DZP
więcej niż prawo

Prawne aspekty usług chmurowych

DZP
więcej niż prawo

Prawne aspekty usług chmurowych

DZP

Spis treści

Wprowadzenie 3
| *dr Aleksandra Auleytner*

Czy grozi nam bałkanizacja Internetu? 5
| *Bartosz Marcinkowski*

O konieczności partnerstwa państwa i sektora prywatnego w budowie systemu cyberbezpieczeństwa 11
| *Wojciech Dziomdziora*

Nowa rola Administratora Bezpieczeństwa Informacji 15
| *Sylwia Kuca*

Ochrona danych medycznych w chmurze 21
| *Piotr Najbuk*

Wiążące reguły korporacyjne (BCR) jako element efektywnej polityki *compliance* 25
| *dr Anna Partyka-Opiela*

Prawa autorskie a usługi chmurowe 31
| *Jakub Kubalski*

Charakter odróżniający znaków towarowych zawierających element „cloud” 35
| *Monika Gebel*

Zespół kancelarii Domański Zakrzewski Palinka 39

Wprowadzenie

dr Aleksandra Auleytner | Radca Prawny, Partner

Informatyczne usługi chmurowe stosowane są coraz powszechniej w niemal każdej dziedzinie życia. Choć ich rozwój trwa już kilka lat, to nadal rodzą one szereg wyzwań i problemów natury prawnej i to z bardzo wielu dziedzin. Jest to proces naturalny. Rozwój tych usług jest procesem ciągłym, stają się one coraz bardziej wyrafinowane i tym samym skomplikowane. Jednocześnie pojawiają się nowe regulacje prawne, zarówno na szczeblu międzynarodowym, europejskim, jak i krajowym. Podejście prawne do tych usług musi być zatem kompleksowe.

W DZP rozumiemy te wyzwania. Tworzymy interdyscyplinarny zespół potrafiący szukać rozwiązań prawnych w sposób całościowy. Wiedzę prawną łączymy ze zrozumieniem procesów biznesowych i technicznych. Dwa lata temu opublikowaliśmy raport „Cloud computing w działalności ubezpieczeniowej", w bieżącym roku raport „Otoczenie regulacyjne telemedycyny w Polsce". Te i wiele innych publikacji, ale przede wszystkim codzienna praca dla wiodących firm z różnych branż, stanowią dowód naszego zaangażowania i wiedzy związanej z różnymi aspektami usług teleinformatycznych.

Prezentowany materiał nie stanowi kompleksowego opisu zagadnień prawnych usług chmurowych, ale ma raczej wskazać, jak wiele aspektów regulacyjnych się z nim wiąże. Zachęcam Państwa do lektury, do bezpośredniego kontaktu z DZP oraz do odwiedzania naszych blogów tematycznych http://blog.dzp.pl/.

Czy grozi nam bałkanizacja Internetu?

Bartosz Marcinkowski | Radca Prawny, Partner

„Czy grozi nam bałkanizacja Internetu?" – tak dziennik Financial Times zatytułował artykuł opisujący możliwe skutki orzeczenia Trybunału Sprawiedliwości Unii Europejskiej w sprawie M. Schrems v Data Protection Commissioner.

Czy określenie to, odnoszące sie do rozpadu Imperium Osmańskiego w XIX w. oraz Jugosławii w latach dwudziestych XX w., może okazać się trafne w kontekście przekazywania danych osobowych między Europą a Stanami Zjednoczonymi, w tym w odniesieniu do cloud computing.

W ostatnich dniach Trybunał Sprawiedliwości UE orzekł o nieważności programu Safe Harbor, zainicjowanego w roku 2000, umożliwiającego dotychczas w określonych przypadkach przekazywanie danych z Unii Europejskiej do firm mieszczących się w USA, a będących uczestnikami owej prawnej *bezpiecznej przystani*. Skrótowo ujmując, uczestnicy Bezpiecznej Przystani, mimo lokalizacji w Stanach Zjednoczonych, uznawani byli za gwarantujących danym osobowym taką ochronę, jaka obowiązuje w Unii Europejskiej. Zatem udział w programie Safe Harbor stanowił jeden z prawnych filarów, umożliwiających działalność takich gigantów, jak Facebook, Twitter czy Google. Ale nie tylko – beneficjentami Bezpiecznej Przystani był także cały szereg innych firm, dla których przekazywanie danych osobowych za Atlantyk stanowi element bieżącej działalności. Łącznie z udogodnień wynikających z programu Safe Harbor korzystało około 5000 firm[1].

