PIU

Polska Izba Ubezpieczeń

Raport o usługach *cloud computing* w działalności ubezpieczeniowej

Dla Polskiej Izby Ubezpieczeń

Warszawa, styczeń 2013

Domański Zakrzewski Palinka

„Raport o usługach *cloud computing* w działalności ubezpieczeniowej" ma na celu przedstawienie czytelnikom podstawowych założeń, korzyści i ryzyk usług przetwarzania w chmurze w działalności ubezpieczeniowej. Został przygotowany przez ekspertów kancelarii prawniczej Domański Zakrzewski Palinka sp. k. dla Polskiej Izby Ubezpieczeń. Raport sporządzono zgodnie ze stanem prawnym obowiązującym na dzień 20 listopada 2012 r.

Autorzy:
Domański Zakrzewski Palinka sp. k.
Aleksandra Auleytner, Janina Ligner-Żeromska, Bartosz Marcinkowski, Julita Zimoch-Tuchołka, Marlena Wach, Monika Malinowska-Hyla, Maria Skrzypczyk, Rafał Surowiec, Jakub Jan Kubalski

Spis treści

1. Wstęp

Prawo często zostaje w tyle za rzeczywistością gospodarczą. Szczególnie dotyczy to IT, w której nowe rodzaje usług powstają niezwykle szybko wraz z rozwojem technologii. Niemniej jednak, nawet gdy w biznesie pojawiają się nowe rozwiązania, dotychczasowe formuły prawne pozostawają nadal aktualne. Kodeks cywilny przykładowo, nie musiał zostać znacząco zmieniony, by dało się dostosować zawarte w nim normy do umów zawieranych przez Internet, a zmiany nie dotknęły istoty ani zasad prawa cywilnego. Być może podobnie będzie w przypadku usług przetwarzania w chmurze. Niepotrzebna jest rewolucja, lecz dostosowanie i być może uzupełnienie prawa.

Proces zmian prawnych jest w toku. Ramy rozwiązań biznesowych opartych na technologiach *cloud computing* obecnie funkcjonują w zmieniającym się środowisku prawnym. Z tego też względu ważna jest znajomość przepisów już obowiązujących oraz propozycji zmian w tym obszarze, a przede wszystkim ich przyczyn i przewidywanych skutków.

Raport ma za zadanie przedstawić czytelnikom zarys pojęciowy i problematykę przetwarzania w chmurze w działalności ubezpieczeniowej, w szczególności w zakresie najbardziej wrażliwej kwestii – ochrony danych osobowych w chmurze.

1.1. Charakterystyka usług przetwarzania w chmurze

Moc obliczeniowa oraz możliwości komputera są zasadniczo ograniczone standardami posiadanego przez nas sprzętu oraz oprogramowania. Jednak czasem niezbędne wydaje się użycie kosztownego oprogramowania i związanej z nim rozbudowanej infrastruktury. Może to być szczególnie istotne w przypadku maszyn do edycji wideo w HD, programów do projektowania budynków, itp. Koszty dostarczenia, wdrożenia, aktualizacji, serwisu i obsługi elementów software oraz hardware są częstokroć bardzo wysokie. W celu ich obniżenia powstała nowa grupa usług w zakresie IT – *cloud computing*, czyli tzw. przetwarzania w chmurze.

Zasadniczo, przetwarzanie w chmurze polega na outsourcingu usług IT poza własne przedsiębiorstwo, z tym że dzieje się to wirtualnie. Jego celem jest elastyczne zapewnienie zasobów IT (zarówno software, jak i hardware) na żądanie użytkowników, przy czym przetwarzanie odbywa się u usługodawcy.

1.2. Zalety *cloud computing*

Zaletami usług przetwarzania w chmurze są przede wszystkim:

- *On-demand* – możliwość uzyskania oczekiwanej mocy obliczeniowej na żądanie bez konieczności inwestowania we własną infrastrukturę sprzętową;

- Redukcja kosztów – z racji tego, że przy jednoczesnym dostarczaniu wymaganych rozwiązań informatycznych nie trzeba inwestować w sprzęt informatyczny, unika się kosztów związanych z rozwojem własnej infrastruktury IT;
- Niezależność od położenia źródeł danych – usługi przetwarzania w chmurze umożliwiają współdzielenie zasobów informatycznych za pomocą różnych urządzeń, z wielu miejsc na świecie, np. z urządzeń mobilnych;
- Mierzalność – usługobiorca ma możliwość określenia minimalnych oraz maksymalnych technicznych wymagań co do przetwarzania w chmurze, np. co do przestrzeni dyskowej, ilości i jakości dedykowanych procesorów, wielkość pamięci, przepustowości łącza wychodzącego, liczby użytkowników, lub na podstawie innej metody określania mocy obliczeniowej – jest to szczególnie istotne w przypadku opierania rozwiązania IT na PCU (ang. *Peak Concurrent Users);*
- Skalowalność – usługodawca może dostosowywać parametry techniczne usługi do bieżących potrzeb, tj. zwiększyć lub zmniejszyć moc obliczeniową bez potrzeby inwestowania w sprzęt;
- Łatwiejsze utrzymanie – to usługodawca jest odpowiedzialny za infrastrukturę sprzętową, przy użyciu której następuje świadczenie usług przetwarzania w chmurze i ponosi wszelkie koszty związane z jej utrzymaniem.

1.3. Rozwiązania mobilne a *cloud computing*

Cloud computing jest immanentnie związany z technologiami mobilnymi. Z racji tego, że całość operacji wykonywana jest w chmurze, aplikacje oraz urządzenia mobilne pomimo swoich ograniczeń technicznych mogą mieć dostęp do systemów i mocy obliczeniowej dużych korporacyjnych systemów IT. Przykładowo, usługi przetwarzania w chmurze mogą umożliwiać mobilny dostęp, chociażby poprzez telefon komórkowy, do oprogramowania biurowego, użytkowego, które standardowo potrzebuje konkretnych systemów operacyjnych oraz ma wysokie wymagania sprzętowe.

W celu mobilnego korzystania z usług *cloud computing* potrzebne jest jednak z reguły łącze o bardzo wysokiej przepustowości. Wynika to z rozwiązań technicznych wymagających często *streamingu* obrazu z serwerów w chmurze do urządzenia mobilnego.

1.4. Modele usług oraz świadczenia usług przetwarzania w chmurze

1.4.1. Techniczne modele usług przetwarzania w chmurze

Poniższy podział wyodrębnia rodzaje usług *cloud computing* ze względu na treść usługi, tj. jakie konkretne usługi usługodawca świadczy w ramach umowy (podział przedmiotowy).

1.4.1.1. Kolokacja

Kolokacja w skrócie sprowadza się do tego, że usługodawca udostępnia usługobiorcy jedynie przestrzeń na infrastrukturę sieciową jego organizacji, tj. tzw. serwerownię, meble – *server racks*, usługi klimatyzacji, połączenia z siecią elektryczną, urządzeń UPS, dostępu do LAN, itp. Oprogramowanie oraz osprzęt pochodzi od usługobiorcy.

Kolokacja jest pojęciem prawnym. W rozumieniu art. 2 pkt 15 Prawa telekomunikacyjnego oznacza ono:

> *udostępnianie fizycznej przestrzeni lub urządzeń technicznych w celu umieszczenia i podłączenia niezbędnego sprzętu operatora podłączającego swoją sieć do sieci innego operatora lub korzystającego z dostępu do lokalnej pętli abonenckiej.*

Ponadto warto nadmienić, iż przepis art. 29 ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych zawiera określone obowiązki przedsiębiorcy telekomunikacyjnego w zakresie przekazywania informacji Prezesowi UKE o posiadanej infrastrukturze telekomunikacyjnej, publicznych sieciach telekomunikacyjnych i budynkach umożliwiających kolokację. Do tego przepisu zostało wydane rozporządzenie określające szczegóły tej inwentaryzacji.

1.4.1.2. *Infrastructure as a Service* (IaaS)

W modelu IaaS usługodawca udostępnia, obsługuje, serwisuje osprzęt – tj. serwery, dyski twarde. Oprogramowanie, bazy danych, systemy operacyjne pozostają odpowiedzialnością usługobiorcy.

1.4.1.3. *Platform as a Service* (PaaS)

Poza udostępnianiem infrastruktury, w ramach PaaS usługodawca zapewnia system operacyjny, na którym usługobiorca ma możliwość uruchamiania lub pisania własnego oprogramowania.

1.4.1.4. *Software as a Service* (SaaS)

Najdalej (obecnie) idący model przetwarzania w chmurze zakłada świadczenie usług w zakresie udostępniania infrastruktury, systemu operacyjnego oraz gotowych aplikacji. Przykładem zastosowania takiego modelu mogą być chociażby skrzynki e-mailowe udostępniane przez popularne witryny internetowe.

1.4.2. Modele świadczenia usług przetwarzania w chmurze

W praktyce spotyka się również podział usług przetwarzania w chmurze ze względu na ilość podmiotów uprawnionych do korzystania z usługi, tj. czy chmura jest dostępna dla ogółu publiczności, czy też dostęp do niej jest ograniczony (podział podmiotowy).

1.4.2.1. Chmura prywatna – w której to jeden podmiot jest właścicielem lub wyłącznie uprawnionym do korzystania z chmury obliczeniowej.

1.4.2.2. Chmura grupowa – usługa, w ramach której zamknięty krąg odbiorców współdzieli chmurę obliczeniową między sobą.

1.4.2.3. Chmura publiczna – poprzez którą rozumie się dostępną dla ogółu społeczeństwa przestrzeń obliczeniową w chmurze (niezależnie od tego, czy za wynagrodzeniem, czy nieodpłatnie).

1.4.2.4. Chmura hybrydowa – model łączący dwa lub więcej modeli świadczenia usług w chmurze.

2. Uregulowania prawne dotyczące ubezpieczeń w kontekście outsourcingu usług IT

W związku z rozmowami na poziomie instytucji Unii Europejskiej (trwają otwarte publiczne konsultacje Komisji Europejskiej dotyczące przetwarzania w chmurze[1]) oraz z równoległymi pracami nad projektem regulacji w Stanach Zjednoczonych[2], w niedalekiej przyszłości będzie można polegać na generalnie obowiązujących przepisach wyznaczających obowiązki stron przy konkretnych zakresach korzystania lub świadczenia usług przetwarzania w chmurze.

Na chwilę obecną, przed ewentualnym wprowadzeniem do porządku prawnego kompleksowej regulacji dotyczącej usług *cloud computing*, rekomenduje się daleko posuniętą ostrożność w kwestiach prawnych. Zarówno usługobiorca, jak i usługodawca, podczas negocjowania umowy na świadczenie usług przetwarzania w chmurze powinni zwrócić uwagę na proponowane postanowienia umowne i odnieść je do swoich założeń biznesowych oraz wymagań stawianych przez powszechnie obowiązujące prawo.

Niewątpliwie, na dzień dzisiejszy, istotne znaczenie w outsourcingu usług IT mają uregulowania prawne dotyczące praw autorskich, świadczenia usług drogą elektroniczną, ochrony baz danych, ochrony danych osobowych. W kontekście świadczenia usług ubezpieczeniowych należy mieć na uwadze przepisy regulujące świadczenie usług ubezpieczeniowych.

2.1. Obostrzenia w przypadku tajemnicy ubezpieczeniowej – kwestia odpowiedzialności

Ustawa o działalności ubezpieczeniowej w art. 19 ust. 1 określa generalną zasadę ochrony tajemnicy ubezpieczeniowej, tj.:

> *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.*

W świetle przytoczonego przepisu można przyjąć, że tajemnica ubezpieczeniowa dotyczy:

- Wszelkich danych związanych z umowami ubezpieczeniowymi, tj. danych ubezpieczonych, ubezpieczających, ewentualnych innych stron, konkretnych postanowień umownych, jak również informacji o tym, iż taka umowa została w ogóle zawarta;

1. http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=cloudcomputing&lang=en.
2. http://www.legalcloudcentral.com/2011/05/articles/regulation/regulating-the-cloud-the-cloud-computing-act-of-2011/.

- Wszelkich danych związanych z wykonaniem umowy, przetwarzanych przez zakład ubezpieczeń w związku z umową ubezpieczenia lub nawet jeżeli do zawarcia umowy nie doszło.

