawnego i niezakłóconego działania funduszu emerytalnego, w tym również usługi informatycznych wykonywanych w formie cloud computingu.

Podobnie jak przy czynnościach regulowanych Prawem bankowym oraz ufi, uoiffe aiwera szczegółowe regulacje dotyczące tajemnicy zawodowej. W przypadku, gdyby w ramach świadczonych na rzecz funduszu emerytalnego usług dostawca usługi przetwarzania chmurowego miał możliwość dostępu do danych objętych tajemnicą zawodową regulacje te muszą być wzięte pod uwagę.

Na mocy art. 49 uoiffe do zachowania tajemnicy zawodowej dotyczącej działalności funduszu emerytalnego zobowiązane są przede wszystkim osoby pozostające z towarzystwem lub funduszem w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze oraz pracownicy podmiotów pozostających z towarzystwem lub funduszem takim stosunku. Postanowienie to będzie miało więc zastosowanie również do dostawcy usług cloud computingu i wszystkich jego pracowników. Tajemnica zawodowa w uoiffe uregulowana jest jednak mniej szeroko niż w ufi. Tajemnica zawodowa w rozumieniu uoiffe obejmuje bowiem „informacje związane z lokatami funduszu, rejestrem członków funduszu, rozporządzeniami członków funduszu na wypadek śmierci oraz oświadczeniami, o których mowa w art. 83 [o stosunkach majątkowych istniejących między uczestnikiem funduszu a jego małżonkiem], których ujawnienie mogłoby naruszyć interes członków funduszu lub interes uczestników obrotu na rynku regulowanym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi".

Wskazać również należy, iż uoiffe, podobnie jak ufi przewiduje odpowiedzialność za ujawnienie lub wykorzystanie informacji stanowiących tajemnicę zawodową. Zgodnie z art. 220 ust. 1 zachowanie takie podlega karze grzywny do 1.000.000 zł lub karze pozbawienia wolności do lat 3, przy czym, jeśli ujawnienie lub wykorzystanie tajemnicy zawodowej było dokonane w celu osiągnięcia korzyści majątkowej lub osobistej, osoba dopuszczająca się takiego czynu podlega grzywnie do 5.000.000 zł lub karze pozbawienia wolności do lat 5.

Podsumowanie. Mając na względzie omówione powyżej regulacje, należy stwierdzić, iż świadczenie na rzecz podmiotów z sektora funduszy emerytalnych usług z zakresu technologii informatycznych z wykorzystaniem modelu chmury jest dopuszczalne, zaś wykonywanie takich czynności powinno uwzględniać wymogi uoiffe dotyczące zachowania tajemnicy zawodowej.

6.3 Cloud Computing w regulacjach z zakresu działalności firm inwestycyjnych

Outsourcing działalności firmy inwestycyjnej. Zagadnienie outsourcingu w działalności firmy inwestycyjnej uregulowane jest w art. 81 a – 81 g ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (tekst jednolity DZ. U. 10.211.1384 ze zmianami) (dale jako „**ustawa o obrocie”**). Przepisy te zostały dodane do ustawy o obrocie 21 października 2009 r., gdy weszła w życie jej nowelizacja tej ustawy implementująca przepis dwóch dyrektyw:

- dyrektywy 2004/39/WE Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych zmieniająca dyrektywę Rady 85/611/EWG i 93/6/EWG i dyrektywę 2000/12/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 93/22/EWG oraz

- dyrektywy Komisji 2006/73/WE z dnia 10 sierpnia 2006 r. wprowadzającej środki wykonawcze do dyrektywy 2004/39/WE Parlamentu Europejskiego i Rady w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez przedsiębiorstwa inwestycyjne oraz pojęć zdefiniowanych na potrzeby tejże dyrektywy (dalej jako „**MiFID**”).

Regulacja outsourcingu w ustawie o obrocie odwołuje się do zasady swobody korzystania z usług innych przedsiębiorców przez outsorcera, przy zachowaniu odpowiedzialności outsorcera wobec jego klientów za wyrządzone szkody oraz odpowiedzialności przedsiębiorcy w stosunku do outsorcera za wyrządzone mu szkody (obu rodzajów tej odpowiedzialności nie można wyłączyć lub ograniczyć). Ponadto ustawa o obrocie wymaga zapewnienia bieżącego nadzoru outsorcera nad przedsiębiorcą i dokonywania bieżącej oceny jakości wykonywania powierzonych czynności. Ustawa o obrocie wyłącza jednak dopuszczalność przekazania prowadzenia działalności maklerskiej w sposób powodujący brak faktycznego wykonywania danej czynności z działalności maklerskiej przez firmę inwestycyjną. Podobnie, niedozwolony jest outsorcing prowadzący do przekazania reprezentowania, prowadzenia spraw lub przekazania zarządzania firmą inwestycyjną w rozumieniu przepisów Kodeksu spółek handlowych.

Warunki zawarcia umowy outsourcingowej wskazane zostały w przepisie art. 81 b ust. 1 pkt 1 – 10 ustawy o obrocie, w szczególności poprzez określenie wymogu, by przedsiębiorca, któremu powierzono czynności posiadał uprawnienia do wykonywania czynności w zakresie przedmiotu umowy (jeżeli z przepisów prawa wynika obowiązek posiadania takich uprawnień) albo zajmował się wykonywaniem tych czynności w sposób zawodowy i posiadał niezbędną wiedzę, doświadczenie oraz zapewniał warunki techniczne i organizacyjne niezbędne do prawidłowego wykonania umowy, w tym znajdował się w sytuacji finansowej zapewniającej prawidłowe wykonanie tej umowy.

Wymogi te nie dotyczą **tzw. outsourcingu nieistotnego**, tj. zgodnie z brzmieniem przepisu art. 81 f ust. 1 ustawy o obrocie, dotyczącego czynności niemających istotnego znaczenia dla prawidłowego wykonywania przez firmę inwestycyjną obowiązków określonych przepisami prawa, sytuacji finansowej firmy, ciągłości lub stabilności prowadzenia działalności maklerskiej przez firmę inwestycyjną. Ustawa o obrocie przykładowo wymienia, że z outsourcingiem nieistotnym mamy do czynienia w przypadku świadczenia na rzecz firmy inwestycyjnej usług doradztwa prawnego, szkolenia pracowników, prowadzenia ksiąg rachunkowych, ochrony osób lub mienia, usług wystandaryzowanych, w tym usług polegających na dostarczaniu informacji rynkowych lub informacji o notowaniach instrumentów finansowych.

Wypada odnotować, że wejście w życie przepisów art. 81 a – 81 g ustawy o obrocie doprowadziło do powstania dualizmu regulacyjnego w zakresie tzw. outsourcingu bankowego, który do tej pory podlegał jednolitej regulacji, określonej przepisami art. 6a-6d Prawa bankowego. Działalność banku, wypełniająca przesłanki określone w art. 69 ustawy o obrocie, z wyłączeniem wyjątków wynikających z przepisów art. 70 ust. 2 i 3 ustawy o obrocie, ma bowiem charakter działalności maklerskiej. W szczególności za działalność maklerską banku trzeba uznać przyjmowanie i przekazywanie zleceń nabycia lub zbycia instrumentów

finansowych oraz oferowanie instrumentów finansowych, jeżeli instrumenty finansowe będące przedmiotem tych czynności banku zostały dopuszczone do obrotu zorganizowanego (np. znajdujące się w obrocie zorganizowanym akcje lub certyfikaty inwestycyjne emitowane przez fundusze inwestycyjne zamknięte). W takim przypadku bank jest zobowiązany do stosowania wprost przepisów ustawy o obrocie dotyczących outsourcingu. Należy jednak zauważyć, że zgodnie z przepisem art. 70 ust. 4 ustawy o obrocie również w zakresie wyjątków wskazanych w przepisach art. 70 ust. 2 i 3 ustawy o obrocie (tj. w zakresie wykonywania czynności, o których mowa w art. 69 ust. 2 pkt 1-7 ustawy o obrocie) przepisy ustawy o obrocie dotyczące outsourcingu stosuje się do banków – w tym przypadku „odpowiednio".

Podsumowując, bank wykonując czynności wskazane w art. 69 ustawy o obrocie, podlega przepisom ustawy o obrocie regulującym outsourcing, a nie stosuje przepisów art. 6a- 6d Prawa bankowego. W doktrynie przyjmuje się, że przepisy ustawy o obrocie mają w opisanej sytuacji pierwszeństwo przed regulacją Prawa bankowego ze względu na zastosowanie powszechnie akceptowanych zasad: pierwszeństwa regulacji późniejszych przed wcześniejszymi (przepisy art. 81 a – 81 g ustawy o obrocie mają charakter „lex posterior" w stosunku do przepisów art. 6a-6d Prawa bankowego), pierwszeństwa przepisów o charakterze szczególnym wobec regulacji ogólnych (przepisy art. 81 a – 81 g ustawy o obrocie mają charakter „lex specialis" w stosunku do przepisów art. 6a-6d Prawa bankowego, gdyż normują jedynie fragment działalności banku), pełnej i efektywnej implementacji dyrektyw MiFID.