Orzeczenie unieważniające program Safe Harbor pociąga zatem za sobą istotne konsekwencje, choć przywołany tytuł zastosowany przez Financial Times zdaje się być na wyrost.

[1] https://safeharbor.export.gov/list.aspx

Dlaczego Bezpieczna Przystań przestała być bezpieczna?

Przybliżmy istotę zagadnienia i tego, co spowodowało, że luksemburski Trybunał Sprawiedliwości zanegował istnienie Bezpiecznej Przystani w jej obecnym kształcie.

Program Safe Harbor w szczególności zakładał, że dane osobowe pochodzące z Unii Europejskiej mogły być przetwarzane w USA dzięki autocertyfikacji, dokonywanej przez amerykańskie przedsiębiorstwa, działające pod stosunkowo luźnym nadzorem Departamentu Handlu (Department of Commerce, DC) oraz Federalnej Komisji Handlu (Federal Trade Commission, FTC).

W konsekwencji pojawił się problem braku realnej kontroli nad przetwarzaniem danych ze strony osób, których dane dotyczą. Co więcej, w praktyce, Safe Harbor nie zapewniał należytej kontroli nad **dalszym przekazywaniem** danych, co rodziło ryzyko wycieku danych z Bezpiecznej Przystani. Tym sposobem ochrona danych stawała się, zwłaszcza z perspektywy osób, których dane dotyczą, iluzoryczna.

Amerykańskie realia wobec europejskiej regulacji

Opisany stan rzeczy jest w Unii Europejskiej nieakceptowalny: unijne prawodawstwo zakłada znaczną ochronę podmiotów (to jest osób, których dane dotyczą), w tym zapewnia pomoc ze strony organów ochrony danych (takich, jak polski Generalny Inspektor Ochrony Danych Osobowych). Tymczasem w Stanach Zjednoczonych nie tylko brak uniwersalnej regulacji dotyczącej ochrony danych, w rodzaju polskiej ustawy o ochronie danych osobowych z 1997 r. czy Dyrektywy 95/46/WE o ochronie danych i ich swobodnym przepływie, ale również brak wyspecjalizowanego organu ochrony. Co prawda, w USA ochroną prywatności informacyjnej zajmuje się jeden ze stosunkowo nowo powołanych wydziałów Federalnej Komisji Handlowej, to jednak możliwość jego oddziaływania na praktykę obrotu jest ograniczona, między innymi ze względu na brak generalnego zakazu przekazywania danych kolejnym odbiorcom.

Co więcej, zgodnie z zasadami Safe Harbor, ograniczenia i gwarancje Bezpiecznej Przystani nie wiązały podmiotu przetwarzającego dane, jeśli wymagały tego m.in. względy bezpieczeństwa narodowego czy interesu publicznego.

Właśnie na te wyjątki zwrócił uwagę Trybunał Sprawiedliwości UE, w swoim orzeczeniu wskazując, że umożliwiały one amerykańskiej administracji praktycznie nieograniczony dostęp do danych przetwarzanych na amerykańskich serwerach w ramach Bezpiecznej Przystani, podkreślając, że Safe Harbor nie zapewnia instrumentów umożliwiających jednostkom skuteczną ochronę przed ingerencją w ich dane osobowe.

Sprawa trafiła do Trybunału Sprawiedliwości UE w związku ze skargą obywatela austriackiego Max Schremsa, który po ujawnieniu przez Edwarda Snowdena rewelacji dotyczących poziomu inwigilacji ze strony administracji USA, sprzeciwił się przetwarzaniu swoich danych na serwerach Facebooka, fizycznie znajdujących się w Stanach Zjednoczonych, argumentując między innymi, iż porozumienie Safe Harbor nie stanowiło gwarancji prawidłowego przetwarzania danych w USA.