Ustawa o działalności ubezpieczeniowej w art. 19 ust. 2 zawiera listę podmiotów, które mogą wnioskować, aby zakład ubezpieczeń udzielił im informacji stanowiących tajemnicę ubezpieczeniową. Dotyczy to m.in.:

> *podmiotu przetwarzającego, na zlecenie zakładu ubezpieczeń, dane dotyczące ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umów ubezpieczenia oraz administrujących indywidualnymi kontami jednostek uczestnictwa w ubezpieczeniowym funduszu kapitałowym.*

Tak opisany podmiot wypełnia przesłanki usługodawcy usług przetwarzania w chmurze. W związku z tym, w ramach stosunku prawnego łączącego zakład ubezpieczeń i usługodawcę rozwiązań *cloud computing*, usługodawca powinien złożyć odpowiedni wniosek w celu przetwarzania danych stanowiących tajemnicę ubezpieczeniową.

Należy pamiętać, iż ustawa o działalności ubezpieczeniowej zawiera ograniczenia co do swobody kreowania zasad dotyczących odpowiedzialności stron umów. Pomimo tego, że zakład ubezpieczeń może zlecić przetwarzanie danych osobie trzeciej, to jednak, na podstawie art. 19 ust. 3 ustawy o działalności ubezpieczeniowej, nie wyłącza to ani nie ogranicza odpowiedzialności zakładu ubezpieczeń z tytułu naruszenia obowiązku zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia. Oznacza to, że odpowiedzialność za wszelkie szkody wyrządzone osobom trzecim w związku z przetwarzaniem danych przez podmiot przetwarzający je na zlecenie zakładu ubezpieczeń będzie ponosić zakład ubezpieczeń. Ubezpieczyciel nie będzie mógł zwolnić się z tej odpowiedzialności przez wskazanie np. na okoliczność, że przetwarzanie danych powierzył profesjonaliście (art. 429 kodeksu cywilnego nie znajdzie tu zastosowania). Nie ma natomiast przeszkód, aby zasady odpowiedzialności usługodawcy rozwiązań *cloud computing* wobec ubezpieczyciela, w tym także za szkody wyrządzone osobom trzecim, za które odpowiedzialność będzie musiał ponieść ubezpieczyciel, uregulować w umowie z usługodawcą w sposób odpowiadający oczekiwaniom ubezpieczyciela w tym zakresie.

2.2. Podstawy prawne i warunki, które musi spełniać outsourcing w działalności ubezpieczeniowej

Ustawa o działalności ubezpieczeniowej wymienia konkretne czynności ubezpieczeniowe, które mogą być zlecane podmiotom trzecim. Co istotne, czynności wykonywane przez podmioty trzecie w ramach outsourcingu traktowane są jak czynności ubezpieczeniowe w zakresie, w jakim są wykonywane w imieniu i na rzecz zakładu ubezpieczeń. Czynnościami tymi są:

- Ocena ryzyka w ubezpieczeniach osobowych i ubezpieczeniach majątkowych oraz w umowach gwarancji ubezpieczeniowych;
- Wypłacanie odszkodowań i innych świadczeń należnych z tytułu umów, o których mowa w tej ustawie;
- Przejmowanie i zbywanie przedmiotów lub praw nabytych przez zakład ubezpieczeń w związku z wykonywaniem umowy ubezpieczenia lub umowy gwarancji ubezpieczeniowej;

- Prowadzenie 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;
- Prowadzenie postępowań regresowych oraz postępowań windykacyjnych związanych z wykonywaniem umów ubezpieczenia i umów gwarancji ubezpieczeniowych; umów reasekuracji w zakresie cedowania ryzyka z umów ubezpieczenia i umów gwarancji ubezpieczeniowych;
- Lokowanie środków zakładu ubezpieczeń;
- Ustalanie przyczyn i okoliczności zdarzeń losowych;
- Ustalanie wysokości szkód i rozmiaru odszkodowań oraz innych świadczeń należnych uprawnionym z umów ubezpieczenia lub umów gwarancji ubezpieczeniowych;
- Ustalanie wartości przedmiotu ubezpieczenia;
- Czynności zapobiegania powstawaniu albo zmniejszenia skutków wypadków ubezpieczeniowych lub finansowanie tych działań z funduszu prewencyjnego.

Najbardziej jednak istotny z punktu widzenia możliwości zastosowania rozwiązań *cloud computing* będzie outsourcing czynności przetwarzania danych dotyczących ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umów ubezpieczenia oraz administrujących indywidualnymi kontami jednostek uczestnictwa w ubezpieczeniowym funduszu kapitałowym. Odbywać się to będzie na podstawie wyżej opisanego art. 19 ust. pkt. 23 ustawy o działalności ubezpieczeniowej.

Ponadto zakład ubezpieczeń, na podstawie art. 26 ustawy o działalności ubezpieczeniowej, może zlecać innym podmiotom usługi dotyczące zabezpieczania dokumentów związanych z zawieraniem i wykonywaniem umów ubezpieczenia, a sporządzonych na informatycznych nośnikach danych. W tym zakresie zastosowanie będą miały techniczne przepisy zawarte w Rozporządzeniu Ministra Finansów z dnia 31 października 2003 r.

2.3. Zmiany spodziewane w związku z implementacją dyrektywy 2009/138/WE w sprawie podejmowania i wykonywania działalności ubezpieczeniowej i reasekuracyjnej

Na dzień sporządzenia niniejszego raportu prowadzone są prace nad implementacją w Polsce Dyrektywy 2009/138/WE w sprawie podejmowania i wykonywania działalności ubezpieczeniowej i reasekuracyjnej (tzw. Wypłacalność II) w ramach uzgodnień międzyresortowych. Jednocześnie sama Dyrektywa 2009/138/WE ulega nadal pewnym modyfikacjom, w szczególności w zakresie terminu jej wejścia w życie i dopasowania jej regulacji do tzw. Dyrektywy Omnibus II. Po uchwaleniu dnia 3 lipca 2012 r. przez Parlament Europejski tzw. dyrektywy naprawczej datą wejścia w życie Dyrektywy 2009/138/WE jest obecnie 1 stycznia 2014 roku.[3]

Zamiarem ustawodawcy europejskiego jest uregulowanie kwestii outsourcingu istotnych funkcji lub rodzajów działalności ubezpieczeniowej (co w polskiej terminologii trzeba rozumieć jako outsourcing czynności ubezpieczeniowych) w jednolity sposób we wszystkich państwach członkowskich UE, celem

3. Dyrektywa Parlamentu Europejskiego i Rady 2012/23/UE z dnia 12 września 2012 r. zmieniająca dyrektywę 2009/138/WE (Wypłacalność II) w odniesieniu do terminu jej transpozycji, daty rozpoczęcia jej stosowania oraz daty uchylenia niektórych dyrektyw, Dziennik Urzędowy UE z 14.09.2012 r. L249/1.

zaś regulacji outsourcingu czynności ubezpieczeniowych jest w pierwszej kolejności zapewnienie efektywnego nadzoru nad takimi czynnościami zlecanymi w ramach outsourcingu. W punkcie 37 Preambuły Dyrektywy 2009/138/WE stwierdza się, że:

> *konieczne jest, by organy, które sprawują nadzór nad zakładem ubezpieczeń lub zakładem reasekuracji dokonującym outsourcingu miały, niezależnie od tego, czy zleceniobiorca jest jednostką regulowaną czy nie, dostęp do wszystkich istotnych danych posiadanych przez zleceniobiorcę, a także prawo do przeprowadzania kontroli na miejscu. Celem uwzględnienia zmian zachodzących na rynku oraz zagwarantowania, że warunki dokonywania outsourcingu są w dalszym ciągu spełniane, organy nadzoru powinny być informowane przed dokonaniem outsourcingu podstawowych lub istotnych funkcji lub rodzajów działalności. Wymogi te powinny uwzględniać prace Wspólnego Forum i odpowiadać aktualnym regulacjom i praktykom w sektorze bankowym, a także dyrektywie 2004/39/WE i jej zastosowaniu w odniesieniu do instytucji kredytowych.*

W związku z koniecznością implementacji Dyrektywy 2009/138/WE do polskiego porządku prawnego planowana jest gruntowna zmiana ustawy o działalności ubezpieczeniowej. W chwili obecnej dostępny jest opracowany przez Ministerstwo Finansów „Projekt założeń do projektu ustawy o działalności ubezpieczeniowej i reasekuracyjnej" z maja 2012 roku, w którym proponuje się rozwiązania wzorowane na przepisach Dyrektywy 2009/138/WE i mające na celu ich szczegółową implementację. Dokument ten nie zawiera jednak propozycji tekstu nowej ustawy, lecz jedynie jej założenia. Na obecnym etapie trudno jeszcze wskazać, jaki konkretnie kształt przyjmą przepisy nowej ustawy o działalności ubezpieczeniowej i reasekuracyjnej, opracowane na podstawie wskazanego wyżej „Projektu założeń". Można jednak przyjąć, że treść konkretnych przepisów ustawy będzie w znacznym stopniu zbliżona do wskazanej w treści „Projektu założeń".

Należy zatem spodziewać się, że – analogicznie do przepisów Dyrektywy 2009/138/WE – polska ustawa będzie zawierała definicję outsourcingu, które to określenie według „Projektu założeń" będzie oznaczać:

> *umowę między zakładem ubezpieczeń albo zakładem reasekuracji a dostawcą usług, na podstawie której dostawca – bezpośrednio bądź w drodze dalszego outsourcingu – wykonuje czynności, funkcje należące do systemu zarządzania, które w innym przypadku zostałyby wykonane przez sam zakład ubezpieczeń lub zakład reasekuracji.*

Zdaniem autorów „Projektu założeń" obecna ustawa o działalności ubezpieczeniowej reguluje kwestie związane ze zlecaniem czynności ubezpieczeniowych w sposób niepełny i wymagający istotnych zmian. Przewidziane są zatem następujące modyfikacje:

- Co do zasady powinna pozostać utrzymana dotychczasowa możliwość zlecania przez zakład ubezpieczeń innym podmiotom wykonania czynności ubezpieczeniowych wskazanych w art. 3 ust. 6 i 9 ustawy o działalności ubezpieczeniowej. Dodatkowo ma być wprowadzona możliwość zlecania innym podmiotom wykonywania funkcji należących do systemu zarządzania zgodnie z punktem 31 preambuły i art. 49 Dyrektywy 2009/138/WE;
- Zakład ubezpieczeń będzie miał obowiązek zawiadomić KNF o zamiarze powierzenia takich czynności innemu podmiotowi. Obowiązkowi notyfikacji podlegać będzie także każda istotna zmiana, rozwiązanie lub wygaśnięcie umowy outsourcingu.

Analogicznie do przepisu obowiązującego w prawie bankowym (art. 6b ustawy – prawo bankowe) w ustawie o działalności ubezpieczeniowej ma być doprecyzowana zasada pełnej odpowiedzialności zakładów ubezpieczeń za wykonanie obowiązków z zakresu outsourcingu:

- Odpowiedzialności zakładu ubezpieczeń za szkody wyrządzone ubezpieczającym, ubezpieczonym, uposażonym lub uprawnionym z umów ubezpieczenia wskutek niewykonania lub nienależytego wykonania outsourcingu nie można wyłączyć ani ograniczyć;
- Odpowiedzialności zakładu ubezpieczeń i zakładu reasekuracji za szkody wyrządzone cedentom wskutek niewykonania lub nienależytego wykonania outsourcingu nie można wyłączyć ani ograniczyć.

W zakresie warunków, jakie musi spełniać outsourcing czynności ubezpieczeniowych, na wzór art. 38 Dyrektywy 2009/138/WE, „Projekt założeń" przewiduje, że:

- Dostawca usług będzie współpracował z organem nadzoru w zakresie powierzonych w ramach outsourcingu czynności lub funkcji;
- Zakład ubezpieczeń, jego podmiot uprawniony do badania sprawozdań finansowych oraz organ nadzoru będą posiadały faktyczny dostęp do danych związanych z powierzonymi funkcjami lub działaniami;
- Organ nadzoru będzie miał możliwość prowadzenia kontroli działalności i stanu majątkowego dostawcy usług w zakresie powierzonych czynności i funkcji.

Dodatkowo outsourcing podstawowych lub ważnych funkcji, bądź funkcji należących do systemu zarządzania nie będzie mógł odbywać się w sposób prowadzący do:

- Przekazania zarządzania zakładem ubezpieczeń w rozumieniu art. 368 § 1 kodeksu spółek handlowych (przepis ten stanowi, że to zarząd prowadzi sprawy spółki i reprezentuje ją na zewnątrz);
- Przekazania wykonywania działalności ubezpieczeniowej w sposób powodujący brak faktycznego wykonywania działalności przez zakład ubezpieczeń;
- Pogorszenia jakości systemu zarządzania zakładu ubezpieczeń;
- Zwiększenia ryzyka operacyjnego;
- Pogorszenia możliwości monitorowania przez organ nadzoru przestrzegania przez zakład ubezpieczeń jego obowiązków;
- Pogorszenia jakości świadczenia usług ubezpieczającym, ubezpieczonym, uposażonym lub uprawnionym z umów ubezpieczenia oraz cedentom.