Opisany dualizm prawny prowadzi do wielu problemów ze stosowaniem przepisów, w szczególności w przypadku, gdy usługa wydzielana na zewnątrz dotyczy zarówno działalności banku, mającej charakter opisany w art. 69 ustawy o obrocie, jak i działalności innej, np. w sytuacji zlecenia usług z zakresu utrzymania systemu informatycznego, wykorzystywanego przez klientów banku zarówno do dokonywania operacji na instrumentach finansowych, jak i zakładania depozytów. W takim wypadku, w braku jednoznacznego stanowiska regulatora w tym zakresie, banki z ostrożności mogą skłaniać się do stosowania bardziej restrykcyjnego reżimu outsourcingowego, uregulowanego w Prawie bankowym.

Podsumowanie. Mając na względzie powyższe należy stwierdzić, iż świadczenie na rzecz firm inwestycyjnych usług z zakresu technologii informatycznych z wykorzystaniem modelu chmury jest dopuszczalne. Potencjalnie problematyczne może okazać się jednak zaklasyfikowanie danego zakresu usług, jako związanych lub niezwiązanych bezpośrednio z działalnością maklerską. Powierzenie tych ostatnich czynności, niezależnie od modelu świadczenia na rzecz firmy inwestycyjnej usług (więc także w ramach cloud computing'u) objęte będzie reżimem outsourcingu wynikającym z ustawy o obrocie. Dotyczyć to będzie również banków - w zakresie, w jakim czynności mające być przedmiotem powierzenia podlegają regulacjom ustawy o obrocie.

6.4 Cloud Computing w działalności ubezpieczeniowej

Podobnie jak w zakresie działalności bankowej, działalności firm inwestycyjnych i działalności funduszy inwestycyjnych, omówienia wymaga zakres tajemnicy ubezpieczeniowej i prawne rygory outsourcingu w działalności zakładów ubezpieczeń (dla przejrzystości wywodów pomijamy specyfikę działalności zakładów reasekuracji).

a) Tajemnica ubezpieczeniowa

Zgodnie z art. 19 ust. 1 ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz.U.10.11.66) (dalej jako **„udu"**) *zakład ubezpieczeń i osoby w nim zatrudnione lub osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia.*

Udu nie posługuje się przyjmowanym powszechnie terminem „tajemnica ubezpieczeniowa", a obowiązku zachowania tajemnicy nie odnosi do czynności ubezpieczeniowych (tak jak czyni to art. 104 ust. 1 Prawa bankowego, odnosząc obowiązek zachowania tajemnicy nazwanej „tajemnicą bankową" do „wszystkich informacji dotyczących czynności bankowej, uzyskanych w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje"). Przyjmuje się w wyniku wykładni

celowościowej, że pomimo, iż w art. 19 ust. 1 udu mówi się o „zachowaniu tajemnicy dotyczącej poszczególnych umów ubezpieczenia", to tajemnica ubezpieczeniowa ma szerszy zakres i obejmuje:

- informacje dotyczące zawarcia umowy ubezpieczenia z danym ubezpieczającym,
- wszelkie informacje stanowiące treść zawartej umowy ubezpieczenia,
- informacje pozyskane przez zakład ubezpieczeń samodzielnie lub od ubezpieczającego w związku z zawartą umową ubezpieczenia (także w toku jej wykonywania),
- informacje pozyskane przez zakład ubezpieczeń od potencjalnych kontrahentów w związku z zawieraniem przez zakład ubezpieczeń umów ubezpieczenia, choćby w danym przypadku do zawarcia umowy ubezpieczenia nie doszło (zdaniem niektórych, ten przypadek nie znajduje jednak podstawy prawnej de lege lata, lecz powinien być postulowany de lege ferenda).

Ustawa o działalności ubezpieczeniowej nie zawiera analogicznego do zawartego w prawie bankowym przepisu dopuszczającego udostępnianie informacji objętych tajemnicą ubezpieczeniową na podstawie zgody udzielonej zakładowi ubezpieczeń przez podmiot, którego te informacje dotyczą. Pomimo to można twierdzić, że jest to dopuszczalne. Wskazuje na to m. in. stanowisko Trybunału Konstytucyjnego wyrażone w wyroku z dnia 20 listopada 2002 roku (K 41/02), w myśl którego istota „zasady autonomii informacyjnej" sprowadza się do pozostawienia każdej osobie swobody w określeniu sfery dostępności dla innych wiedzy o sobie. Źródła uprawnienia do wyrażenia zgody na ujawnienie informacji objętych tajemnicą ubezpieczeniową można poszukiwać również w konstrukcji dóbr osobistych, w szczególności prawa do prywatności, przyjmuje się bowiem, że zgoda uprawnionego uchyla bezprawność naruszenia dobra osobistego. Takie argumenty nie usuwają jednak do końca wątpliwości co do znaczenia zgody beneficjenta tajemnicy ubezpieczeniowej na udostępnienie osobom trzecim informacji objętych tajemnicą jako przesłanki legalizującej takie działanie zakładu ubezpieczeń.

Przy interpretowaniu ustawowego kręgu podmiotów zobowiązanych do zachowania tajemnicy ubezpieczeniowej, zwłaszcza co do osób zatrudnionych w zakładzie ubezpieczeń, aktualne pozostają przedstawione wcześniej uwagi dotyczące ustawowego określenia w prawie bankowym podmiotów zobowiązanych do zachowania tajemnicy bankowej.

W art. 19 ust. 2 został określony krąg podmiotów, którym na ich wniosek zakład ubezpieczeń może (a w niektórych przypadkach, jak należy rozumieć, jest zobowiązany) udzielać informacji objętych tajemnicą ubezpieczeniową. Pomijając organy państwowe, uprawnione do żądania takich informacji od zakładu ubezpieczeń w ustawowo określonym zakresie, „podmioty sektorowe" wskazane z nazwy – w zakresie przypisanych im ustawowo kompetencji, oraz inne zakłady ubezpieczeń i zakłady reasekuracji w celach ustawowo sprecyzowanych, a także osoby uczestniczące w danym stosunku ubezpieczenia (to jest ubezpieczającego, ubezpieczonego, uposażonego, uprawnionego), wśród podmiotów, którym zakład ubezpieczeń może udzielić informacji objętych tajemnicą ubezpieczeniową, przepis ten wskazuje:

- podmioty przetwarzające, na zlecenie zakładu ubezpieczeń, dane dotyczące ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umów ubezpieczenia oraz podmioty administrujące indywidualnymi kontami jednostek uczestnictwa w ubezpieczeniowym funduszu kapitałowym (art. 19 ust. 2 pkt 23). Należy uznać, że dostawca chmury mieści się właśnie w tej kategorii.

Zgodnie z art. 19 ust. 3, „przetwarzanie danych oraz wykonywanie czynności przez podmioty, o których mowa w ust. 2 pkt 23 i 24, nie ogranicza odpowiedzialności wynikającej z zakazu, o którym mowa w ust. 1". Jest to nieprecyzyjne sformułowanie - brak wskazania, o jaki rodzaj prawnej odpowiedzialności i o czyją odpowiedzialność chodzi. Zapewne ma ono oznaczać, że pomimo prawnie dopuszczalnego udostępnienia wskazanym podmiotom informacji chronionych tajemnicą ubezpieczeniową za ewentualne szkody wynikłe z tego faktu dla osoby, której te informacje dotyczą, będzie odpowiadał zakład ubezpieczeń. Jeżeli bowiem chodzi o odpowiedzialność karną, to przepis art. 19 ust. 3 nie może mieć do niej zastosowania. Art. 232 udu nie pozostawia wątpliwości, że przestępstwo ujawnienia lub wykorzystania informacji stanowiących tajemnicę ubezpieczeniową może być popełnione przez każdego, kto jest zobowiązany do zachowania tajemnicy ubezpieczeniowej (zagrożenie karą grzywny lub karą pozbawienia wolności do lat 3, a jeżeli czyn

miał na celu osiągnięcie korzyści majątkowej lub osobistej – do lat 5). Wśród zobowiązanych do zachowania tajemnicy ubezpieczeniowej są zaś także „osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe" (art. 19 ust. 1).

Ustawowe wskazanie podmiotów wymienionych w art. 19 ust. 2 pkt. 23 i 24 jako uprawnionych do pozyskiwania od zakładu ubezpieczeń informacji objętych tajemnicą ubezpieczeniową ściśle wiąże się z kwestią outsourcingu w działalności zakładu ubezpieczeń.

b) Outsourcing w działalności zakładu ubezpieczeń

Regulacja outsourcingu jest w udu mało przejrzysta w zakresie określenia czynności, jakie mogą być zlecane zewnętrznym usługodawcom. Jest to jednocześnie regulacja znacznie ogólniejsza i bardziej liberalna niż zawarta w Prawie bankowym dla outsourcingu w działalności bankowej.