Ważenie wartości. Trudne zadanie Trybunału

Trybunał Sprawiedliwości UE musiał zważyć, czy prawa podstawowe, w tym prawo do prywatności, doznają uszczerbku wobec rozwiązań przyjętych w programie Safe Harbor. W wyroku Trybunał stwierdził, że Dyrektywa 95/46/WE, stanowiąca podstawę ochrony danych osobowych w Unii Europejskiej, ma zapewnić nie tylko efektywną i kompletną ochronę podstawowych praw i wolności osób fizycznych, ale w szczególności tych, gwarantujących fundamentalne prawo do poszanowania życia prywatnego, w odniesieniu do przetwarzania danych osobowych. Zatem systemowe rozwiązania grożące tym wartościom nie zasługują, w ocenie Trybunału, na uznanie.

Co dalej – praktyka po wyroku Trybunału?

Po ogłoszeniu orzeczenia Trybunału pojawiły się głosy krytykujące przyjęte stanowisko z uwagi na daleko idące skutki praktyczne. W szczególności częste są argumenty, iż usztywnianie regulacji w celu wzmocnienia ochrony danych osobowych w konsekwencji przyniesie w transatlantyckich relacjach – z perspektywy wymiany handlowej, naukowej czy kulturalnej – więcej szkody niż ewentualnych korzyści.

Nie rozstrzygając teraz wspomnianej kwestii, trzeba stwierdzić, iż Trybunał Sprawiedliwości UE jednoznacznie opowiedział się za zapewnieniem ochrony podstawowych praw obywateli. Taki wyrok stanowi zresztą przejaw konsekwentnie rozwijanej przez Trybunał linii orzeczniczej, dotyczącej gwarancji praw i wolności jednostki, jako wartości nadrzędnej.

Niemniej, praktyczne skutki wyroku mogą być poważne dla przedsiębiorców dotychczas uczestniczących w programie Safe Harbor wedle stanowiska Grupy Roboczej Artykułu 29 (roboczego zespołu ds. ochrony danych osobowych, składającego się m.in. z przedstawicieli organów ochrony danych poszczególnych państw członkowskich UE), organy odpowiedzialne za ochronę danych osobowych, w tym polski Generalny Inspektor Ochrony Danych Osobowych, do końca stycznia 2016 r. będą uznawały przekazywanie danych osobowych w ramach programu Bezpieczna Przystań tak, jakby gwarancje ochrony nadal w pełni obowiązywały (tymczasowe przyjęcie fikcji, iż Safe Harbor nadal obowiązuje i należycie wypełnia swoje zadania).

Po upływie terminu wskazanego okresu przejściowego, czyli na początku lutego 2016 r., państwowe organy ochrony danych osobowych państw członkowskich UE podejmą stosowne „skoordynowane działania wykonawcze". Jednocześnie Grupa Robocza Art. 29 podkreśliła, że przesyłanie danych osobowych z UE do USA na podstawie programu Safe Harbor jest już teraz obarczone wysokim ryzykiem naruszenia bezpieczeństwa danych i zasugerowała możliwe daleko idące ograniczenie z jego korzystania.

Alternatywa czy mniejsze zło?

W związku z unieważnieniem programu Safe Harbor, przedsiębiorcy przesyłający dane do USA będą musieli korzystać z innych podstaw. Od początku 2016 r. polska ustawa o ochronie danych osobowych pozwala na stosowanie standardowych klauzuli umownych (Standard Contractual Clauses) opracowanych przez Komisję Europejską, bez uzyskiwania dodatkowej akceptacji Generalnego Inspektora Ochrony Danych Osobowych. Możliwe jest również przyjęcie przez międzynarodowe korporacje odpowiednich regulacji wewnętrznych (Binding Corporate Rules), określających zasady transferu danych osobowych pomiędzy członkami korporacji; tego rodzaju regulacje wymagają jednak zatwierdzania przez organy ochrony danych w państwach członkowskich UE, z których dane mają być eksportowane za ocean. Innym możliwym rozwiązaniem jest uzyskiwanie pisemnej zgody od każdej osoby, której dane miałyby być transferowane do USA, co w razie znacznych ilości danych okazuje się z oczywistych względów wysoce niepraktyczne czy zgoła niewykonalne.