W związku z nowymi wymogami odnośnie outsourcingu wynikającymi z Dyrektywy 2009/138/WE zostaną wprowadzone także odpowiednie zmiany w dotychczasowych przepisach dotyczących nadzoru ubezpieczeniowego w zakresie zlecania czynności ubezpieczeniowych, tj. w art. 208 ust. 2 i art. 210 ustawy o działalności ubezpieczeniowej. W szczególności „Projekt założeń" przewiduje wprowadzenie nowych uprawnień nadzorczych KNF, tj. nakazania zakładowi ubezpieczeń rozwiązania umowy outsourcingu, zakazania planowanego outsourcingu podstawowych lub ważnych czynności ubezpieczeniowych oraz funkcji należących do systemu zarządzania oraz jego istotnej zmiany.

KNF będzie miał prawo przeprowadzenia kontroli dostawcy usług na miejscu, w jego lokalu, w przypadku zaś dostawców umiejscowionych w innym państwie członkowskim Unii Europejskiej możliwa będzie kontrola przez organ nadzoru tego państwa członkowskiego, w którym umiejscowiony jest dostawca usług. W ramach kontroli organ nadzoru będzie miał możliwość przeprowadzenia kontroli działalności

i stanu majątkowego dostawcy usług w zakresie powierzonych w drodze outsourcingu czynności ubezpieczeniowych i reasekuracyjnych oraz funkcji należących do systemu zarządzania. Również organy nadzoru innych państw członkowskich Unii Europejskiej będą miały możliwość przeprowadzania kontroli dostawców usług umiejscowionych na terytorium Rzeczypospolitej Polskiej w zakresie czynności powierzonych przez zagraniczny zakład ubezpieczeń. Do kontroli dostawców usług, którzy wykonują w drodze outsourcingu czynności ubezpieczeniowe i reasekuracyjne oraz funkcje należące do systemu zarządzania powierzone przez zakład ubezpieczeń lub zakład reasekuracji, będą stosowały się odpowiednio przepisy o kontroli zakładów ubezpieczeń i zakładów reasekuracji, a ponadto przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej.

Niezależnie od wskazanych wyżej planowanych zmian do ustawy o działalności ubezpieczeniowej trzeba mieć na uwadze, że również na poziomie ustawodawstwa europejskiego prowadzone są intensywne prace nad nowymi przepisami, z których znaczna część będzie miała charakter przepisów bezpośrednio obowiązujących (bez konieczności wdrożenia ich do polskiego systemu prawnego w formie ustaw). Przepisy europejskie wprowadzające system Wypłacalność II, podobnie jak inne regulacje normujące funkcjonowanie sektora finansowego, mają strukturę trzypoziomową i obejmują:

i. Akt podstawowy, czyli dyrektywę ramową (akt poziomu 1) – jest to przede wszystkim omówiona wyżej Dyrektywa 2009/138/WE regulująca podstawowe zasady nowego systemu;
ii. Akty 2 poziomu – szczegółowe rozwiązania znajdą się w aktach wykonawczych do dyrektywy, zwanych aktami delegowanymi (ang. *delegated acts*), które będą wydawane na podstawie art. 290 Traktatu o Funkcjonowaniu Unii Europejskiej w formie rozporządzeń. W zakresie outsourcingu Dyrektywa 2009/138/WE wprost przewiduje, że Komisja Europejska przyjmie środki wykonawcze w celu bliższego określenia warunków, przy których spełnieniu można dokonywać outsourcingu, w szczególności w przypadku dostawców usług zlokalizowanych w państwach trzecich (art. 50 ust. 1 Dyrektywy 2009/138/WE). Akty te będę obowiązywały wprost bez konieczności ich implementowania do polskiego systemu prawnego.
iii. Akty 3 poziomu – będą zawierały dalsze szczegółowe przepisy, z których część będzie miała charakter niewiążących prawnie wytycznych (ang. *guidelines*), obowiązujących na zasadzie tzw. *comply or explain* (tj. stosuj się do przyjętych rozwiązań, a jeśli nie, to wytłumacz, dlaczego nie możesz się do nich stosować). Część natomiast będzie wydawana w formie prawnie wiążących, wykonawczych standardów technicznych (ang. *binding technical standards* – BTS lub *implementing technical standards* – ITS).

Treść projektów tych regulacji jest obecnie opracowywana i nie ma jeszcze dostępu do ostatecznego kształtu projektowanych przepisów.

2.4. Aspekty oraz charakterystyka umów IT w kontekście usług *cloud computing*

Istotą usług *cloud computing* jest przetwarzanie danych w infrastrukturze technicznej usługodawcy bez bliżej określonej lokalizacji. Przykładowo, pozwala to na zdalne łączenie wielu „farm" serwerów w jedną chmurę obliczeniową.

Taka chmura obliczeniowa, na co wskazaliśmy na wstępie raportu, może być udostępniana do powszechnego odbioru bliżej nieokreślonemu adresatowi (chmura publiczna) bądź udostępniana tylko jednemu

podmiotowi (chmura prywatna). Między tymi dwoma modelami istnieje model pośredni – chmura grupowa, oraz modele hybrydowe łączące cechy innych modeli świadczenia usług *cloud computing*.

W zakresie umów podział ten ma zasadnicze implikacje. Mianowicie chmura publiczna z racji swojej cechy powszechności będzie oparta na nienegocjowanej umowie lub regulaminie, który ma charakter adhezyjny, tj. usługobiorca nie będzie miał wpływu na treść jego postanowień. Tego typu rozwiązania są powszechne na poziomie *consumer* i *small business grade* i z reguły usługobiorca ma niewielkie możliwości dostosowania usługi przetwarzania w chmurze do własnych potrzeb. Natomiast chmura prywatna jest z reguły rozwiązaniem dopasowanym do indywidualnych potrzeb usługobiorcy. W związku z tym umowa, na której podstawie usługi przetwarzania w chmurze są świadczone, jest sporządzana przez obydwie strony bądź też nawet pierwszy jej projekt jest tworzony przez usługobiorcę, w zależności od pozycji negocjacyjnej stron. Poza standardowymi postanowieniami usługobiorca w tym modelu usług może chcieć sobie zagwarantować usługi SLA, geolokalizacji serwerów, kontroli, itp.

2.5 Podstawowe założenia i struktura umowy outsourcingowej w kontekście przetwarzania w chmurze prywatnej

2.5.1. Komparycja

Jak każda umowa, także ta z zakresu technologii informatycznych zaczyna się od kwestii podstawowych, tj. przedstawienia stron umowy, daty, miejsca zawarcia, czyli od tzw. komparycji.

2.5.2. Definicje

W skomplikowanych umowach pomocne okazuje się stworzenie listy definicji, które mają zastosowanie do umowy. Sporządzenie właściwych definicji pozwala na zaoszczędzenie czasu i objętości umowy.

2.5.3. Oświadczenia stron

Oświadczenia i deklaracje stron określają cele i zamiary stron w związku z zawarciem umowy. Deklaracje te, pełniące niejako funkcje preambuły, stanowią czasami pomoc w przypadku wątpliwości w interpretacji postanowień umownych. Strony przedstawiają także stan faktyczny np. co do posiadanej infrastruktury lub struktury korporacyjnej, określenia poziomu staranności, języka oprogramowania oraz języka dokumentacji, miejsca wykonywania prac, określenia metodyki pracy i współpracy, konsultacji między stronami.

2.5.4. Przedmiot

Najważniejszym elementem każdej umowy jest właściwe określenie jej przedmiotu. W tym zakresie właściwe jest określenie, jakich konkretnie usług przetwarzania w chmurze dotyczy umowa – dokładne określenie modelu, zakresu treściowego i czasowego jej obowiązywania. Istotne jest, czy strony przewidują jakiekolwiek usługi dodatkowe, utrzymaniowe, wdrożeniowe, serwisowe, szkoleniowe, wsparcia technicznego, jak rozwiązane są kwestie ewentualnych praw autorskich itp.

2.5.5. Proces prac – harmonogram, etapy realizacyjne, odbiory

W ramach tworzenia chmury obliczeniowej od podstaw ukierunkowanej na konkretne potrzeby usługobiorcy, uzasadnienie znajdują postanowienia pozwalające usługobiorcy kontrolować postępy w pracach tworzenia infrastruktury systemu poprzez określenie środowisk testowych, tj. *sandboxów* (udzielenie licencji testowych lub deweloperskich usługobiorcy). Usługobiorca może mieć słuszne oczekiwanie, iż oprogramowanie i system plików funkcjonujący w chmurze będzie kompatybilny z tymi stosowanymi w ramach infrastruktury jego przedsiębiorstwa.

Niezmiernie istotne znaczenie ma harmonogram prac i wskazanie etapów realizacji projektu. Przy dużych projektach zazwyczaj wynagrodzenie wypłacane jest częściami, powiązanymi ze zrealizowaniem, przekazaniem i odebraniem bez zastrzeżeń danego etapu realizacyjnego.

W ścisłej relacji z harmonogramem prac pozostają postanowienia odnoszące się do procedury odbiorów i testów. Spotyka się regulacje dotyczące odbiorów, testów częściowych, protokołów zdawczo-odbiorczych, protokołów rozbieżności, postanowienia określające kolejne kroki w zakresie procesu prac – księgi zmian dokonywanych przez konkretne osoby, raportów z przeprowadzonych prac.

Co istotne, udzielenie licencji do utworów w rozumieniu prawa autorskiego (o ile takowe powstają) zasadniczo następuje dopiero przy odbiorze końcowym, jednak można się umówić, że przyjęcie utworu (jego odpowiedniej części) będzie następowało przy każdym częściowym odbiorze np. danego etapu prac.

2.5.6. Role, personel, podwykonawcy

Umowy IT nadają osobom występującym po obu stronach umowy odpowiednie role, wraz ze szczegółowym określeniem celów, odpowiedzialności, terminów i zadań, np. koordynatorzy, menedżerowie, komitety sterujące. Komitety sterujące są ustanawiane przykładowo w celu dokonania końcowej akceptacji odbiorów częściowych, zlecania testów, zmian w harmonogramie (jeżeli takie nie wymagają zmiany umowy) i innych czynności, które są szczegółowo określone w samej umowie.

Umowy niejednokrotnie precyzują kluczowy personel, którego zmiana wymaga zgody obu stron umowy lub usługobiorcy. Spotykane są również postanowienia o zobowiązaniu usługodawcy do związania swoich pracowników zakazem konkurencji przez określony czas.

Umowy regulują również najczęściej uprawnienie zlecenia realizacji określonej części prac przez podwykonawców oraz możliwość przekazywania praw i obowiązków z umowy podmiotom trzecim.

2.5.7. Audyt, kontrole

W umowie zazwyczaj regulowana jest możliwość przeprowadzenia kontroli lub audytu przez zleceniodawcę, bądź wskazywany jest zewnętrzny audytor w celu weryfikacji należytego wykonywania usług w zgodzie z postanowieniami umownymi oraz standardami. Raporty poaudytowe mogą być podstawą

odbiorów częściowych lub końcowych. Audyt może dotyczyć zarówno efektów pracy wykonawcy, jak i sposobu wykonywania usług.

Należy podkreślić, że w związku z regulacjami dotyczącymi outsourcingu ubezpieczeniowego zawartymi w Dyrektywie 2009/38/WE oraz europejskich przepisach wykonawczych, a także w związku z planowanymi zmianami w ustawie o działalności ubezpieczeniowej w zakresie outsourcingu, umowa powinna uwzględniać także aspekty nadzoru ubezpieczeniowego nad czynnościami ubezpieczeniowymi zleconymi w drodze outsourcingu. W szczególności winna umożliwiać kontrolę prawidłowego wykonania tych czynności, nie tylko przez uprawnione organy nadzoru ubezpieczeniowego (gdyż tu uprawnienie organu będzie wynikać z mocy samego prawa), lecz także w takim samym zakresie – przez ubezpieczyciela. Prawo kontroli ubezpieczyciela u usługodawcy powinno bowiem zapewniać ubezpieczycielowi możliwość weryfikacji prawidłowości wykonywanych procedur, zwłaszcza w kontekście odpowiedzialności ubezpieczyciela za właściwe wykonanie czynności zleconych w drodze outsourcingu.

2.5.8. Wynagrodzenie

W przypadku umów dotyczących przetwarzania w chmurze, szczególnego znaczenia nabiera prawidłowe i precyzyjne określenie wynagrodzenia za świadczenie usług. W przypadku umów długoterminowych (a takie będą najczęściej umowy przetwarzania w chmurze) należy pamiętać o mechanizmach ewentualnych zmian bądź indeksacji wynagrodzenia.