Udu wskazuje, że outsourcing działalności zakładu ubezpieczeń, jeżeli pominąć działanie przez uprawnionych pośredników ubezpieczeniowych zgodnie z ustawą z dnia 22 maja 2003 r. o pośrednictwie ubezpieczeniowym, może polegać na zleceniu przez zakład ubezpieczeń:

1) na podstawie wnioskowania z art. 19 ust. 2 pkt 23 – czynności przetwarzania danych dotyczących ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umów ubezpieczenia oraz administrowania indywidualnymi kontami jednostek uczestnictwa w ubezpieczeniowym funduszu kapitałowym;

2) na podstawie art. 26 ust. 1 zd. 2 – usług związanych z zabezpieczeniem dokumentów dotyczących zawierania i wykonywania umów ubezpieczenia, sporządzonych na informatycznych nośnikach danych.

a nadto (co dla cloud computingu nie wydaje już się istotne):

3) na podstawie art. 3 ust. 6 - czynności ubezpieczeniowych, o których mowa w art. 3 ust. 4 pkt 1 - 6 oraz ust. 5, to jest:

- oceny ryzyka w ubezpieczeniach osobowych i ubezpieczeniach majątkowych oraz w umowach gwarancji ubezpieczeniowych,
- wypłacania odszkodowań i innych świadczeń należnych z tytułu umów ubezpieczenia i umów gwarancji ubezpieczeniowych,
- przejmowania i zbywania przedmiotów lub praw nabytych przez zakład ubezpieczeń w związku z wykonywaniem umowy ubezpieczenia lub umowy gwarancji ubezpieczeniowej,
- prowadzenia kontroli przestrzegania przez ubezpieczających lub ubezpieczonych, zastrzeżonych w umowie lub w ogólnych warunkach ubezpieczeń, obowiązków i zasad bezpieczeństwa odnoszących się do przedmiotów objętych ochroną ubezpieczeniową,
- prowadzenia postępowań regresowych oraz postępowań windykacyjnych związanych z wykonywaniem umów ubezpieczenia i umów gwarancji ubezpieczeniowych,
- lokowania środków zakładu ubezpieczeń,
- ustalania przyczyn i okoliczności zdarzeń losowych,
- ustalania wysokości szkód oraz rozmiaru odszkodowań oraz innych świadczeń należnych uprawnionym z umów ubezpieczenia lub umów gwarancji ubezpieczeniowych,
- ustalania wartości przedmiotu ubezpieczenia,

- zapobiegania powstawaniu albo zmniejszania skutków wypadków ubezpieczeniowych lub finansowania tych działań z funduszu prewencyjnego;

4) na podstawie art. 3 ust. 9 - czynności, o których mowa w art. 3 ust. 3 pkt 2, to jest składania oświadczeń woli w sprawach roszczeń o odszkodowania lub inne świadczenia należne z tytułu umów ubezpieczenia i umów gwarancji ubezpieczeniowych;

Udu milczy o innych czynnościach, jakie zakład ubezpieczeń może zlecać podmiotom zewnętrznym w ramach outsourcingu. Należy to rozumieć w ten sposób, że skoro zakład ubezpieczeń może prowadzić jedynie działalność ubezpieczeniową rozumianą jako „wykonywanie czynności ubezpieczeniowych związanych z oferowaniem i udzielaniem ochrony na wypadek ryzyka wystąpienia skutków zdarzeń losowych" (art. 3 ust. 1), oraz działalność „bezpośrednio związaną" z działalnością ubezpieczeniową (art. 3 ust. 2), a udu nie zawiera wyraźnego ograniczenia dopuszczalności outsourcingu w zakresie działalności bezpośrednio związanej z działalnością ubezpieczeniową, to taka działalność może być przez zakład ubezpieczeń zlecana w ramach outsourcingu usługodawcom zewnętrznym. W ramach takiej działalności mieści się np. reklama, marketing oraz IT dla działalności ubezpieczeniowej.

Zgodnie z art. 30 ust. 1 udu zarząd zakładu ubezpieczeń „odpowiada za opracowanie, wprowadzenie i funkcjonowanie regulacji wewnętrznych określających sposób wykonywania działalności ubezpieczeniowej, w szczególności w zakresie czynności zleconych innym podmiotom /.../".

Organ nadzoru może nakazać zakładowi ubezpieczeń rozwiązanie w wyznaczonym terminie umowy, na podstawie której zlecono wykonywanie czynności ubezpieczeniowych innemu podmiotowi, w przypadku stwierdzenia, że wykonywanie czynności odbywa się z naruszeniem prawa, wpływa niekorzystnie na wykonywanie działalności ubezpieczeniowej przez zakład ubezpieczeń zgodnie z przepisami prawa, na ostrożne i stabilne zarządzanie zakładem ubezpieczeń lub na interesy ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umów ubezpieczenia (art. 210 ust. 1). W takim przypadku nie stosuje się przewidzianych w umowie outsourcingowej ograniczeń w zakresie możliwości i terminów jej rozwiązywania lub wypowiadania (art. 210 ust. 2). W przypadku nierozwiązania umowy w wyznaczonym terminie organ nadzoru może na podstawie art. 210 ust 3 nałożyć kary pieniężne, o których mowa w art. 212 ust. 1 pkt 1 i 2, to jest:

- na członków zarządu lub prokurentów zakładu ubezpieczeń kary pieniężne do wysokości odpowiadającej trzykrotnemu przeciętnemu miesięcznemu wynagrodzeniu z ostatnich 12 miesięcy;

- na zakład ubezpieczeń kary pieniężne do wysokości 0,5 % składki przypisanej brutto uzyskanej przez zakład ubezpieczeń w roku poprzednim, a w przypadku gdy zakład ubezpieczeń nie prowadził działalności lub miał zbiór składki przypisanej poniżej 20 mln złotych - do wysokości 100.000 złotych.

c) Spodziewane zmiany w ustawie o działalności ubezpieczeniowej

W interesującym nas zakresie zmiany wymusi konieczność implementowania do krajowego porządku prawnego przepisów dyrektywy 2009/138/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. w sprawie podejmowania i wykonywania działalności ubezpieczeniowej i reasekuracyjnej – Wypłacalność II (Dz. Urz. UE L 335 z 17.12.2009, s.1). Zgodnie z art. 309 ust. 1 dyrektywy państwa członkowskie muszą dokonać transpozycji jej wskazanych w tym artykule postanowień (w tym dotyczących outsourcingu) do dnia 31 października 2012 roku.

Istotnych zmian w ustawie o działalności ubezpieczeniowej można się spodziewać w zakresie outsourcingu, obecnie w udu uregulowanego wyrywkowo i niespójnie.

Przede wszystkim, dyrektywa wprowadza definicję, w myśl której „outsourcing oznacza dowolnego rodzaju umowę między zakładem ubezpieczeń lub zakładem reasekuracji a dostawcą usług, będącym jednostką nadzorowaną lub nie, na podstawie której dostawca – bezpośrednio bądź w drodze suboutsourcingu – wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez sam zakład ubezpieczeń lub zakład reasekuracji" (art. 13 pkt 28). Można spodziewać się przeniesienia tej definicji do udu.

Zgodnie z punktem 37 preambuły dyrektywy, organy nadzoru powinny być informowane przed dokonaniem przez zakład ubezpieczeń outsourcingu podstawowych lub istotnych funkcji lub rodzajów działalności i konieczne jest, aby organy nadzoru miały prawo pełnej kontroli zleceniobiorcy w zakresie wykonywania przezeń zleconych mu czynności. Wymogi dla outsourcingu ubezpieczeniowego powinny zaś odpowiadać „aktualnym regulacjom i praktykom w sektorze bankowym,"

Zgodnie z art. 38 dyrektywy, państwa członkowskie mają zapewnić, aby zakłady ubezpieczeń podejmowały działania niezbędne do zapewnienia spełnienia następujących warunków:

- dostawca usług musi współpracować z organami sprawującymi nadzór nad zakładem ubezpieczeń w związku z funkcją lub działaniem zleconym w ramach outsourcingu;
- zakłady ubezpieczeń, ich biegli rewidenci i organy nadzoru muszą posiadać faktyczny dostęp do danych związanych z funkcjami lub działaniami zlecanymi w drodze outsourcingu;
- organy nadzoru muszą posiadać rzeczywisty dostęp do lokali dostawcy usług i muszą być w stanie egzekwować te prawa dostępu.

W przypadkach outsourcingu wykonywanego przez zleceniobiorcę z państwa członkowskiego innego niż to, w którym ma siedzibę zakład ubezpieczeń, państwo członkowskie, w którym umiejscowiony jest dostawca usług, zezwala organom sprawującym nadzór nad zakładem ubezpieczeń na przeprowadzenie samodzielnie lub za pośrednictwem osób, które wyznaczają do tego celu, kontroli na miejscu w lokalu dostawcy usług. Organy nadzoru państwa członkowskiego siedziby zakładu ubezpieczeń mogą powierzyć zadanie przeprowadzenia takich kontroli na miejscu organom nadzoru państwa członkowskiego, w którym umiejscowiony jest dostawca usług.