Wprowadzenie trzymiesięcznego okresu przejściowego ma na celu umożliwienie uczestnikom transatlantyckiej wymiany danych dostosowanie do nowych okoliczności, tj.:

- ocenę ilości, częstotliwości i charakteru danych przekazywanych do USA w ramach dotychczas obowiązującego programu Safe Harbor,
- wypracowanie i wdrożenie alternatywnych rozwiązań prawnych, na przykład takich jak standardowe klauzule umowne czy wiążące reguły korporacyjne.

Są to jednak wszystko rozwiązania *ad hoc*, które nie zastąpią mechanizmów strukturalnych o uniwersalnym charakterze (tj. takich jakim w swoich założeniach był Safe Harbor).

Wyrok i poszkodowany. Skutki dla Internetu i cloud computing

Czy zatem wyrok oznacza początek końca transferu danych przez Atlantyk, co miałoby skutkować początkiem końca Internetu, w kształcie, jaki znamy? A zwłaszcza, czy wyrok może stanowić początek końca cloud computing?

Program Safe Harbor można przyrównać do Strefy Schengen – owszem, brak porozumienia Bezpiecznej Przystani może skutkować tym, czym skutkowałoby zamknięcie granic i przywrócenie szczegółowych kontroli paszportowych. Przepływ danych nadal będzie się odbywał, ale może stracić na płynności, gdyż stosowane będą rozwiązania o partykularnym (choć niekoniecznie jednorazowym) charakterze, które przykładowo wskazaliśmy powyżej.

Jak się wydaje, na nowe rozwiązanie systemowe trzeba będzie poczekać; doświadczenie uczy, iż negocjacje pomiędzy UE a USA w dziedzinie ochrony danych osobowych nie są ani łatwe, ani szybkie, zatem konieczne będzie posiłkowanie się w obrocie doraźnymi rozwiązaniami. Czy poziom ochrony prywatności jako jednego z praw podstawowych faktycznie wzrośnie, przekonamy się zapewne już niedługo, obserwując praktykę i stopień przestrzegania wymogów tymczasowo zastępujących Safe Harbor. Obrót, w tym usługi chmurowe, mogą stracić na płynności, gdyż będą wymagały stosownie niedopasowanych do swej specyfiki i natury rozwiązań formalnych.

共和新路立交
GONGHEXIN RD INTERCHANGE
卢浦大桥
LUPU BRIDGE

O konieczności partnerstwa państwa i sektora prywatnego w budowie systemu cyberbezpieczeństwa

Wojciech Dziomdziora | Radca Prawny, Counsel

Czym jest cyberprzestrzeń?

Normatywna definicja „cyberprzestrzeni" znajduje się w ustawie z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Cyberprzestrzenią jest przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami. System informatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą, **właściwego dla danego rodzaju sieci**, telekomunikacyjnego urządzenia końcowego[2].

[2] Definicja z art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Państwo nas nie chroni

Bezpieczeństwem, w tym bezpieczeństwem cyberprzestrzeni, zajmować się muszą właściwe organy władzy państwowej. W dzisiejszych czasach kwestie cyberbezpieczeństwa czy cyberwojny są istotnym elementem doktryn wojennych i obronnych wielu państw świata. Zagrożenia w tym obszarze wynikają również ze strony międzynarodowych grupo terrorystycznych i przestępczych. Ofiarami cyberprzestępczości padają państwa, poszczególne urzędy, systemy energetyczne, bankowe i inne. Ofiarami są także obywatele.

Na mocy art. 2 ust. 1 ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, art. 2 ust. 1 ustawy o stanie wyjątkowym, art. 2 ustawy o stanie klęski żywiołowej.