Istotne jest, aby pamiętać o wynagrodzeniu za ewentualne korzystanie z autorskich praw majątkowych, prawa do wykonywania autorskich praw zależnych i prawa do zlecania wykonywania zależnych praw autorskich w sytuacjach, w których może być mowa o prawach autorskich (szczególnie jeśli usługodawca będzie tworzył specjalne rozwiązania, będące utworami w znaczeniu prawa autorskiego).

2.5.9. Kary umowne, ograniczenie odpowiedzialności

Umowy outsourcingowe zawierają częstokroć premie finansowe, które mają motywować usługodawcę do jak najszybszego dostarczenia usługi wolnej od wad, a także kary umowne mające na celu zdyscyplinowanie usługodawcy i zabezpieczenie sprawnego wyrównania ewentualnych szkód usługobiorcy.

Strony mogą (lecz nie muszą) wyłączyć możliwość dochodzenia odszkodowania przewyższającego wysokość kar umownych na podstawie zasad ogólnych kodeksu cywilnego.

Zgodnie z przepisami kodeksu cywilnego, można dochodzić szkody rzeczywistej, czyli szkody, która rzeczywiście nastąpiła, oraz z tytułu utraconych korzyści, czyli korzyści, jakich spodziewał się poszkodowany, ale których nie osiągnął z uwagi na to, że naruszający nie wykonał swego zobowiązania i przez to wyrządził mu szkodę uniemożliwiającą ich osiągnięcie.

Utrudnieniem konstrukcji odpowiedzialności cywilnej w kodeksie cywilnym jest to, iż podmiot podnoszący roszczenia odszkodowawcze na takiej podstawie ma obowiązek wykazania wysokości szkody lub utraconej korzyści (co często jest utrudnione czy wręcz niemożliwe), wykazania zdarzenia, które

spowodowało szkodę, oraz udowodnienia relewantnego związku przyczynowo-skutkowego między zdarzeniem oraz szkodą lub utraconą korzyścią.

W przypadku dochodzenia zapłaty kar umownych, standardowo wystarczającą podstawą prawną jest sama umowa zawierająca postanowienie o takich karach, oraz ewentualnie wykazanie zdarzenia, które leży w hipotezie takiego postanowienia.

Strony umowy mogą dość swobodnie (i często to czynią) ograniczyć swoją wzajemną odpowiedzialność np. przez odniesienie się do wartości umowy. Spotyka się także formy mieszane, tj. za część ewentualnych naruszeń strony są odpowiedzialne w sposób ograniczony, a za część (przykładowo naruszenie postanowień w kwestii danych osobowych lub praw autorskich) odpowiedzialność pozostaje nieograniczona.

2.5.10. Wniosek w celu przetwarzania danych

W związku z regulacją art. 19 ust. 2 ustawy o działalności ubezpieczeniowej, w ramach stosunku prawnego łączącego zakład ubezpieczeń i usługodawcy rozwiązań *cloud computing*, usługodawca powinien złożyć odpowiedni wniosek w celu przetwarzania danych stanowiących tajemnicę ubezpieczeniową. Przepisy ustawy o działalności ubezpieczeniowej nie precyzują jednak, jakie elementy taki wniosek ma zawierać. Nie ma w każdym razie przeszkód, aby wniosek ten był ujęty w treści umowy i wskazywał taki zakres danych, jaki będzie przetwarzany na podstawie umowy.

2.5.11. Dane osobowe

Istotne jest, aby dane przetwarzane w chmurze spełniały warunki zgodnego z prawem przetwarzania na podstawie ustawy o ochronie danych osobowych. W tym zakresie znaczenie ma ustalenie, która ze stron będzie pełniła rolę administratora danych osobowych. Jeżeli infrastruktura, która leży u podstawy chmury obliczeniowej, jest poza terytorium RP, powinna ona znajdować się w państwie, które zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. Z tej również przyczyny ważne jest, aby umożliwić geolokalizację zasobów informatycznych, które są wykorzystywane do przetwarzania danych osobowych.

2.5.12. Odstąpienie, rozwiązanie umowy

Podstawową różnicą między odstąpieniem od umowy a jej rozwiązaniem za wypowiedzeniem lub bez wypowiedzenia jest to, że odstąpienie od umowy pociąga za sobą skutki od jej zawarcia (skutek wsteczny – *ex tunc*), a rozwiązanie odnosi skutek od dnia wypowiedzenia/powiadomienia drugiej strony (skutek na przyszłość – *ex nunc*). Odstąpienie będzie oznaczało, iż strony będą musiały zwrócić to, co sobie świadczyły na podstawie umowy, a umowę pod względem formalnym traktuje się jak niezawartą. W praktyce odstąpienie od umowy w przypadku umów przetwarzania w chmurze w zasadzie nie będzie występowało.

Rozwiązanie umowy może zależeć od wielu zdarzeń – zawinionych przez strony, takich jak zwłoka, wadliwe wykonywanie przedmiotu umowy, wady prawne, bądź od nich niezależnych, takich jak zdarzenia związane z siłą wyższą, itp.

2.5.13. Spory i ADR

W celu uniknięcia przyszłych wątpliwości praktyką i rekomendacją jest wskazanie prawa właściwego oraz jurysdykcji, w ramach której ewentualne spory będą rozstrzygane.

W tym zakresie spotyka się najczęściej zapisy na sądy polubowne, arbitraż lub inne alternatywne metody rozwiązywania sporów. Popularnością cieszą się tzw. procedury eskalacyjne, w ramach których strony ustawiają w swoich organizacjach stopnie, które spór „musi przejść", zanim będzie rozpatrywany przez sąd.

2.6. Postanowienia umowne dotyczące odpowiedzialności za dane; *Business Continuity Planning*; redundantność systemów; *Recovery Point Objective/ Recovery Time Objective*; *exit plan*, odwracalność – kwestia kompatybilności i konwersji danych

2.6.1. *Business Continuity Planning*

W zakresie procesów tzw. *Business Continuity Planning* istotne znaczenie mają wymagania dotyczące redundantności systemów, np. klimatyzacji, podłączenia do sieci energetycznej, dostępu do sieci Internet o określonej przepustowości od różnych dostawców, urządzeń typu firewall, itp.

W tym celu ustanawiane są również tzw. RPO/RTO (*Recovery Point Objective/Recovery Time Objective*). *Recovery Point Objective* stanowi akceptowalną przez strony ilość danych utraconych w trakcie nieprzewidzianego zdarzenia. Natomiast poprzez *Recovery Time Objective* wyznacza się maksymalny czas na wznowienie i przywrócenie usługi po awarii lub innych zakłóceniach.

W przypadku istotnych zagrożeń lub zakłóceń w świadczeniu usług przetwarzania w chmurze, z myślą o usługobiorcy tworzy się tzw. *exit plan*, zakładający możliwość przeniesienia przetwarzanych danych oraz świadczenia usług na podmiot trzeci. Może to jednak powodować powstanie nadmiernych kosztów po stronie usługodawcy, który nie dość, że może być dotknięty nieprzewidzianym zdarzeniem, zobowiązany jest do przeniesienia plików na nowego usługodawcę. Podobnie jak w przypadku odwracalności, może to skutkować problemami z kompatybilnością oraz konwersją plików. W celu zabezpieczenia jakości przeniesienia, tak jak w procesie odwracalności, standardowo wyznaczany jest tzw. manager wyjścia.

2.6.2. Odwracalność

W przypadku wypowiedzenia umowy lub rozwiązania stosunku umownego w inny sposób naturalnym oczekiwaniem usługobiorcy, wydawałoby się, jest odzyskanie swoich danych. Jednakże, z racji tego, iż owe dane lub oprogramowanie funkcjonowały w środowisku informatycznym usługodawcy, materiały te mogą nie być kompatybilne ze środowiskiem pracy usługobiorcy. Częstym rozwiązaniem takiego problemu jest konwersja plików (co jednak może być czaso- i pracochłonne) bądź też takie stworzenie usługi przetwarzania w chmurze, u podstaw której leżałaby interoperacyjność systemów usługobiorcy i usług *cloud computing*.

2.7. *Service Level Agreement*

Service Level Agreement, czyli umowa lub postanowienia umowne dotyczące jakości świadczonych usług, zawierają postanowienia dotyczące wymaganych poziomów niezawodności pod względem konkretnych parametrów technicznych lub zakresów czasowych dostępności usług.

Postanowienia te są tworzone w celu zapobiegania lub minimalizacji zagrożeń dla usługobiorcy, płynących z korzystania z usług *cloud computing*. Do tych zagrożeń zalicza się m.in.:

- Ryzyko braku dostępu do danych lub ich utrata;
- Brak fizycznej kontroli użytkownika nad danymi;
- Przerwy w dostępie do danych oraz aplikacji;
- Brak odpowiedniego szyfrowania.

Z powodu tych zagrożeń postanowienia SLA z reguły zabezpieczają usługobiorcę bardziej, aniżeli miałoby to miejsce w przypadku klasycznej umowy wdrożeniowej czy „standardowego" outsourcingu.

W zależności od stopnia skomplikowania usług, aplikacji, przetwarzania danych, SLA w różnym stopniu może zabezpieczać jakość świadczeń usługodawcy. Co do kwestii poziomu staranności usługodawcy, zwykle zastrzega się najwyższy lub inny szczególny poziom profesjonalnej staranności, także poprzez wskazanie kodeksu dobrych praktyk, np. Dobre standardy branży outsourcingowej (standardy International Association of Outsourcing Professional – IAOP), ewentualnie przyszły *soft law* – wytyczne Komisji Europejskiej.

Wyznaczane są okresy, w ramach których usługa ma być świadczona bez zakłóceń (z reguły jest to 99–99,95% czasu dostępności usługi w ciągu danego roku lub miesiąca kalendarzowego). Dla nieprzewidzianych przestojów w dostarczaniu usług, przewidywane są odrębne okresy.

W usługach typu *cloud computing* umowy SLA mogą rozciągać się również na oprogramowanie klienckie, tj. oprogramowanie funkcjonujące u usługobiorcy, umożliwiające mu dostęp do usług w ramach przetwarzania w chmurze. Mogą się tu pojawiać kwestie związane z interoperacyjnością, bezpieczeństwem w wykorzystywaniu niektórych technologii, np. mobilnych.

2.7.1. Minimalne poziomy usług

Poza ujęciem czasowym, umowy SLA wyznaczają minimalne poziomy szybkości przetwarzania danych, mocy obliczeniowej lub dostępnej pamięci operacyjnej, procesorów lub rdzeniów procesorów, itp.

Dla usługobiorcy istotne są usługi backup oraz redundantność systemów obsługujących serwery, na których odbywa się przetwarzanie. W zależności od stopnia zaawansowania usługi przetwarzania w chmurze oraz zakresu *back-up*, kopie bezpieczeństwa są określane z częstotliwością liczoną w dniach, tygodniach lub nawet miesiącach.

W negocjacjach umów *cloud computing* problematyczne jest często ustalenie, kto ma ponosić koszty oraz ryzyko związane z przechowywaniem kopii zapasowej.

2.7.2. Błędy

Błędy w działaniu usług są usuwane w ramach czasowych właściwych dla danej zdefiniowanej kategorii błędu (np. drobna usterka – 48 h, błąd krytyczny – 4 h). Istotna jest procedura przyjmowania błędów, tj. w jakiej formie błąd ma być opisany, jaka osoba jest władna do wysłania zawiadomienia do usługodawcy o błędzie.

2.8. Prawa autorskie

Niektóre modele *cloud computing*, konkretnie *Platform as a service* (PaaS) oraz *Software as a service* (SaaS), zakładają dostęp usługobiorców do aplikacji i oprogramowania, które funkcjonuje i jest uruchamiane w ramach infrastruktury sprzętowej usługodawcy. Zatem technicznie rzecz ujmując, usługobiorca ma dostęp do korzystania z danego oprogramowania, jednak samo to oprogramowanie nie jest odtwarzane ani uruchamiane, ani w większości przypadków nie znajduje się nawet w pamięciach urządzeń usługobiorcy.