Zgodnie z art. 49 dyrektywy, outsourcing podstawowych lub ważnych funkcji lub czynności operacyjnych nie może odbywać się w sposób prowadzący do:

- istotnego pogorszenia jakości systemu zarządzania danego zakładu;
- nadmiernego zwiększenia ryzyka operacyjnego;
- pogorszenia możliwości monitorowania przez organ nadzoru przestrzegania przez zakład jego obowiązków;
- pogorszenia w zakresie świadczenia ciągłych i zadowalających usług ubezpieczającym,

a zakłady ubezpieczeń informują organy nadzoru z odpowiednim wyprzedzeniem o outsourcingu podstawowych lub ważnych funkcji lub czynności oraz o wszelkich późniejszych istotnych zmianach w odniesieniu do tych funkcji lub czynności.

Biorąc pod uwagę powyższe zapisy dyrektywy, w tym zapisany w punkcie 37 preambuły wyraźny postulat poddania outsourcingu ubezpieczeniowego rygorom outsourcingu bankowego, można być pewnym rychłego doregulowania outsourcingu w ustawie o działalności ubezpieczeniowej w kierunku przyjętym w prawie bankowym.

Cloud Computing w Regulacjach dot. Informacji Niejawnych (Tajemnica Państwowa)

7. Cloud Computing w Regulacjach dot. Informacji Niejawnych (Tajemnica Państwowa)

Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.10.182.1228) (dalej jako „**uoin**”) określa podstawowe zasady ochrony informacji niejawnych.

Jako informację niejawną ustawa definiuje w art. 1 wszelkie informacje, których nieuprawnione ujawnienie spowodowałoby lub mogło spowodować szkody dla Rzeczpospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od sposobu i formy ich wyrażenia.

Z punktu widzenia cloud computingu istotne jest, iż przepisy ustawy mają zastosowanie do przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych (art. 1 ust. 2 pkt 6 uoin). W tym zakresie istotne są zasady (i) przetwarzania informacji niejawnych (art. 1 ust. 1 pkt 3 uoin); (ii) postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych (art. 1 ust. 1 pkt 5 uoin); (iii) organizacji kontroli stanu zabezpieczenia informacji niejawnych (art. 1 ust. 1 pkt 6 uoin); (iv) ochrony informacji niejawnych w systemach teleinformatycznych (art. 1 ust. 1 pkt 7 uoin); (v) stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych (art. 1 ust. 1 pkt 7 uoin).

Przez termin przetwarzanie informacji niejawnych ustawodawca rozumie wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie (art. 2 pkt 5 uoin). Jednocześnie uoin w zakresie systemu teleinformatycznego odsyła do ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2002.144.1204)(dalej „usude”) określającej, że systemem teleinformatycznym jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego. Dane, którym została nadana określona klauzula tajności („ściśle tajne”, „tajne”, „poufne”, „zastrzeżone”) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie zgodnie z przepisami określającymi wymagania dot. bezpieczeństwa systemów teleinformatycznych.

Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego. Takiej akredytacji udziela Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego na okres nie dłuższy niż 5 lat dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne”, „tajne” lub „ściśle tajne”. Potwierdzeniem takiej akredytacji jest uzyskanie świadectwa akredytacji systemu teleinformatycznego (wydawane na podstawie m.in. przeprowadzonego audytu systemu).

Samym natomiast warunkiem dopuszczenia przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów jest zdolność do ochrony informacji niejawnych potwierdzana świadectwem bezpieczeństwa przemysłowego.

Cloud Computing w Rachunkowości

8. Cloud Computing w Rachunkowości

Ustawa z 29 września 1994 r. o rachunkowości (Dz.U.09.152.1223) określa podstawowe zasady rachunkowości, tryb badania sprawozdań finansowych przez biegłych rewidentów oraz zasady wykonywania działalności w zakresie usługowego prowadzenia ksiąg rachunkowych, co z punktu dostawców usług w chmurze wydaje się być najbardziej znaczące.

Ustawa nie przewiduje bezpośrednio żadnych regulacji mogących mieć zastosowanie do cloud computingu. Jednak bazując na niektórych normach w niej zawartych można określić kierunek, w którym powinien pójść dostawca usług w chmurze. Akt ten akcentuje przede wszystkim ciągłość działania oraz zapewnienie bezpieczeństwa informacji.

Ciągłość działania

Zgodnie z ustawą przy elektronicznym prowadzeniu ksiąg rachunkowych za równoważne z takimi księgami uważa się odpowiednio zasoby informacyjne rachunkowości. Muszą one być zorganizowane w formie (i) oddzielnych komputerowych zbiorów danych, (ii) baz danych lub wyodrębnionych ich części - bez względu na miejsce ich powstania i przechowywania.

Warunkiem możliwości prowadzenia tego rodzaju rachunkowości jest posiadanie przez dany podmiot oprogramowania umożliwiającego uzyskiwanie czytelnych informacji w odniesieniu do zapisów dokonanych w takich księgach. Ustawodawca wymaga również, aby przy tego rodzaju prowadzeniu ksiąg stosować właściwe procedury i środki chroniące przed zniszczeniem, modyfikacją lub ukryciem zapisu. Zatem chodzi i tutaj o bezpieczeństwo informacji.

Bezpieczeństwo informacji

Księgi rachunkowe mogą mieć formę zbiorów utrwalonych na informatycznych nośnikach danych pod warunkiem, że dostawca usług w chmurze będzie w tym zakresie stosować (i) odporne na zagrożenia nośniki danych, (ii) stosowne środki ochrony zewnętrznej, (iii) systematyczne tworzenie rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych. Ponadto dostawca musi zapewnić (i) trwałość zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych oraz (ii) zapewnić ochronę programów komputerowych i danych systemu informatycznego rachunkowości poprzez stosowanie odpowiednich rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem.

Powyższe wymagania powinna spełniać oczywiście usługa dostawcy chmury, jeśli obejmuje ona systemy księgowe. Wymagania te nie wykraczają jednak, jak widać, poza standardowe wymagania dotyczące bezpieczeństwa informacji, bardziej szczegółowo definiowane przez inne przepisy, jak na przykład przepisy o ochronie danych osobowych.

Regulacje w Zakresie Cloud Computingu w Poszczególnych Państwach Unii Europejskiej

9. Regulacje w Zakresie Cloud Computingu w Poszczególnych Państwach Unii Europejskiej

Poniżej przedstawiamy wyniki krótkiej sondy dotyczącej regulacji cloud computingu w zakresie ochrony danych osobowych i sektorze finansowym w niektórych państwach Unii Europejskiej.

9.1 Ochrona danych osobowych

Państwo	Regulacje istotne dla cloud computingu
Belgia	Nic nie wiadomo o żadnych zmianach, która miałyby powstrzymać rozwój usług w ramach cloud computing.
Czechy	Nie wiadomo nic o żadnych zmianiach, która miałaby powstrzymać rozwój usług w ramach cloud computing. W czeskim prawie, dostawcy usług najprawdopodobniej będą uznani za przetwarzających dane, natomiast będzie to w dużej mierze zależało od charakteru świadczonych usług.
Finlandia	Brak specjalnych zasad, które uniemożliwiałby korzystanie/świadczenie usług w ramach cloud computing w Finlandii. Jednakże, szczególnie w kontekście podmiotów publicznych, mogą występować regulacje, dotyczące ograniczeń ze względów bezpieczeństwa, które mogą mieć skutek ograniczający.
Francja	Według ustawy o ochronie danych we Francji, podmioty muszą precyzyjnie określić kraje trzecie, do których mają być transferowane dane w celu uzyskania autoryzacji francuskich organów ochrony danych. Warto zauważyć, że z raportu francuskiego Zgromadzenia Narodowego z 22 czerwca 2011 roku ("Rapport d'information sur les droits de l'individu dans la révolution numérique") wynika sugestia opracowania nowych regulacji, gdzie narzędzia cloud computing umiejscowione poza UE byłyby wyłączone z przetwarzania wrażliwych danych. Obecnie jednak nie ma żadnych przesłanek wskazujących, że taka regulacja wejdzie w życie.
Hiszpania	Brak informacji o specjalnych ograniczeniach uniemożliwiających korzystanie czy świadczenie usług w ramach cloud computing. W większości przypadków, hiszpańscy dostawcy rozwiązań cloud computing będą określani jako „przetwarzający dane".
Holandia	Zgodnie z holenderską ustawą o ochronie danych, aby uzyskać odpowiednie pozwolenie podmioty muszą określić precyzyjnie państwa trzecie, do których dane będą transferowane, by móc uzyskać pozwolenie.
Niemcy	W prawie niemieckim dostawcy usług w ramach cloud computing są uznawani za uprawnionych do przetwarzania danych. Zarówno rygorystyczne (niemożliwe do zastosowania w praktyce) wymagania dot. umów przetwarzania danych jak i szczególna opinia niemieckiego organu ochrony danych dot. Safe Harbor, są ważnymi problemami w kwestii cloud computing. Istnieją nawet opinie niemieckich organów państwowych stwierdzające, iż cloud computing (w szczególności w "chmurach" spoza UE i EOG) w ogóle nie jest zgodny z niemieckim prawem.