Kwestia, czy w ramach c*loud computing* dochodzi do korzystania z praw autorskich, szczególnie w usługach typu SaaS i PaaS, wywołuje spory wśród prawników, a może mieć niebagatelne znaczenie, zwłaszcza w aspekcie ewentualnych naruszeń tych praw, a także w aspekcie podatkowym. Odpowiedź na to pytanie nie jest przedmiotem raportu i może zależeć od precyzyjnej analizy konkretnego rozwiązania i przyszłego stanowiska judykatury. Warto w tym miejscu jedynie zaznaczyć, iż co do zasady zgodnie z art. 74 ust. 1 ustawy o prawie autorskim:

> *Programy komputerowe podlegają ochronie jak utwory literackie.*

Aby takiej ochronie podlegać, program komputerowy musi zostać uznany za utwór w rozumieniu ustawy, tj. stanowić przejaw działalności twórczej człowieka o indywidualnym charakterze, niezależnie od formy jego ustalenia.

Warto tu natomiast wspomnieć, iż zarówno polskie orzecznictwo, jak i Trybunał Sprawiedliwości UE uznały, iż kod źródłowy i wynikowy podlegają ochronie prawno-autorskiej, lecz zbiór funkcjonalności, język programowania i format plików używanych w programie komputerowym nie są wyrażeniem programu i poprzez to nie podlegają ochronie prawno-autorskiej.

Orzecznictwo zatem wydaje się wdrażać zasadę prawa autorskiego, iż nie są objęte ochroną odkrycia, idee, procedury, metody i zasady działania oraz koncepcje matematyczne.

2.8.1. Treść autorskich praw majątkowych do programu komputerowego

Autorskie prawa majątkowe będące treścią uprawnień do programu komputerowego opisane są w art. 74 ust. 4 ustawy o prawie autorskim i prawach pokrewnych i obejmują prawo do:

1) *trwałego lub czasowego zwielokrotnienia programu komputerowego w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie; w zakresie, w którym dla wprowadzania, wy-*

świetlania, stosowania, przekazywania i przechowywania programu komputerowego niezbędne jest jego zwielokrotnienie, czynności te wymagają zgody uprawnionego;

2) *tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym, z zachowaniem praw osoby, która tych zmian dokonała;*
3) *rozpowszechniania, w tym użyczenia lub najmu, programu komputerowego lub jego kopii.*

Powyższe wyliczenie ma charakter wyczerpujący (z tym zastrzeżeniem, że powyższe co do zasady nie wyłącza art. 50 ustawy, który zawiera generalne wyliczenie pól eksploatacji, z których część może mieć zastosowanie do programów komputerowych).

3. Przetwarzanie danych osobowych w chmurze

Dla zapewnienia właściwego i zgodnego z prawem przetwarzania danych osobowych w chmurze konieczne jest rozstrzygnięcie kilku kwestii, które przy tradycyjnym przetwarzaniu, co do zasady, nie nastręczają większych wątpliwości, natomiast ze względu na specyfikę *cloud computing* wymagają pogłębionej analizy. W szczególności dotyczy to rozstrzygnięcia, w jakiej roli występują poszczególne podmioty uczestniczące w przetwarzaniu oraz jaki jest ich zakres obowiązków i odpowiedzialności wynikający z przepisów regulujących przetwarzanie danych osobowych.

Poniższe uwagi nie stanowią próby wyczerpującego opisu systemu ochrony danych osobowych, a jedynie wskazują na te aspekty przetwarzania danych, które są specyficzne dla chmury obliczeniowej.

3.1. Funkcje pełnione przez poszczególne podmioty przy przetwarzaniu danych

Podmioty biorące udział w przetwarzaniu danych można sklasyfikować jako administratorów danych lub jako przetwarzających dane, którym powierzono przetwarzanie danych. Zależy to od pełnionych funkcji.

Obowiązująca Dyrektywa o ochronie danych UE (95/46/WE) jako administratora danych określa:

> *osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania.*

Podążając dalej za wskazaną Dyrektywą, przetwarzającym dane (procesorem) jest:

> *osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami przetwarza dane osobowe w imieniu administratora.*

Polska ustawa o ochronie danych osobowych („uodo") nawiązuje do definicji unijnych, m.in. poprzez zdefiniowanie „administratora danych" jako:

> *organ, jednostkę organizacyjną, podmiot lub osobę [E] decydujących o celach i środkach przetwarzania danych osobowych*[4].

Natomiast za „przetwarzającego dane" uważa się:

> *podmiot, któremu powierzono przetwarzanie danych w drodze umowy zawartej na piśmie (art. 31 uodo) – procesor zatem to podmiot, który przetwarza dane dla potrzeb administratora na jego zlecenie.*

4. Por. art. 7 ustawy z dnia 29 sierpnia 1997 r. – ustawa o ochronie danych osobowych (Dz. U. z 2011 Nr 230, poz. 1371).

3.2. Obowiązki klienta usług świadczonych w chmurze i dostawcy takich usług

Biorąc pod uwagę powyższą klasyfikację, można przypisać odpowiednie funkcje, a także wynikające z nich obowiązki, głównym podmiotom biorącym udział w przetwarzaniu danych w chmurze – klientowi usług świadczonych w chmurze oraz dostawcy takich usług.

Co do zasady, uznaje się, że to do użytkownika należy określenie celu przetwarzania danych, a zatem jego uznaje się za administratora danych – jakkolwiek w środowisku chmury nie jest to jednoznaczne (dostawca usług, udostępniając określone oprogramowanie czy środki sprzętowe, określa, jakimi metodami dane mogą być przetwarzane, a w wielu przypadkach funkcjonalności udostępnionych usług informatycznych będą determinować również cel przetwarzania).

Z tytułu pełnienia funkcji administratora danych ciąży na kliencie usługi w chmurze główna odpowiedzialność za przestrzeganie przepisów w zakresie ochrony danych osobowych, choć zakres jego obowiązków jest modyfikowany przez specyfikę działania w chmurze.

Dostawca usługi w chmurze uznany winien być za przetwarzającego dane w zakresie, w jakim dostarcza środki oraz platformę swojemu klientowi. Jak uznano w Opinii nr 5/2012 Grupy Roboczej Art. 29:

> *rolą dostawcy usług w chmurze będzie rola wykonawcy względem klienta*[5].

Do obowiązków dostawcy usług w chmurze należy zapewnienie poufności. Zgodnie z Dyrektywą 95/46/WE:

> *żadna osoba działająca z upoważnienia administratora danych lub przetwarzającego, włączając samego przetwarzającego, która ma dostęp do danych osobowych, nie może przetwarzać ich bez polecenia administratora danych, chyba że wymaga tego prawo.*

W polskiej praktyce przyjmuje się, że dostawca usług w chmurze może, po spełnieniu określonych warunków, dokonać dalszego powierzenia przetwarzania, niejako „podpowierzyć" dane innym podmiotom. W takiej sytuacji procesor powinien uzyskać uprzednią zgodę administratora danych.

3.3. Wymogi w zakresie ochrony danych w relacji klient–dostawca

Zapewnienie legalności przetwarzania danych wiąże się z koniecznością dołożenia przez administratora szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.

Zgodnie z art. 26 uodo, na administratorze danych ciąży obowiązek zapewnienia, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych zgodnie z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, a także przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

5. Opinia nr 5/2012 Grupy Roboczej Art. 29 ds. Ochrony Danych w sprawie przetwarzania danych w chmurze obliczeniowej, s. 11.

Klient usługi w chmurze, działający w charakterze administratora danych, zobowiązany jest do przekazania osobie, której dane dotyczą, określonych informacji. Administrator danych, w przypadku zbierania danych osobowych od osoby, której one dotyczą, zobowiązany jest poinformować tę osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, prawie dostępu do treści swoich danych oraz ich poprawiania, a także dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

W przypadku gdy dane zbierane są od osoby, której one nie dotyczą, administrator danych jest zobowiązany poinformować tę osobę również o źródle danych, a także szczególnych uprawnieniach wynikających z przepisów prawa[6].

Przejrzystość przetwarzania danych osobowych odnosi się także do aspektów technologicznych. W tym ujęciu mówi się m.in. o rozliczalności przetwarzania danych osobowych.

Cele przetwarzania danych osobowych muszą być legalne, jednoznaczne oraz określone przed rozpoczęciem zbierania danych, a osoba, której dotyczą gromadzone dane, musi zostać o nich należycie poinformowana. Wobec tego, za niedopuszczalne należy uznać przetwarzanie danych osobowych w sposób niezgodny ze wskazanymi celami oraz w innych celach aniżeli pierwotne.

Przechowywanie danych osobowych wiąże się z koniecznością zapewnienia, aby dane osobowe, które nie są już potrzebne, zostały usunięte. Podmiotem zobowiązanym do zapewnienia usunięcia danych osobowych po ustaniu celu ich przechowywania jest administrator danych, to jest klient usługi świadczonej w chmurze. Zgodnie z opinią Grupy Roboczej z Art. 29:

> *klient usługi w chmurze powinien zadbać o to, aby dostawca usługi w chmurze zapewnił bezpieczne usuwanie [...] oraz aby umowa pomiędzy dostawcą a klientem zawierała wyraźne postanowienie dotyczące usuwania danych osobowych*[7].

3.4. Zabezpieczenie umowne relacji klient–dostawca usługi

Administratorzy danych decydujący się na powierzenie przetwarzania danych w chmurze zobowiązani są do wybrania przetwarzającego, który zapewni wystarczające techniczne i organizacyjne środki bezpieczeństwa. Wobec tego są jednocześnie zobowiązani do zawarcia umowy z dostawcą usługi przetwarzania danych w chmurze (lub włączenia odpowiednich klauzul do innej wiążącej strony umowy). Umowa lub jej części dotyczące ochrony danych i wymogów w zakresie środków technicznych i organizacyjnych powinny zostać sporządzone na piśmie lub w innej równoważnej formie (np. z kwalifikowanym podpisem cyfrowym).

6. Por. art. 24 i 25 uodo.
7. Opinia nr 5/2012 Grupy Roboczej Art. 29 (op. cit.), s. 17.

Zgodnie z Opinią nr 5/2012:

> *umowa musi co najmniej ustanawiać fakt, w szczególności, że przetwarzający ma przestrzegać instrukcji administratora oraz że przetwarzający (procesor) musi wdrożyć środki techniczne i organizacyjne, aby odpowiednio chronić dane.*[8]

Art. 31 uodo w dalszych ustępach mówi, iż podmiot, któremu powierzono przetwarzanie danych, może je przetwarzać wyłącznie w zakresie i celu przewidzianym w umowie. Ponadto przetwarzający jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych oraz spełnić wymagania określone w innych przepisach. W zakresie przestrzegania tych przepisów podmiot przetwarzający ponosi odpowiedzialność jako administrator danych. Tak więc, choć co do zasady odpowiedzialność za przestrzeganie przepisów uodo spoczywa na administratorze danych, nie wyłącza to odpowiedzialności podmiotu, któremu powierzono przetwarzanie.

Jakkolwiek dla wypełnienia ustawowych minimalnych warunków powierzenia danych wystarczy w umowie wskazanie celu i zakresu przetwarzania, Grupa Robocza Art. 29 sformułowała wytyczne dotyczące wymogów, którym powinna odpowiadać umowa między usługobiorcą a usługodawcą usług w chmurze, a które mogą okazać się pomocne przy konstruowaniu takich umów. W szczególności:

i. Umowa powinna zawierać szczegółowe informacje na temat zakresu, w jakim usługobiorca powierza przetwarzanie danych, obiektywne i wymierne informacje o gwarantowanym poziomie usług oraz o sankcjach za ewentualne naruszenia;
ii. Umowa powinna wskazywać środki bezpieczeństwa, do których stosować się musi usługodawca w chmurze – środki te powinny być adekwatne do zagrożeń związanych z przetwarzaniem i do charakteru danych. Istotne jest, aby wskazane zostały konkretne środki techniczne i organizacyjne;
iii. Umowa musi określać ramy czasowe świadczenia usługi, zakres, sposób i cel przetwarzania, jak również rodzaje przetwarzanych danych osobowych;
iv. Umowa powinna regulować zasady zwrotu danych lub zniszczenia danych po zakończeniu realizacji usługi. Ponadto powinna zapewnić, aby dane osobowe były usuwane, jeżeli wniesie o to klient;
v. Umowa powinna zawierać klauzulę poufności, wiążącą zarówno usługodawcę w chmurze, jak i wszelkich jego pracowników, którzy mogą mieć dostęp do danych;
vi. Umowa powinna zobowiązywać dostawcę usługi do wspierania klienta w wykonywaniu jego obowiązków, jako administratora, w tym obowiązku zapewnienia podmiotom danych (innych niż sam klient) prawa dostępu do swoich danych, ich poprawienia i usunięcia;
vii. Umowa powinna wyraźnie stanowić, że dostawca usługi w chmurze nie może przekazywać danych stronom trzecim, chyba że umowa przewiduje możliwość dalszego powierzenia przetwarzania. Podpowierzenie zawsze wymaga zgody klienta. Należy również zapewnić, aby umowy między dostawcą usługi a podmiotem, któremu podpowierzono jej realizację, odzwierciedlały postanowienia umowy między klientem a dostawcą;
viii. Umowa powinna wskazywać na obowiązek usługodawcy zawiadomienia klienta o wszelkich przypadkach naruszeń ochrony danych;

8. Opinia nr 5/2012 Grupy Roboczej Art. 29 (op. cit.), s. 17.

ix. Umowa powinna nakładać na usługodawcę obowiązek wskazania klientowi listy lokalizacji, w których dostawca będzie dane przetwarzał;
x. Umowa powinna zapewniać klientowi prawo do monitorowania i kontroli przetwarzania przez usługodawcę;
xi. Umowa powinna nakładać na usługodawcę obowiązek informowania klienta o istotnych zmianach dotyczących świadczonej usługi, np. takich jak wdrożenie dodatkowych funkcji;
xii. Umowa powinna przewidywać rejestrowanie i kontrolowanie istotnych operacji przetwarzania danych osobowych, które są dokonywane przez dostawcę usługi w chmurze lub podmioty, którym podpowierzono ich realizację;
xiii. Umowa powinna nakładać na usługodawcę obowiązek zawiadamiania klienta o każdym prawnie wiążącym wniosku o udostępnienie danych osobowych przez organ egzekwowania prawa, o ile nie jest zakazane w inny sposób, na przykład na mocy prawa przepisów szczególnych.

3.5. Środki techniczne i organizacyjne w zakresie ochrony danych i bezpieczeństwa danych w chmurze

Zapewnienie technicznych i organizacyjnych środków bezpieczeństwa mających na celu ochronę danych osobowych należy do obowiązków usługodawcy, to jest podmiotu przetwarzającego dane.

W przypadku przetwarzania w chmurze dostępność danych może napotkać liczne zagrożenia, takie jak przypadkowa utrata połączenia, uszkodzenie sprzętu, awarie zasilania oraz inne problemy z funkcjonowaniem rozwiązań technicznych i infrastrukturalnych. W związku z tym konieczne jest zastosowanie środków zapewniających ciągłość świadczenia usługi (np. zapewnienie zapasowych łączy internetowych, nadmiarowe zasoby czy skuteczne mechanizmy wykonywania kopii zapasowych).

Innym kluczowym celem w zakresie bezpieczeństwa danych jest integralność, czyli:

> *fakt, że dane są prawdziwe i nie zostały celowo lub przypadkowo zmienione podczas przetwarzania, przechowywania lub przekazywania*[9] *wymaga zastosowania odpowiednich środków pozwalających na wykrycie niepożądanych ingerencji w treść danych. Środkami takimi mogą być np. mechanizmy uwierzytelniania kryptograficznego. Wymagane jest również stosowanie mechanizmów służących wykrywaniu lub zapobieganiu włamaniom do systemu.*

W zakresie zapewnienia poufności danych wymogi, które zgodnie z wytycznymi Grupy Roboczej Art. 29 powinien spełnić dostawca usług w chmurze, to szyfrowanie stosowane zarówno wobec „danych w tranzycie", jak i danych przechowywanych na serwerach, oraz mechanizmy autoryzacji.

Inną istotną kwestią o doniosłym znaczeniu praktycznym jest zapewnienie przez dostawcę usług w chmurze odpowiednich środków pozwalających klientowi usługi na przeniesienie danych od jednego dostawcy usługi w chmurze do innego.

9. Opinia nr 5/2012 Grupy Roboczej Art. 29 (op. cit.), s. 21.

Z punktu widzenia odpowiedzialności poszczególnych podmiotów istotne jest również zapewnienie, aby platforma *cloud computing* umożliwiała wiarygodny monitoring i mechanizmy rejestrowania działań na danych osobowych, pozwalające na identyfikację wszystkich operacji przetwarzania danych i przypisania do nich podmiotu, który je podjął.

3.6. Zasady przekazywania danych osobowych za granicę – do państw członkowskich EOG lub do państw trzecich

W związku z brakiem stałej lokalizacji danych w ramach sieci dostawcy usługi w chmurze, szczególny problem stanowi stosowanie regulacji dotyczących przekazywania danych do państw trzecich (spoza EOG), niezapewniających odpowiedniej ochrony danych osobowych.

Co do zasady, przepisy europejskie, w tym polskie, mocno ograniczają możliwość przekazywania danych do państw trzecich niezapewniających takiego samego poziomu ich zabezpieczenia, jak państwa członkowskie UE (czyli w praktyce niemal do wszystkich pozostałych państw świata), obwarowując taki transfer licznymi wymogami i warunkami.

Jednakże w przypadku przetwarzania w chmurze serwery, na których umieszczone są aplikacje, mogą znajdować się w dowolnym miejscu (a dane między nimi swobodnie przepływać), ponadto użytkownicy mają dostęp do danych z każdego miejsca na świecie, z którego tylko można połączyć się z siecią internetową. „Geograficzna" koncepcja ochrony się tu nie sprawdza i nie może znaleźć zastosowania.

Wobec tego wyraźna staje się potrzeba rozwiązania problemu transgranicznego przetwarzania danych w drodze legislacyjnej.

3.7. Wytyczne dla klientów i dostawców usług przetwarzania w chmurze

Opinia nr 5/2012 Grupy Roboczej Art. 29 zawiera pewne szczegółowe wytyczne dla klientów i dostawców usług przetwarzania danych w chmurze, w tym:

i. Relacja administrator – przetwarzający: Grupa Robocza Art. 29 podkreśliła, że mogą istnieć sytuacje, gdy dostawca usług w chmurze, generalnie pełniący funkcję przetwarzającego dane, pełnić będzie funkcję administratora danych, a mianowicie podczas przetwarzania danych dla własnych celów. Wiąże się to z ponoszeniem przez dostawcę usług w chmurze pełnej odpowiedzialności za przetwarzanie danych oraz z koniecznością spełnienia zobowiązań przewidzianych przez dyrektywę 95/46/WE.
ii. Przestrzeganie podstawowych zasad ochrony danych:
    - Przejrzystości;
    - Określenia i ograniczenia celu;
    - Zatrzymywania danych.
iii. Zabezpieczenia umowne:
    - Transgraniczne przekazywanie danych: konieczność zapewnienia przez klienta sprawdzenia, czy dostawca usług w chmurze gwarantuje legalność transgranicznego przekazywania danych oraz daje klientowi możliwość ograniczenia przypadku przekazywania danych do wybranych krajów;
    - Rejestrowanie i kontrolowanie przetwarzania: wymóg rejestrowania operacji przetwarzania danych;

- Środki techniczne i organizacyjne: eliminacja lub złagodzenie zagrożeń wynikających z braku kontroli i braku informacji (zapewnienie środków mających na celu zapewnienie dostępności, integralności, poufności, odizolowania, możliwości interwencji i przenoszenia danych).

3.8. Spodziewane zmiany regulacji ochrony danych osobowych i działalności ubezpieczeniowej

Należy spodziewać się, iż na przestrzeni nadchodzących lat regulacja istotnie się zmieni. Dyrektywa 95/46 oraz uodo mają zostać zastąpione ogólnym rozporządzeniem o ochronie danych osobowych, które ujednolici w pełni regulacje w całej UE.

Należy także uwzględnić zmiany regulacji wchodzące w życie wraz z Dyrektywą 2009/138/WE opisane w punkcie 2.3, w szczególności w zakresie wymogów, jakie musi spełniać outsourcing czynności ubezpieczeniowych, odpowiedzialności zakładów ubezpieczeń za czynności powierzone w ramach outsourcingu oraz poddania podmiotów wykonujących usługi na rzecz ubezpieczycieli, w tym także tych z siedzibą za granicą, nadzorowi ubezpieczeniowemu.

4. Dobre standardy w kontekście *cloud computing*

Outsourcing Professional Body of Knowledge (dalej: OPBOK) jest dokumentem wydanym przez International Association of Outsourcing Professionals (dalej: IAOP)[10].

Jest zaadresowany do podmiotów związanych z outsourcingiem na wszystkich szczeblach wdrażania usługi – zarówno do usługodawców i usługobiorców, jak i doradców w dziedzinie outsourcingu. Opisuje, czym jest outsourcing oraz jak wpasowuje się on we współczesną działalność biznesową.

OPBOK ponadto dostarcza wiedzę o obszarach powszechnie uznawanych za krytyczne w skutecznym wdrożeniu outsourcingu. Częścią OPBOK są Dobre standardy branży outsourcingowej International Association of Outsourcing Professional IAOP [11] (dalej: Standardy).

O ile obecnie nie istnieją zapisane standardy dotyczące konkretnie usług przetwarzania w chmurze[12], to z racji tego, że *cloud computing* może być uznany za rodzaj outsourcingu, mogą mieć do niego zastosowanie pokrótce opisane poniżej Standardy.

4.1. Definicje i założenia umowy zgodnie ze Standardami

W Standardach podkreśla się konieczność definiowania outsourcingu za pomocą terminów zrozumiałych dla osób zaangażowanych w świadczenie usług outsourcingu, a także dla innych osób, łącznie z akcjonariuszami i ogółem ludności. Standardy określają przede wszystkim, na co usługodawcy powinni zwracać uwagę przy tworzeniu umów oraz przy wykonywaniu usług outsourcingu. Zgodnie ze Standardami istotne jest:

- Stworzenie definicji terminów często występujących w outsourcingu (np. *Business Process Outsourcing* – BTO czy *Information Technology Outsourcing* – ITO), form outsourcingu – rozróżnienie pomiędzy outsourcingiem, offshoringiem i offshore outsourcingiem;
- Zidentyfikowanie potencjału rynku, możliwości usług i usługodawców i utworzenie studium przypadków dla różnych form outsourcingu, w tym: analizy porównawczej, wykorzystania wiedzy rynkowej w zdefiniowaniu strategii outsourcingowej i celów dla usługobiorcy lub usługodawcy;
- Zdefiniowanie zewnętrznych i wewnętrznych czynników biznesowych, takich jak rozwój konkurencji, globalizacja, rozwój technologii, zmiany w przepisach prawa; ram czasowych (*timeframes*) i spodziewanych korzyści wynikających z outsourcingu, takich jak: obniżenie kosztów, zwiększenie

10. http://www.iaop.org/Content/19/206/3040.
11. http://www.iaop.org/Download/Default.aspx?ID=556.
12. Standardy są obecnie tworzone niezależnie przez różne organizacje, por. w szczególności: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500–291_Jul15A.pdf; http://www.information-management.com/news/cloud-computing-standards-security-SLA-OMG-DMTF-10021934–1.html.

skupienia na istotnych przedmiotach działalności, możliwość skorzystania z usług ekspertów niedostępnych wewnętrznie dla usługobiorcy;

- Umiejętność usługobiorcy do określenia powszechnych zagrożeń i wyzwań dla osiągnięcia powodzenia w korzystaniu z usług outsourcingu, m.in. poprzez określenie realistycznych oczekiwań, odpowiedni wybór rodzaju outsourcingu, który z największym prawdopodobieństwem pozwoli na osiągnięcie zamierzonych przez usługobiorcę celów; wybór najbardziej doświadczonych usługodawców; określenie wewnętrznych przeszkód przed powierzeniem procesów biznesowych do outsourcingu ze względu na obawę przed utratą kontroli, negatywną postawą klienteli, pracowników lub ogółu ludności; potrzeba identyfikacji procesów biznesowych, które są zbyt istotne dla działalności usługodawcy, aby mogły być przedmiotem outsourcingu.

4.2. Modele zgodnie ze Standardami

W Standardach zwraca się uwagę na konieczność opracowania i zarządzania całościowym procesem outsourcingu. Konieczne jest w tym procesie wybranie modelu outsourcingu (np. wybór jednego dostawcy lub wielu dostawców). W trakcie opracowywania procesu wdrażania outsourcingu należy precyzyjnie zaplanować wszystkie jego etapy – od procesu oceny usługi, przez wdrożenie, aż do zarządzania outsourcingiem. Podkreśla się również istotę umiejętność oceny i rozwoju zdolność usługobiorcy do outsourcingu kolejnych procesów biznesowych.

4.3. Zmiany i zespoły projektowe

Standardy ponadto zwracają uwagę na istotność analizy możliwości korzystania z usług outsourcingu w perspektywie aktualnego stanu prawnego, m.in. Sarbanes-Oxley, HIPAA, regulacji dotyczących prywatności, ze szczególnym uwzględnieniem dyrektyw UE dotyczących ochrony danych osobowych.