Słowacja	W słowackim prawie nie ma ograniczeń dla prywatnego sektora w sferze korzystania/świadczenia usług w ramach cloud computing wewnątrz UE. Jednakże organy państwowe mogą mieć problemy z korzystaniem z usług cloud computing świadczonych z innych krajów w odniesieniu do informacji niejawnych.
Szwecja	Brak specjalnych zasad, które uniemożliwiałby korzystanie/świadczenie usług w ramach cloud computing w Szwecji. Jednakże (szczególnie w kontekście podmiotów publicznych) mogą występować regulacje, dotyczące ograniczeń ze względów bezpieczeństwa, które mogą mieć taki skutek.
Węgry	Na Węgrzech nie wiadomo nic o żadnych specjalnych regulacjach, które miałyby uniemożliwiać korzystanie/dostarczanie usług w ramach cloud computing. Węgierski Parlament uchwalił w lipcu nową ustawę o ochronie danych (będzie obowiązywała od 1 stycznia 2012 r.), ale nie zawiera ona żadnych specjalnych regulacji dotyczących cloud computing.
Włochy	Włoski organ ochrony danych osobowych wydał ogólną Rezolucję, opublikowaną w Dzienniku Urzędowym nr 153 z 4 lipca 2011 roku, która przedstawia nowe zasady powoływania podmiotów uprawnionych do przetwarzania danych przez przedsiębiorstwa, które powierzają dane zewnętrznym agencjom. Według Rezolucji, przedsiębiorstwa, które zlecają pracę zewnętrznym podmiotom, ale "zachowują operacyjną kontrolę" -muszą formalnie mianować te agencje „przetwarzającymi dane".
Wielka Brytania	Brak specjalnych regulacji uniemożliwiających świadczenie usług w ramach cloud computing w Wielkiej Brytanii. Stosuje się wszystkie zwykłe reguły (należy oszacować i stosować środki bezpieczeństwa, transfery danych itp.).

9.2 Sektor finansowy

Wielka Brytania

W Wielkiej Brytanii regulatorem rynku usług finansowych jest Financial Services Autorithy (FSA). W zakresie cloud computingu istotne znaczenie ma FSA Handbook (materiał pomocniczy wydany przez FSA) określający podstawowe regulacje i wytyczne obowiązujące instytucje finansowe działające na terenie Wielkiej Brytanii.

Poza FSA Handbook istnieje również MiFID Connect – jest to wspólny projekt różnych organizacji handlowych mający na celu wsparcie Wielkiej Brytanii w implementacji Dyrektywy w sprawie rynków instrumentów finansowych (Market in Financial Instruments Directive). Wiele wskazówek znajdujących się w tym dokumencie, mimo że nie obowiązującym powszechnie, jest stosowanych przez firmy z sektora oraz brane pod uwagę przez FSA w kontekście jej nadzoru nad podmiotami.

Branża płatnicza wdraża też globalnie standardy opracowywane przez PCI Security Standards Council. PCI Security Standards Council jest podmiotem zarządzanym przez 5 największych firm branży płatniczej (American Express, Discovery Financial Services, JCB International, MasterCard Worldwide, Visa Inc), który wyznacza standardy bezpieczeństwa dla banków i podmiotów handlowych korzystających z płatności kartami.

Poniżej zestawienie wymogów z ww. dokumentów, które mają zastosowanie do regulacji dot. cloud computingu w Wielkiej Brytanii.

Regulacja/ Standard	Wymogi	Cloud computing
FSA Handbook	FSA Handbook określa 11 zasad, które fimy są zobligowane wdrożyć: Zasada 2 stanowi, że *firma musi wykonywać swoje działania z należną dbałością i starannością.* Zasada 3 stanowi, że *firma musi z należytą starannością organizować i kontrolować swoje działania uwzględniając odpowiednie systemy zarządzania ryzykiem.* Zasada 5 stanowi *firma musi stosować się do odpowiednich standardów zachowania rynkowego.* Zasada 6 stanowi *firma musi płacić odpowiednie należności stosownie do interesu jej klientów oraz traktować ich uczciwie.*	Firmy z sektora finansowe muszą brać te zasady pod uwagę w momencie decydowania o przejściu do chmury oraz określić czy dany dostawca bądź usługa będą odpowiednie w kontekście tych regulacji. Żadna decyzja w zakresie chmury nie może skutkować naruszeniem kontroli wymaganej na mocy Zasady 3. Wszelkie finansowe korzyści dotyczące chmury muszą by równoważone z ewentualnym ryzykiem dla danych klientów.
	FSA Handbook przewiduje także zestaw zaasd działania, systemów i kontroli wyższego managementu – Senior Managment Arrangments System and Controls (Sysce). Wiele z nich ma wpływ na świadczenia ze stron firm z branży IT, np.: SYSC 4.1.1R stanowi, że *firma musi mieć odpowiednie ustalenia w zakresie zarządzania, które zawierają jasną strukturę organizacyjną z odpowiednio zdefiniowanym oraz transparentnym i konsekwentnym zakresem odpowiedzialności, efektywnym procesem identyfikacji, zarządzania, monitorowania i raportowania ryzyk bądź możliwości ich zaistnienia a także wewnętrznymi mechanizmami kontroli włączając w to logiczną organizację i procedury księgowe a także efektywną kontrolę i postanowienia dot. zabezpieczeń oraz systemów przetwarzania informacji.* SYSC 6.2.1. wymaga regulacji wewnętrznych firm, w których znajdują się odpowiednie i proporcjonalne mechanizmy oraz postanowienia zapewniające system kontroli wewnętrznej, który jest w stanie rewidować i szacować adekwatność oraz efektywność systemów firmowych.	Usługi w chmurze często obejmują transfer kontroli nad danymi do dostawcy. Może to być sprzeczne z SYSC 4.1.1R. Wiele podmiotów świadczących usługi w chmurze nie pozwala na audyty klienckie. Jest to trudne do pogodzenia z postanowieniami SYSC 6,2,1. lub punkt 9 SYSC 8.1.8R. Skorzystanie z usług podmiotu trzeciego w większości przypadków wypełni definicję outsourcingu z SYSC 8.1. Jeżeli jest to outsourcing usług istotnych dla firm z sektora finansowego – będą musiały one spełnić wszystkie wymagania SYSC 8.1.8R. Największe wyzwanie w kontekście cloud computingu stanowić mogą punkty 2,3,8,9 and 11.

	SYSC 8.1.8R wymaga od firm dokonujących outsourcingu w zakresie swoich istotnych bądź krytycznych zadań zapewnienia, że: 1) dostawca systemu musi mieć możliwość, wydajność oraz wszelkie uprawnienia wymagane przez prawo do świadczenia niezawodnych i profesjonalnych usług outsourcingowych; 2) dostawca musi świadczyć usługi outsourcingowe efektywnie a firma korzystająca z usług jest zobowiązana ustanowić metody oceny standardów działania dostawcy; 3) dostawca ma obowiązek nadzoru w zakresie dokonywanego przez siebie outsourcingu oraz odpowiedniego zarządzania ryzykiem powiązanym z outsourcingiem; 4) odpowiednie działania muszą zostać podjęte w razie, gdyby okazało się, że dostawca nie działa w zakresie nałożonych na niego obowiązków świadczenia usług outsourcingowych efektywnie oraz stosownie do regulacji prawnych i wymagań regulatorów; 5) firma musi utrzymywać odpowiednie umiejętności celem sprawowania efektywnego nadzoru nad zleconym outsourcingiem oraz zarządzać ryzykiem powiązanym z outsourcingiem a także nadzorowi te umiejętności; 6) dostawca ma obowiązek ujawniania firmie wszelkich wydarzeń mogących mieć istotny wpływ na możliwość efektywnego oraz zgodnego z prawem i wymaganiami regulatora świadczenia przez niego usług outsourcingowych; 7) firma musi mieć możliwość wypowiedzenia umowy	