Zaleca się również wdrożenie odpowiednich mechanizmów pozwalających na zarządzanie zmianami w organizacji usługobiorcy oraz zapewniających efektywną komunikację tych zmian wobec personelu.

IAOP w Standardach wskazuje także na konieczność tworzenia specjalistycznych zespołów projektowych, które będą odpowiedzialne za poszczególne etapy każdego z projektów outsourcingowych.

4.4. Cele i rezultaty usług zgodnie ze Standardami

Ważne jest jasne określenie celów i wymaganych rezultatów.

Określone cele należy ująć w jednym lub większej ilości dokumentów, które będą zawierały bieżące i przyszłe wymogi i wybrane kryteria, którymi usługodawca i usługobiorca będą się kierować. W Standardach znalazły się przykładowe dokumenty dotyczące m.in.: oczekiwań w stosunku do potencjalnego dostawcy, zawierających takie czynniki jak to, ile czasu dostawca prowadzi działalność, określenie jego sytuacji finansowej, aktualny zakres świadczonych przez niego usług, listę klientów, a także wykaz cen.

W Standardach wymienia się takie dokumenty zawierające te oczekiwania i cele usługobiorcy, jak zapytania dotyczące informacji (*Request for Information* – RFI), wyceny (*Request for Quotation* – RFQ) oraz zapytanie ofertowe (*Request for Proposal* – RFP).

4.5. Wybór dostawcy zgodnie ze Standardami

Standardy zawierają wskazówki dotyczące wyboru dostawcy usług outsourcingowych.

Przy wyborze dostawcy należy brać pod uwagę model outsourcingu. Usługobiorca powinien utworzyć listę kryteriów potrzebnych do wyboru dostawcy usługi. Przy dokonywaniu wyboru warto posłużyć się wspominanymi wcześniej dokumentami (RFI, RFQ, RFP).

Standardy zawierają wiele technik mających pomóc w wyborze potencjalnego dostawcy usługi, takich jak: wykorzystanie kontaktów biznesowych do określenia, czym zajmuje się konkurencja dostawcy i z kim pracuje, praca z konsultantami i innymi doradcami w wyborze dostawcy, możliwość przeprowadzenia procesu *due diligence* u proponowanego dostawcy.

4.6. Model biznesowy zgodnie ze Standardami

Standardy wskazują, iż należy opracować finansowy model biznesowy zakładający wszystkie konsekwencje finansowe wynikające z procesu wdrażania outsourcingu.

- Istotne jest określenie kosztów bieżących, przewidywanie przyszłych ewentualnych kosztów, które mogą wynikać ze zmian działalności biznesowej, potencjalnych zmian technologii i innych czynników mogących wpływać na sposób przeprowadzania procesu;
- Ponadto należy określić koszty bezpośrednio związane z oceną, planowaniem, wykonywaniem i zarządzaniem stosunkami między usługodawcą i usługobiorcą wynikającymi z zawarcia umów outsourcingowych. W Standardach wymieniono m.in. koszty wynagrodzeń personelu, podróży, dokumentacji, negocjacji i zawierania umowy z dostawcą, wynagrodzenie dla konsultantów, prawników i zewnętrznych doradców. Przy planowaniu kosztów związanych z outsourcingiem trzeba brać pod uwagę także koszty przejściowe, takie jak: jednorazowe inwestycje w nowe technologie i systemy, koszty pokrywające działania podczas okresu wstępnego;
- Oprócz kosztów należy odzwierciedlić w modelu finansowym także korzyści płynące z outsourcingu;
- Konieczna jest ocena i określenie kosztów związanych z ewentualnym zakończeniem współpracy z pierwotnym dostawcą usług outsourcingowych, m.in. ew. kosztów wypowiedzenia umowy, opłat związanych z transferem licencjonowanego oprogramowania, lub materiałów na innego dostawcę, kosztów przeprowadzki ewentualnej infrastruktury, konsekwencji podatkowych;
- Ceny usług muszą zostać określone zgodnie z aktualną i przewidywaną przyszłą kondycją rynku.

4.7. Struktura umów zgodnie ze Standardami

Należy określić strukturę dla umów outsourcingowych przy użyciu odrębnych postanowień umownych dotyczących terminów, zakresu usług i cen.

Należy upewnić się, że wszystkie rozwiązania prawne dla wszystkich jurysdykcji odpowiednich dla umowy zostały wzięte pod uwagę. Zgodnie ze Standardami w postanowieniach umownych należy jasno określić zamiar stron i warunki ich współpracy. Umowa powinna zawierać postanowienia dotyczące:

- Rozwiązania umowy i odstąpienia od niej;
- Wynagrodzenia;
- Kar umownych;
- *Business continuity planning,* ochrony własności intelektualnej.

Konieczne jest określenie tego, jak warunki umowy wpływają na stosowany model współpracy między usługodawcą i usługobiorcą. Przywoływana jest tu możliwość wprowadzenia procesu renegocjacji jako koniecznego etapu przed rozwiązaniem umowy.

Należy także opisać typ i zakres każdej z usług przewidzianych przez umowę, jakość ich świadczenia przez usługodawcę oraz terminy ich wykonania.

W części dotyczącej cen powinny się znaleźć przyjęte zasady kształtowania cen, stawki i terminy zapłaty.

Umowa powinna ponadto objąć postanowienia dotyczące stosunku usługodawcy do pracowników usługobiorcy (wybór, ewentualne wynagrodzenie wyrównawcze).

4.8. Plany przejścia zgodnie ze Standardami

Należy opracować kompleksowy plan przejścia do środowiska objętego outsourcingiem, określający m.in. sposób przeniesienia aktywów, przejścia pracowników, procesów i technologii, zarządzanie zmianami podczas okresu przejściowego, wstępne ramy zarządzania. Istotną kwestią jest określenie procedur przy zmianach kadrowych oraz przewidywanie konsekwencji zmian przepisów prawa pracy.

Konieczna jest ocena potencjalnych reakcji społeczeństwa i mediów oraz zaplanowanie działań mających na celu zminimalizowanie ryzyk z tym związanych.

Należy także ustanowić plan przejścia zwrotnego w razie rozwiązania umowy, włączając plan jako część modelu umowy.

Na zakończenie, Standardy wskazują na istotną umiejętność określenia polityki zarządzania świadczeniem usług outsourcingu oraz należytej implementacji tej polityki.

5. Podsumowanie

5.1. Procesy ubezpieczeniowe w kontekście chmury publicznej, prywatnej i hybrydowej

Ze wskazanych w raporcie rodzajów usług przetwarzania w chmurze, wyodrębnionych ze względu na liczbę podmiotów uprawnionych do korzystania z usługi, do przetwarzania danych ubezpieczeniowych mogą mieć zastosowanie jedynie te chmury, w których dostęp do danych jest ograniczony, a dodatkowo ze względu na wymogi wynikające z przepisów o ochronie tajemnicy ubezpieczeniowej, ograniczenie to co do zasady musi dotyczyć danych należących do jednego ubezpieczyciela. Wymóg ten będzie spełniony w zasadzie jedynie w przypadku chmury prywatnej. Dopuszczalność zastosowania chmury grupowej lub chmury hybrydowej będzie natomiast uzależniona od zastosowania rozwiązań technicznych, które zagwarantują, że dane przekazane przez danego ubezpieczyciela nie będą dostępne dla innych korzystających z chmury.

5.2. Tabela głównych ryzyk związanych z zastosowaniem wybranych modeli *cloud computing*

Model *cloud computing*	Zastosowanie w ubezpieczeniach	Ryzyka
Chmura prywatna	Dopuszczalne	Chmura prywatna charakteryzuje się tym, że pozwala usługobiorcy na ustalenie wspólnie z usługodawcą postanowień umownych, które będą zabezpieczały należycie usługobiorcę pod względem tajemnicy ubezpieczeniowej, właściwego i bezpiecznego przetwarzania danych osobowych oraz postanowień dot. SLA, zarządzania ewentualnymi sytuacjami kryzysowymi, geolokalizację, etc. Nie można wykluczyć, iż mimo odpowiedniej umowy nastąpią sytuacje szczególne, które mogą spowodować: • Ryzyko braku dostępu do danych lub ich utratę; • Brak fizycznej kontroli użytkownika nad danymi, w tym niekontrolowane przeniesienie danych np. poza obszar EOG, np. wskutek zmian organizacyjnych po stronie dostawcy; • Przerwy w dostępie do danych oraz aplikacji. Nawet przy należytym zabezpieczeniu umownym sytuacji kryzysowych nie można wykluczyć problemów z: • Minimalnymi poziomami usług; • Przywracaniem pełnej funkcjonalności usług po sytuacji kryzysowej; • Terminowością i naprawą błędów; • Odwracalnością i konwersją plików.

Chmura prywatna	Dopuszczalne	W kontekście ryzyk chmura prywatna niewiele się różni od klasycznego outsourcingu usług IT. Ponieważ odpowiedzialności zakładu ubezpieczeń za szkody wyrządzone ubezpieczającym, ubezpieczonym, uposażonym lub uprawnionym z umów ubezpieczenia wskutek niewykonania lub nienależytego wykonania outsourcingu nie można wyłączyć ani ograniczyć, zakład ubezpieczeń zawsze będzie ponosił pełną odpowiedzialność wobec tych osób za szkody wyrządzone wskutek niewykonania lub nienależytego wykonania usług przetwarzania w chmurze. W związku z powyższymi ryzykami należy pamiętać o uprawnieniach kontrolnych Komisji Nadzoru Finansowego oraz Generalnego Inspektora Ochrony Danych Osobowych oraz związanej z tym odpowiedzialności za ewentualne naruszenia (w przypadku KNF m.in. kary finansowe). W razie stwierdzenia naruszeń regulacji ochrony danych osobowych istnieje ryzyko, że o ile naruszenia te nie zostaną usunięte w zakreślonym terminie, Generalny Inspektor Danych Osobowych nakaże zaprzestanie przetwarzania danych osobowych w chmurze.
Chmura grupowa/ Chmura hybrydowa	Teoretycznie dopuszczalne warunkowo	Regulacje prawne nie zakazują wprost współdzielenia infrastruktury z innymi podmiotami. Ryzykiem, na które warto zwrócić szczególną uwagę w tym modelu, jest zwiększone prawdopodobieństwo dotarcia do danych przez osobę nieuprawnioną. Z założenia chmura grupowa/hybrydowa zakłada pewne współdzielenie infrastruktury dostawcy przez różnych usługobiorców. Należy zadbać w umowie o odpowiednie postanowienia odnośnie ochrony poufności oraz odpowiedzialności usługodawcy za ewentualny nieuprawniony dostęp do danych. Szczególnie istotny staje się wybór wiarygodnego i zabezpieczonego odpowiednimi standardami dostawcy usług. Jeżeli natomiast chmura grupowa/hybrydowa w swoich cechach jest bliższa chmurze publicznej, istnieje ryzyko braku zapewnienia odpowiedniego poziomu zabezpieczeń związanych z przetwarzaniem danych osobowych oraz danych, które są przedmiotem tajemnicy ubezpieczeniowej.
Chmura publiczna	Niedopuszczalne	Chmura publiczna, z racji swojej cechy powszechności, będzie oparta na nienegocjowanej umowie lub regulaminie, który ma charakter adhezyjny, tj. usługobiorca nie będzie miał wpływu na treść jego postanowień. W związku z tym nie będzie możliwości zawarcia umów na takie usługi przetwarzania w chmurze publicznej przede wszystkim z uwagi na brak możliwości określenia w umowie odpowiednich postanowień zapewniających należyty poziom i bezpieczeństwo usług.

Załącznik – słownik pojęć

Administrator danych – w rozumieniu uodo jest to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 uodo, decydujące o celach i środkach przetwarzania danych osobowych. O fakcie, czy dany podmiot jest, czy też nie administratorem decyduje jego faktyczna „decyzyjność" w zakresie środków i celów przetwarzania. Na administratorze danych ciąży obowiązek: zapewnienia, aby dane były przetwarzanie zgodnie z prawem, zbierane dla oznaczonych zgodnie z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, a także przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

ADR (ang. *Alternative Dispute Resolution*) – alternatywne (pozasądowe) metody rozwiązywania sporów, takie jak: zapisy na sądy polubowne, arbitraż lub tzw. procedura eskalacyjna.

API (ang. *Application Programming Interface*) – interfejs programowania aplikacji, czyli ściśle określony zestaw reguł i ich opisów, za pomocą którego programy komunikują się między sobą.

BPO (ang. *Business Process Outsourcing*) – zlecanie wybranych funkcji lub procesów biznesowych (procesy związane z zarządzaniem przedsiębiorstwem, takie jak: HR, finanse, księgowość, obsługa klienta) przez zewnętrzne przedsiębiorstwa zajmujące się outsourcingiem.