	outsourcingowego za każdym razem, gdy jest to konieczne bez szkody dla możliwości kontynuowania i jakości usług świadczonych względem klientów; 8) dostawca ma obowiązek współpracować w zakresie działań powiązanych z outsourcingiem z FSA a także każdym innym odpowiednim organem; 9) firma, jej audytorzy, FSA a także każdy inny kompetentny organ musi mieć możliwość odpowiedniego dostępu do danych powiązanych z działaniami outsourcingowymi a także pomieszczeń dostawcy; FSA oraz każdy odpowiedni organ muszą mieć zapewnioną możliwość wykonywania prawa dostępu; 10) dostawca ma obowiązek ochrony jakichkolwiek informacji poufnych powiązanych z firmą lub jej klientami; 11) firma oraz dostawca muszą stworzyć, implementować oraz utrzymywać plan awaryjny dla krytycznej infrastruktury technicznej a także dokonywać okresowego testowania systemów w zakresie kopii bezpieczeństwa mając na względzie funkcje oraz działania powiązane z outsourcingiem; SYSC.13.7 wyznacza podobne zasady w zakresie outsourcingu dla sektora ubezpieczeniowego. [Uwaga: FSA Handbook definiuje „Outsourcing" dla celów SYSC8 jako *porozumienie w każdej formie pomiędzy firmą i dostawcą na mocy którego dostawca dokonuje procesu, świadczy usługę lub inny rodzaj działalności, który w innym wypadku wykonany byłby przez firmę samodzielnie.]*	
Wskazówki z MiFID Connect	Wskazówki MiFID Connect w zakresie outsourcingu odwołuje się do SYSC 8 i proponuje stosowanie się do niektórych	Te wskazówki powinny być modyfikowane i stosowane odpowiednio przez każdą firmę z sektora finansowego działającą w

	wynikających z niego reguł.	ramach cloud computingu. Niektóre wskazówki są niemożliwe do zastosowania w kontekście cloud computingu jako usługi znacznie bardziej rozbudowanej względem outsourcingu. Problematyczne może być np. zgoda na ilościowy oraz jakościowy zakres świadczonych usług a także ich wartość, odbywanie regularnych spotkań z dostawcą etc.
Brytyjska Ustawa o Ochronie Danych z 1998 r.	Ustawa o Ochronie Danych implementuje postanowienia Dyrektywy o Ochronie Danych (95/46/EC) w Wielkiej Brytanii. Zasada 2 wymaga, aby *dane osobowe były pozyskiwane tylko dla jednego lub więcej wyszczególnionych i zgodnych z prawem celów i nie powinny być przetwarzane inna metodą niezgodną z tym celem lub celami.* Zasada 7 wymaga, aby *odpowiednie techniczne oraz organizacyjne środki były podjęte przeciwko nieautoryzowanemu i niezgodnemu z prawem przetwarzaniu danych osobowych a także przeciwko przypadkowej ich utracie albo zniszczeniu lub naruszeniu tych danych.* Zasada 8 wymaga, aby *dane osobowe nie były transferowane do kraju lub terytorium pozostającym poza EOG, chyba że kraj ten lub terytorium zapewnia adekwatny poziom ochrony praw i obowiązków powiązanych z danym w zakresie przetwarzania danych osobowych.*	Jakikolwiek transfer danych do kraju trzeciego wymaga zgody klienta, zwłaszcza jeżeli dane mają być gromadzone poza terytorim EOG. Do większości usług w chmurze klienci nie otrzymują odpowiedniego dostępu oraz informacji określających czy dostawca posiada odpowiednie techniczne oraz organizacyjne zabezpieczenia.
PCI Data Security Standard (DSS) – Standard ochrony danych PCI	PCI DSS jest złożonym standardem w zakresie bezpieczeństwa zawierającym wymagania odnośnie zarządzania bezpieczeństwem, odpowiednie polityki, procedury, architekturę sieci, projekt oprogramowania a także inne środki ochrony krytycznej. Podstawowym celem tego standardu jest pomoc w organizacji proaktywnej polityki ochrony danych finansowych klientów.	Firmy z sektora finansowego będą musiał zapewnić względem każdej znaczącej aplikacji użytkowanej w chmurze zapewnienie spełnienia standardów wymaganych na mocy PCI DSS celem możliwości dalszego zapewniania usług płatności kartą.
BS 7858:2006	Ten standard brytyjski określa rekomendacje co do weryfikacji osób fizycznych, które mają zostać zatrudnione w środowisku, gdzie bezpieczeństwo osób, dóbr lub mienia jest wymagane dla	Często nie jest wiadome, czy i w jakim zakresie dostawcy chmury dokonują weryfikacji swoich pracowników.

	operacji dokonywanych przez pracodawcę lub gdzie taka kontrola jest w interesie publicznym.	
ISO27001 / ISO27002	Te standardy dotyczące bezpieczeństwa informacji opisano we wcześniejszej części niniejszego opracowania	W przypadku braku uprawnienia do bezpośredniego audytu dostawcy chmury, odbiorcy chmury często opierają się na tym, że dostawca uzyskuje certyfikację względem niezależnych standardów takich jak ISO 27001/27002
Dobre praktyki FSA w zakresie ochrony danych w usługach finansowych (kwiecień 2008)	Raport został opublikowany jako konsekwencja oceny dokonanej przez FSA w zakresie jak firmy z sektora finansowego w Wielkiej Brytanii działają w zakresie ryzyka utraty bądź kradzieży danych należących do ich klientów i wykorzystanych następnie do popełnienia oszustwa lub innego przestępstwa finansowego. Nie są to oficjalne wytyczne FSA jednak oczekuje ona od firm respektowania tego raportu, aby tworzyć bardziej ocenę ryzyka oraz wdrożyć bardziej efektywną kontrolę jako część zobowiązania do wypełnienia zasady 2 i 3 określonej w FSA Handbook (patrz powyżej)	Nie jasne jest, w jaki sposób lepiej doświadczeni dostawcy z sektora cloud computingu mają się stosować do szczegółowych dobrych praktyk skierowanych do firm z sektora finansowego oraz działać stosownie do zakresu tych wytycznych.
Ustawa regulująca uprawnienia śledcze (Regulation of Investigatory Powers Act - RIPA)	RIPA reguluje uprawnienia organów publicznych do prowadzenia obserwacji oraz dochodzenia a także przechwytywania różnego rodzaju komunikacji. Regulacja została wprowadzona celem dostosowania do zmian technologicznych takich jak rozwój Internetu oraz silniejsza utajnianie danych. RIPA może być podstawą do działania władz za pomocą różnego rodzaju aktów rządowych w zakresie bezpieczeństwa narodowego a także dla celów wykrywania przestępstw, przeciwdziałania niepokojom, dla publicznego bezpieczeństwa oraz ochrony zdrowia publicznego lub w interesie interesu ekonomicznego Wielkiej Brytanii.	Firmy z sektora finansowego muszą zapewnić, że rozwój chmury nie doprowadzi do nie możliwości spełniania przez nie wymagań stawianych przez RIPA. Ponadto firmy muszą zapewnić również, że zawiadomią o każdym ujawnieniu tajemnicy danych dotyczących samej firmy lub jej klientów przez dostawcę chmury lub ISP (Internet Service Provider) niezgodnego z RIPA.

Francja

Francuskie prawo nie przewiduje specjalnych przepisów dotyczących zastosowania cloud computingu w sektorze finansowym. Również żadny podmioty takie jak regulator rynku, organizacje zrzeszające profesjonalistów lub instytucje finansowe nie zajęły stanowiska w tym temacie. Francuska ustawa o ochronie danych z 6 stycznia 1978 roku oraz Rozporządzenie 97-02 z 21 lutego 1997

roku dotyczące wewnętrznej kontroli instytucji kredytowych oraz firm inwestycyjnych przewidują postanowienia dotyczące tajemnicy, które stosują się również do chmury.

Regulacja/ Standard	Wymogi	Cloud computing
Ustawa o ochronie danych z 6 stycznia 1978 r.	Zgodnie z francuskim prawem administrator danych jest zobowiązany do zachowania wymogów bezpieczeństwa. Stosownie do art. 34 ustawy o ochronie danych administrator danych jest zobowiązany do dostarczenia wszelkich użytecznych zabezpieczeń stosownie do rodzaju danych i ryzyka ich przetwarzania, aby zabezpieczyć te dane w szczególności przed ich zamianą, zniszczeniem lub uzyskaniem nieautoryzowanego dostępu przez osoby trzecie. Co więcej, w przypadku outsourcingu danych – przetwarzający dane powinien dostarczyć adekwatny poziom ochrony przez zapewnienie odpowiednich środków bezpieczeństwa i poufności. Jednakże te wymagania nie zwalniają administratora danych od obowiązku zapewnienia nadzoru w stosowaniu środków określonych powyżej. Umowa pomiedzy przetwarzającym a administratorem danych powinna określać obowiązki ciążące na przetwarzającym jako zobowiązanym do zapewnienia bezpieczeństwa i poufności danych oraz gwarantować, że przetwarzający będzie działał tylko w przypadkach wyraźnie wskazanych przez administratora. Wynika z tego, że kontrakt musi gwarantować brak możliwości zlecenia przez przetwarzającego dane podwykonawstwa jakiegokolwiek fragmentu przetwarzania danych bez	Firmy z sektora finansowego powinny uwzględniać obowiązki w zakresie bezpieczeństwa w umowach podpisywanych z dostawcami usług w chmurze. Jednakże będą oni ponosić odpowiedzialność za każdą utratę, zniszczenie lub ujawnienie danych w razie jakiegokolwiek naruszenia kontraktu przez dostawcę. Muszą oni również zwrócić się do dostawcy o wypełnianie wysokich standardów technologicznych (ISO/CEI 27001 and ISO 27005 lub PCI DSS). Dostawca powinien dostarczyć listę wszystkich centrów danych oraz wykonawców, które zostaną użyte/użyci przy przetwarzaniu danych. Jeżeli centra danych/wykonawcy mający dostęp do danych osobowych mają siedzibę poza EOG – spowoduje to konieczność zawarcie umowy transferu danych bazującej na standardowych klauzulach umownych Komisji Europejskiej z każdym z przetwarzających dane (włączając własnych wykonawców przetwarzającego) oraz otrzymania wcześniejszej autoryzacji dokonanej przez CNIL. W związku z tym firmy z sektora finansowego powinny preferować dostawców z siedzibą w krajach zapewniających adekwatny poziom ochrony.

	uprzedniej zgody administratora. Ponadto, transfer danych osobowych poza terytorium UE lub do kraju trzeciego nie spełniającego adekwatnego poziomu ochrony musi być autoryzowany przed transferem przez francuski organ odpowiedzialnych za ochronę danych osobowych (CNIL). Celem spełnienia wymogu autoryzacji, administrator danych musi przedstawić listę wszystkich krajów, do których nastąpi transfer, dane wszystkich podmiotów przetwarzających te dane oraz listę wszystkich centrów przechowywania danych.	
Rozporządzenie 97-02 z 21 lutego 1997 r. w zakresie kontroli wewnętrznej instytucji kredytowych oraz firm inwestycyjnych.	Zgodnie z Rozporządzeniem 97-02, artykuł 37-2, Banki oraz instytucje finansowe musze w przypadku outsourcingu kluczowych/krytycznych dla nich usług utrzymywać odpowiednie umiejętności i wiedzę w zakresie zapewnienia efektywności kontroli outsourcowanych zadań lub usług oraz radzenia sobie z takimi zadaniami. W szczególności, podmioty te muszą zawrzeć umowę w formie posiemnej z dostawcą usługi, która musi zapewniać, że dostawca: • zapewni tym podmiotom i odpowiednim organom, w razie takiej konieczności, dostęp (także fizyczny dostęp) do jakichkolwiek informacji lub usług dostępnych dla dostawcy w powiązaniu z regulacjami dot. ujawnienia informacji poufnych, • zapewni poziom odpowiedniej funkcjonalności usługi w	Wymogi dot. możliwości dostępu oraz audytu są nie zawsze zgodne z rozwiązaniami stosowanymi w chmurze bazującymi na losowym rozpowszechnianiu danych na kilku serwerach. Firmy z sektora finansowego powinny zapewnić (rozumiejąc przez to środki techniczne, organizacyjne oraz kontraktowe), że wdrożenie usług w chmurze będzie dokonane zgodnie z postanowieniami Rozporządzenia 97-02. W praktyce będzie to oznaczać ograniczenie ilości oraz lokalizacji centrów danych.

	razie wystąpienia jakiegokolwiek zdarzenia, • zapewni ochronę informacji poufnych, • wdroży adekwatny plan kontynuacji świadczenia, • nie ma prawa do jednostronnej i znaczącej modyfikacji usługi dopóki nie zostanie to prawidłowo zatwierdzone, • zastosuje się do wewnętrznych procedur kontrolnych instytucji finansowych, • udostępni, jeżeli będzie to niezbędne dostęp (włączając dostęp fizyczny) do wszelkich informacji dot. świadczenia usługi • poinformuje o jakimkolwiek zdarzeniu mogącym mieć istotny wpływ na możliwość świadczenia usługi • zaakceptuje możliwość dostępu do informacji (włączając dostęp fizyczny) przez francuskich regulatorów finansowych oraz regulatorów z każdego innego państwa obcego zapewniającego adekwatną ochronę.	
Artykuł 511-33 Kodeksu pieniężnego i finansowego odnoszącego się do tajemnicy bankowej	Zgodnie z art. 511-33 Kodeksu pieniężnego i finansowego, pracownicy, Banki oraz instytucje finansowe są związane tajemnicą zawodową. Stosownie do tego, wszelkie środki (techniczne oraz kontraktowe) muszą zostać podjęte celem zapewnienia przestrzegania tajemnicy zawodowej. Dzielenie lub transfer danych jest ściśle limitowany bazując na „teście konieczności”	Instytucje finansowe muszą zapewnić (przez środki techniczne oraz kontraktowe), że wdrożenie usług w chmurze odbędzie się zgodnie z francuskimi postanowieniami prawnymi dot. tajemnicy bankowej Instytucje finansowe powinny zapewnić, że otrzymały wszelkie wymagane zgody od klientów.

	określonym przez artykuły 511-33 lub na podstawie wyraźnej zgody udzielonej przez poinformowanego klienta. Pod pewnymi warunkami (bankowość prywatna, specyficzne wzmocnione umowy o zachowanie poufności), zgoda klienta może być uznana za wiążącą, kiedy w momencie udzielenie zgody, informacja została dostarczona do klienta w odniesieniu do krajów, gdzie dane są przetwarzane.	

Autorzy

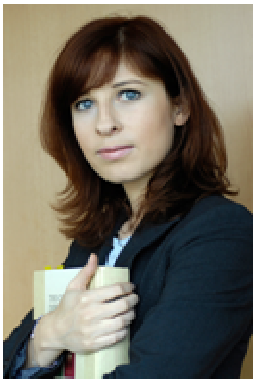
Autorzy

Maciej Gawroński
Partner
Szef polskiego biura Bird & Bird
Szef praktyki IT
Radca Prawny
maciej.gawronski@twobirds.com

<u>Redakcja raportu</u>
oraz autor poszczególnych rozdziałów:
Outsourcing w sektorze bankowym (2)
Standardy branżowe (5)

Maciej Gawroński doradza przedsiębiorcom od 1994 roku. Maciej jest ekspertem doradztwa prawnego dotyczącego technologii. Przed objęciem kierownictwa warszawskiego biura Bird & Bird był partnerem odpowiedzialnym za praktykę nowoczesnych technologii w niezależnej polskiej kancelarii prawniczej. Specjalizuje się także w negocjacjach i rozwiązywaniu sporów, w bankowości i finansach oraz w ochronie danych osobowych. Maciej doradza nabywcom technologii w ich procesach back-office (wdrożenia IT, outsourcing, przepływ danych, zarządzanie ryzykiem i ciągłością działania), sprawach regulacyjnych oraz w sporach sądowych i arbitrażowych. Jest uznawany za jednego z najlepszych prawników IT w Polsce. Dzięki biznesowemu doświadczeniu, analitycznemu podejściu i nakierowaniu na odnajdywanie rozwiązań Maciej zapewnia konsulting o szczególnej wartości a klienci powierzają mu rolę zaufanego doradcy.

Maciej studiował prawo na Uniwersytecie Jagiellońskim w Krakowie oraz na Uniwersytecie w Tours we Francji.



Emilia Stępień
Szef zespołu ochrony danych osobowych
Radca Prawny

Współautorka rozdziału:
Cloud Computing w regulacjach dot. danych osobowych (1)

Doświadczenie zawodowe Mecenas Emilii Stępień przed rozpoczęciem pracy dla kancelarii Bird & Bird obejmuje staż w Komisji Europejskiej, DG Rynek Wewnętrzny i Usługi, Zespół Własności Przemysłowej, w którym zajmowała się m.in. Patentem Unii Europejskiej oraz Sądem ds. Patentu Europejskiego i Patentu Unii Europejskiej.

Główne specjalizacje Emilii Stępień obejmują: prawo własności intelektualnej, ochrony danych osobowych, handlu elektronicznego oraz prawo konkurencji.

Emilia Stępień ukończyła Wydział Prawa i Administracji Uniwersytetu Warszawskiego, oraz studia z prawa angielskiego i europejskiego Uniwersytetu Cambridge, a także kurs z zakresu prawa konkurencji w Unii Europejskiej – Nowe uprawnienia sądów państwowych przeprowadzony przez Szkołę Prawa Europejskiego w Warszawie, oraz Siódmy Specjalny Moduł dotyczący Wspólnotowego Znaku Towarowego na Uniwersytecie Alicante w Hiszpanii w ramach programu Magister Lvcentinvs.

Emilia Stępień jest wykładowcą Uniwersytetu SAR. Prowadziła także szkolenia z zakresu prawa własności intelektualnej, ochrony danych osobowych oraz prawa konkurencji oraz występowała jako prelegent na polskich i międzynarodowych konferencjach branżowych. Emilia Stępień jest autorką publikacji z zakresu własności intelektualnej, prawa konkurencji oraz ochrony danych osobowych**.**

Izabela Kowalczuk
Associate

Współautorka rozdziału:
Cloud Computing w regulacjach dot. danych osobowych (1)

Izabela Kowalczuk doświadczenie zawodowe zdobywała w polskich sieciowych i niezależnych kancelariach prawniczych oraz w Association for Competitive Technology w Stanach Zjednoczonych. Izabela specjalizuje się w problematyce dotyczącej prawa własności intelektualnej, prawa IT i handlu elektronicznego oraz prawa procesowego, w tym postępowania arbitrażowego.