Dane osobowe – w rozumieniu art. 6 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r., Nr 101, poz. 926, ze zm.) za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Due diligence – proces, któremu zostaje poddane przedsiębiorstwo będące obiektem zainteresowania innego przedsiębiorcy, włącznie z wyczerpującą analizą pod względem jego kondycji handlowej, finansowej, prawnej i podatkowej, przeprowadzany w celu identyfikacji związanych z nim szans i ryzyk przed podjęciem właściwych negocjacji dotyczących transakcji.

Dyrektywa 95/46/WE – Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. L 281 z 23.11.1995, s. 31).

Dyrektywa 2009/138/WE – Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (wersja przekształcona) (Dz. Urz. UE. L 2009, Nr 335, s. 1).

EOG (ang. *European Economic Area*, EEA) – Europejski Obszar Gospodarczy utworzony został na mocy porozumienia podpisanego 2 maja 1992 roku w Porto, w celu rozszerzenia jednolitego rynku Unii Europejskiej na państwa należące do Europejskiego Stowarzyszenia Wolnego Handlu (EFTA) oprócz Szwajcarii, która w wyniku referendum zachowała status obserwatora EOG. Regulacje Unii Europejskiej odnoszące się do jednolitego rynku wewnętrznego są na bieżąco przyjmowane do ustawodawstwa krajów EFTA, a specjalnie powołane do tego organy EFTA nadzorują prawidłowość ich transpozycji i wdrażania. Obecnie EOG obejmuje 27 państw członkowskich i 3 kraje EFTA – Islandię, Norwegię i Księstwo Lichtensteinu.

EU (ang. *European Union*) – Unia Europejska.

Grupa Robocza Art. 29 – grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołana na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, potocznie zwana „Grupą Roboczą Art. 29". Ma ona charakter doradczy i działa w sposób niezależny. W skład grupy roboczej wchodzą przedstawiciele organu lub organów nadzorczych, powołanych przez każde państwo członkowskie, oraz przedstawiciel organu lub organów ustanowionych dla instytucji i organów wspólnotowych, oraz przedstawiciel Komisji. Grupa robocza bada każdą kwestię dotyczącą stosowania krajowych środków przyjętych na mocy Dyrektywy 95/46/WE, aby przyczynić się w ten sposób do jednolitego stosowania tych środków, przekazuje Komisji opinie na temat stopnia ochrony we Wspólnocie i w państwach trzecich, doradza Komisji w sprawie wszelkich proponowanych zmian Dyrektywy 95/46/WE, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych środków wspólnotowych dotyczących praw i wolności, wydaje opinie na temat kodeksów postępowania opracowywanych na poziomie wspólnotowym.

GUI (ang. *Graphical User Interface*) – graficzny interfejs użytkownika, będący ogólnym określeniem sposobu prezentacji informacji przez komputer oraz interakcji z użytkownikiem, polegający na rysowaniu i obsługiwaniu elementów kontrolnych (tzw. widgetów).

IT (ang. *Information Technology*) – technologia informacyjna.

ITO (ang. *Information Technology Outsourcing*) – zlecenie podmiotom zewnętrznym wykonywania funkcji lub usług związanych z technologią informacyjną przedsiębiorstwa.

Klient – usługobiorca usług przetwarzania w chmurze będący stroną umowy z dostawcą usługi w chmurze.

Kodeks cywilny – Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93, ze zm.).

LAN (ang. *Local Area Network*) – sieć komputerowa łącząca komputery na określonym obszarze, takim jak blok, szkoła, laboratorium czy też biuro.

Offshore outsourcing **(ang. *Offshore outside resource using*)** – korzystanie z zasobów zewnętrznych podmiotu zagranicznego. Termin ten oznacza przekazanie pewnych obszarów niebiznesowej działalności przedsiębiorstwa podmiotom w innym państwie.

Offshoring – przeniesienie do innego państwa wybranych procesów biznesowych przedsiębiorstwa przy zachowaniu tej samej grupy klientów. Przeniesienie może objąć procesy produkcji, świadczenia usługi lub realizacji zamówienia. Jednym z rodzajów offshoringu jest offshore outsourcing.

Outsourcing **(ang. *Outside resource using*)** – dosłownie oznacza korzystanie z zasobów zewnętrznych. Outsourcing to zdefiniowanie oraz wydzielenie pewnych obszarów niebiznesowej działalności przedsiębiorstwa, które następnie są przekazywane wyspecjalizowanym w zarządzaniu tymi obszarami podmiotom zewnętrznym. Outsourcing stosowany jest najczęściej w branżach: IT, telekomunikacji, księgowości, zarządzania archiwami i usług prawnych.

Opinia nr 5/2012 Grupy Roboczej Art. 29 – Opinia nr 5/2012 Grupy Roboczej Art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej przyjęta 1 lipca 2012 roku. Grupa Robocza Art. 29 analizuje w Opinii nr 5/2012 wszystkie kwestie istotne dla dostawców usług przetwarzania danych w chmurze działających w EOG oraz ich klientów, określając wszystkie mające zastosowanie zasady z Dyrektywy o ochronie danych UE (95/46/WE) oraz Dyrektywy o prywatności i łączności elektronicznej 2002/58/WE (zrewidowanej Dyrektywą 2009/136/WE), gdy to właściwe.

Peak concurrent users – najwyższa liczba użytkowników korzystających z sieci komputerowej, pliku lub systemu w tym samym czasie.

Prawa autorskie – prawa autorskie służą ochronie utworu przed naruszeniami. Przysługują one twórcy w ramach monopolu autorskiego. Prawa autorskie dzielą się na autorskie prawa osobiste oraz majątkowe. Autorskie prawa osobiste służą ochronie niematerialnej więzi twórcy z jego utworem. Prawa te nie mogą zostać przeniesione na osoby trzecie (są niezbywalne) i są nieograniczone w czasie. Autorskimi prawami osobistymi są m.in. prawa do: autorstwa utworu; oznaczenia utworu swoim nazwiskiem lub pseudonimem, albo do udostępniania go anonimowo. Autorskie prawa majątkowe mogą zostać przeniesione na osoby trzecie (są zbywalne) i są ograniczone w czasie (zasadniczo gasną 70 lat po śmierci twórcy). Służą one ochronie interesów ekonomicznych twórcy związanych z dziełem.

Prawo telekomunikacyjne – Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 r. (Dz. U. Nr 171, poz. 1800, ze zm.).

Prawo ubezpieczeniowe – przepisy określające warunki wykonywania działalności w zakresie ubezpieczeń osobowych i ubezpieczeń majątkowych, działalności reasekuracyjnej, a także zasady wykonywania zawodu aktuariusza, sprawowania nadzoru ubezpieczeniowego, organizacji i funkcjonowania ubezpieczeniowego samorządu gospodarczego, uregulowane w Ustawie o działalności ubezpieczeniowej.

RFP (**ang. *Request For Proposal***) – zapytanie ofertowe; zaproszenie dostawców do wzięcia udziału w procesie składania ofert, mającym na celu dostarczenie konkretnego produktu lub usługi.

RFI (**ang. *Request For Information***) – zapytanie o informacje; pismo zawierające prośbę o informację, którego celem jest gromadzenie informacji pisemnej o możliwościach różnych dostawców.

RFQ (**ang. *Request For Quotation***) – zapytanie o wycenę; pismo zawierające prośbę o wycenę usług, którego celem jest zachęcenie dostawców do procedury przetargowej przedstawienia oferty konkretnych produktów lub usług. RFQ zwykle oznacza to samo co IFB (*Invitation For Bid).*

Rozporządzenie Ministra Finansów z dnia 31 października 2003 r. – Rozporządzenie Ministra Finansów z dnia 31 października 2003 r. w sprawie szczegółowych zasad tworzenia, utrwalania, przechowywania i zabezpieczania dokumentów związanych z zawieraniem i wykonywaniem umów ubezpieczenia (Dz. U. Nr 193, poz. 1889).

Sarbanes-Oxley (nazywana też *SOX* lub *SarOx*) – ustawa uchwalona przez Kongres USA w 2002 roku, wyznaczająca wysokie wymogi niezależności wobec kluczowych graczy na rynku finansowym oraz podnosząca na bardzo wysoki poziom wymagania w zakresie efektywności kontroli wewnętrznej podmiotów zarejestrowanych w US Securities Exchange Commission.

Server racks – urządzenie przemysłowe (tzw. szafa), w standardzie RACK, mające zastosowanie w serwerowniach komputerowych. W szafach montowany jest sprzęt komputerowy.

SLA (ang. *Service Level Agreement*) – umowa lub postanowienia umowne dotyczące jakości świadczonych usług.

Sourcing – strategia przedsiębiorstwa określająca sposób, w jaki obsługiwane będą poszczególne procesy biznesowe bądź obszary funkcjonalne firmy, oraz komu zostanie zlecona ta obsługa (w zakresie działalności przedsiębiorstwa lub outsourcing).

Streaming – technika dostarczania informacji multimedialnej na życzenie. Najczęściej *streaming* opiera się na transmisji skompresowanych danych multimedialnych przez Internet.

TSUE – Trybunał Sprawiedliwości Unii Europejskiej.

UKE – Urząd Komunikacji Elektronicznej, na którego czele stoi prezes będący organem regulacyjnym w zakresie działalności pocztowej, telekomunikacyjnej i gospodarki częstotliwościowej oraz kontroli spełniania wymagań dotyczących kompatybilności elektromagnetycznej.

UPS (ang. *Uninterruptible Power Supply*) – urządzenie lub system, którego funkcją jest nieprzerwane zasilanie innych urządzeń elektrycznych lub elektronicznych.

Ustawa o działalności ubezpieczeniowej – Ustawa o działalności ubezpieczeniowej z dnia 22 maja 2003 r. (tekst jednolity: Dz. U. 2010, Nr 11, poz. 66, ze zm.).

Ustawa o prawie autorskim – Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (tekst jednolity: Dz. U. Nr 90, poz. 631, ze zm.).

Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych – Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych z dnia 7 maja 2010 r. (Dz. U. Nr 106, poz. 675).

Ustawa o ochronie danych osobowych (uodo) – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. Nr 101, poz. 926, ze zm.).

Utwór – każdy przejaw ludzkiej działalności twórczej o indywidualnym charakterze. Oznacza to, iż określony wytwór niematerialny, aby podlegać ochronie na gruncie prawa autorskiego, powinien wykazywać łącznie następujące cechy: 1) stanowić rezultat pracy człowieka (twórcy), 2) stanowić przejaw działalności twórczej, 3) mieć indywidualny charakter. Istotne jest też, aby utwór by ustalony w jakiejkolwiek postaci. Pomysły (odkrycia, idee, procedury, metody, zasady działania, koncepcje matematyczne) nie podlegają ochronie, dopóki nie zostaną wyrażone, np. na kartce papieru lub wygłoszone podczas przemówienia. Dla uzyskania ochrony nie jest istotna postać, w jakiej utwór został ustalony ani jego wartość czy przeznaczenie, ani sposób wyrażenia. Orzecznictwo sądów polskich pokazuje, iż utworem mogą być m.in. Szczególne Istotne Warunki Zamówienia (SIWZ); opis produktu ubezpieczeniowego; krótka jednostka słowna, pełniąca rolę znaku towarowego; grafika na portalu internetowym; podręcznik szkolny; kalendarz; książka kucharska itp. Dla powstania ochrony utworu na podstawie prawa autorskiego nie jest wymagana żadna dodatkowa czynność, w szczególności urzędowe potwierdzenie czy też rejestracja ochrony. Twórcze opracowanie cudzego utworu (tłumaczenie, przeróbka, adaptacja) również stanowi utwór (tzw. utwór zależny). Utwór może stanowić rezultat działania wielu osób (utwór zbiorowy).

Własność intelektualna – zbiorcze pojęcie na określenie wytworów umysłu ludzi. W bezpośredni sposób wytwory te korespondują z konkretnymi prawami własności intelektualnej. Prawa własności intelektualnej są wyłącznymi prawami na dobrach niematerialnych, takich jak: utwory muzyczne, literackie, artystyczne, wynalazki, słowa, slogany, symbole, wzory. Do praw własności intelektualnej zalicza się m.in. prawa autorskie i prawa pokrewne, znaki towarowe, wynalazki, oznaczenia geograficzne, wzory przemysłowe i użytkowe.

Polska Izba Ubezpieczeń, ul. Wspólna 47/49, 00-684 Warszawa
tel. 22 42 05 105, 22 42 05 106, faks 22 42 05 107
office@piu.org.pl, www.piu.org.pl