Izabela Kowalczuk jest absolwentką Wydziału Prawa i Administracji Uniwersytetu Warszawskiego oraz aplikantka II roku w Okręgowej Izbie Radców Prawnych w Warszawie. Ukończyła kurs prawa amerykańskiego na Uniwersytecie Warszawskim. Studiowała także na Katholische Universität Leuven (Belgia).

Michał Balicki
Associate

Szef zespołu dochodzenia należności
Autor rozdziałów:
Outsourcing bankowy (3)
Rekomendacje Komisji Nadzoru Finansowego (4)

Michał Balicki jest absolwentem Uniwersytetu im. Adama Mickiewicza w Poznaniu oraz ukończył kurs prawa handlowego z podstawami ekonomii na Uniwersytecie w Bergen w Norwegii, ukończył także studia podyplomowe z zakresu Zarządzania Ryzykiem w Instytucjach Finansowych w Szkole Głównej Handlowej w Warszawie.

Michał Balicki ma doświadczenie procesowe, w zakresie bankowości i finansów oraz zarządzania ryzykiem, a także w zakresie IT i nowych technologii, ochrony danych osobowych oraz prawa pracy.

Katarzyna Otwinowska
Associate

Autorka rozdziałów:
Cloud Computing w regulacjach dot. sektora funduszy inwestycyjnych (6.1)
Cloud Computing w regulacjach dot. sektora funduszy emerytalnych (6.2)
Cloud Computing w regulacjach z zakresu działalności firm inwestycyjnych (6.3)

Katarzyna zajmuje się praktyką usług i rynków finansowych. Prowadziła także bieżącą obsługę korporacyjną szeregu spółek prawa handlowego, w tym jako samodzielny koordynator projektów, oraz wykonywała czynności w zakresie stałej obsługi prawnej funduszy inwestycyjnych i zarządzającego nimi TFI. Katarzyna specjalizuje się w prawie spółek, zarządzaniu aktywami i funduszami inwestycyjnymi, bankowości i finansach oraz kontraktach.

Katarzyna jest absolwentką Wydziału Prawa i Administracji Uniwersytetu im. Mikołaja Kopernika w Toruniu. W 2005 roku ukończyła kurs *Introduction to English law and the law of the European Union* organizowany przez Institute of Continuing Education, University of Cambridge;

Wojciech Marek
Radca Prawny

Autor rozdziału:
Cloud Computing w działalności ubezpieczeniowej (6.4)

Wojciech Marek jest radcą prawnym z ponad 25 letnim doświadczeniem. W latach 1990-2007 był członkiem zarządu i dyrektorem departamentu prawnego Banku BISE, jak i również członkiem Komitetu Doradczego do spraw Regulacji Nadzorczych i Rady Prawa Bankowego przy Związku Banków Polskich. Brał też udział w postępowaniach w charakterze arbitra ad hoc albo pełnomocnika strony w Sądzie Arbitrażowym przy Związku Banków Polskich. Od 2009 jest arbitrem Sądu Arbitrażowego przy Krajowej Izbie Gospodarczej w Warszawie.

Główne obszary praktyki prawniczej Wojciecha Marka to prawo cywilne, prawo bankowe, prawo spółek handlowych oraz prawo ubezpieczeniowe.

Wojciech Marek jest absolwentem Wydziału Prawa i Administracji Uniwersytetu Warszawskiego. Ma również tytuł doktora nauk prawnych. W latach 1971–1990 był wykładowcą prawa cywilnego i prawa ubezpieczeniowego na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Wojciech Marek jest członkiem Okręgowej Izby Radców Prawnych w Warszawie oraz współautorem książki Prawo Ubezpieczeniowe (1983), jak i autorem ponad 40 artykułów i glos z zakresu prawa cywilnego, prawa ubezpieczeniowego i prawa bankowego.

Filip Łukaszewicz

Operator dokumentu
Autor rozdziałów:
Cloud Computing w regulacjach dot. informacji niejawnych (tajemnica państwowa) (7)
Cloud Computing w rachunkowości (8)

Filip Łukaszewicz jest studentem Wydziału Prawa i Administracji Uniwersytetu Warszawskiego oraz ukończył kurs Centrum Prawa Amerykańskiego UW wraz z Levin College of Law, University of Floryda.

Filip Łukaszewicz ma ponad dwuletnie doświadczenie praktyczne, w szczególności w zakresie prawa pracy, IT i nowych technologii oraz prawa procesowego.

O Forum Technologii Bankowych i o Bird & Bird

Forum Technologii Bankowych (FTB) przy Związku Banków Polskich ukonstytuowało się 14 kwietnia 2004 roku, działa w ramach Rady Bankowości Elektronicznej. Zrzesza firmy technologiczne (dostawców technologii bankowych) współpracujące z bankami i Związkiem Banków Polskich w ramach realizacji zadań statutowych ZBP. Bezpośrednią przyczyną powołania Forum była rosnąca potrzeba współpracy firm technologicznych oraz banków w zakresie automatyzacji obrotu gotówkowego i propagowania obrotu bezgotówkowego, a także wprowadzania nowoczesnych rozwiązań technologicznych w sektorze bankowym w Polsce. Najważniejszymi zadaniami Forum w tym zakresie jest przeciwdziałanie przestępczości w bankowości elektronicznej oraz wdrażanie nowoczesnych produktów bankowych, funkcjonujących w oparciu o najnowocześniejsze rozwiązania.

Do Forum należą uznane firmy, liderzy w swoich dziedzinach. Członkowie FTB mają duże osiągnięcia w ramach realizowanych projektów dla banków, jak i podejmowanych inicjatyw na rzecz społeczeństwa informatycznego a także wzrostu zaufania do bankowości elektronicznej. FTB zrzesza przedsiębiorców posiadających pozytywnie ocenione doświadczenia zweryfikowane w ramach współpracy z bankami.

Forum jest również propagatorem gospodarki i administracji elektronicznej w Polsce. Jednym z głównych celów Forum jest szeroko pojęta promocja gospodarki elektronicznej, obrotu bezgotówkowego, nowoczesnych technologii, elektronicznej tożsamości i szeroko rozumianego bezpieczeństwa.

W ramach Forum tworzymy raporty, analizy i opracowania, które inicjują wdrażanie innowacji. Dobrym przykładem naszych prac są dokumenty dotyczące biometrii, identyfikacji i uwierzytelnienia, zapewnienia ciągłości działania (BCM), bezpieczeństwa transakcji, itd. W pierwszym okresie działalności Forum opracowywała analizy, promowało i pomagało wdrażać standard EMV karty mikroprocesorowej, wieloaplikacyjność rozwiązań na karcie, elektroniczną kartę miejska, czy elektroniczne legitymacje studenckie czy szkolne z aplikacjami płatniczymi, pieniądz elektroniczny i bankowość mobilną. Wiele z tych rozwiązań zostało następnie wdrożonych w praktyce.

Forum jest sformalizowaną grupą, mającą na celu doprowadzenie do przyjęcia w Polsce rozwiązań prawnych umożliwiających dynamiczny rozwój gospodarki elektronicznej.

Forum jak sama nazwa wskazuje jest miejscem wymiany myśli i informacji, jak również edukacji, prezentacji i spotkań z bankowcami.

Posiada własną strukturę i pełną autonomię.

FTB prowadzi działalność edukacyjną ukierunkowaną na środowisko bankowe i jego otoczenie. Dostarcza informacji o najnowocześniejszych rozwiązaniach technologicznych w bankowości i biznesie elektronicznym. Jest stowarzyszeniem otwartym na współpracę i promocję korzystnych dla rozwoju polskiej bankowości i gospodarki elektronicznej rozwiązań.

Bird & Bird jest międzynarodową praktyką prawniczą, w której skład wchodzi Bird & Bird LLP i podmioty z nią stowarzyszone, w tym Bird & Bird Maciej Gawroński sp.k.

Bird & Bird powstał w 1846 roku w Londynie. Obecnie posiada 23 biura w 16 krajach Europy i Azji. Bird & Bird Maciej Gawroński sp.k. jest Ekspertem Prawnym Krajowej Izby Gospodarczej, członkiem Polskiej Izby Informatyki i Telekomunikacji, członkiem British Polish Chamber of Commerce, współpracuje z Forum Technologii Bankowych Związku Banków Polskich. Zespół Bird & Bird doradza podmiotom sektora finansowego przy transakcjach, regulacjach i procesach backoffice. Warszawskim zespołem bankowości i finansów Bird & Bird kierują Aleksandra Widziewicz i Sławomir Szepietowski – radcowie prawni z kilkunastoletnim doświadczeniem w sektorze. Zespołem TMT (Technologia, Media, Telekomunikacja) kieruje Maciej Gawroński - radca prawny pracujący dla sektora finansowego od 1999 roku. Więcej informacji o Bird & Bird na www.twobirds.com. (wersja polska i strona o polskim biurze jest w opracowaniu).