Tymczasem w Polsce poziom działań organów państwa dla zabezpieczenia bezpieczeństwa w cyberprzestrzeni jest bardzo niski. Świadczą o tym wnioski z raportu Najwyższej Izby Kontroli z dnia 23.06.2015 r. Wnioski te są niestety druzgocące dla polskiej administracji. Warto przytoczyć tu kilka zdań z Raportu NIK: „Administracja państwowa nie podjęła dotychczas niezbędnych działań, mających na celu zapewnienie bezpieczeństwa teleinformatycznego Polski. (…) bezpieczeństwo Polski w dalszym ciągu jest postrzegane jedynie w sposób konwencjonalny. Nie dostrzeżono, że powstała nowa kategoria zagrożeń, wymagająca pilnej reakcji państwa. Kierownictwo najważniejszych instytucji publicznych nie było świadome niebezpieczeństw związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z tego faktu nowych zadań administracji państwowej. (…) Działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. (…) Dopiero w czerwcu 2013 r. Rada Ministrów przyjęła „Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" – dokument będący wynikiem braku porozumienia i źle rozumianego kompromisu, o niskiej jakości, nieprecyzyjny i obarczony wieloma błędami merytorycznymi. Nieliczne zadania wynikające bezpośrednio z „Polityki" nie były realizowane przez większość (…) podmiotów, co pozwala stwierdzić, że jej praktyczne zastosowanie w celu poprawy bezpieczeństwa teleinformatycznego państwa było jedynie symboliczne. (…) nie opracowano założeń systemu finansowania działań związanych z ochroną cyberprzestrzeni RP. Zgodnie ze stanowiskiem Ministra Finansów, wskazującym na konieczność „bezkosztowego" wykonywania tych zadań, nie zostały również przydzielone żadne dodatkowe środki finansowe na ich realizację, co (…) praktycznie sparaliżowało działania podmiotów państwowych w zakresie bezpieczeństwa teleinformatycznego. (…) Nie były dotychczas prowadzone żadne prace legislacyjne mające na celu unormowanie zagadnień związanych z bezpieczeństwem teleinformatycznym państwa. (…) Podmioty administracji państwowej nie podejmowały rzetelnych i adekwatnych działań w celu ustanowienia wymogów w zakresie bezpieczeństwa cyberprzestrzeni. (…) Podmioty państwowe w ogóle nie wykonywały w tym zakresie (kontroli przestrzegania ustanowionych wymogów z zakresu bezpieczeństwa teleinformatycznego – przypis DZP) obowiązków wynikających z ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne." Podzielić należy wnioski i zalecenia NIK, a w szczególności:

1. ukierunkowanie działań państwa związanych z utrzymaniem bezpieczeństwa cyberprzestrzeni przede wszystkim na infrastrukturę krytyczną;
2. przyjęcie przez Radę Ministrów narodowej strategii zarządzania zagrożeniami występującymi w cyberprzestrzeni, określającej: cele i strukturę organizacyjną krajowego systemu ochrony

cyberprzestrzeni, zadania poszczególnych jego uczestników i przypisane do nich, precyzyjnie zdefiniowane, produkty, mierniki i terminy realizacji;
3. określenie systemu finansowania zadań związanych z ochroną cyberprzestrzeni;
4. przyjęcie ram prawnych krajowego systemu ochrony cyberprzestrzeni, poprzez uchwalenie odrębnej ustawy, jak również dokonanie inwentaryzacji i nowelizacji istniejących obecnie regulacji prawnych, dotyczących m.in. zarządzania kryzysowego, Prawa telekomunikacyjnego, informatyzacji;
5. wyznaczenie krajowego organu koordynującego działania innych podmiotów w zakresie ochrony cyberprzestrzeni, będącego jednocześnie CERTem narodowym.

Konieczność partnerstwa państwa i podmiotów prywatnych

Zaleceniem, nad którym szczególnie warto się zatrzymać, jest wskazanie przez NIK, że warunkiem efektywnej ochrony cyberprzestrzeni, jest wdrożenie mechanizmów współpracy podmiotów prywatnych i państwowych. NIK zasadnie wskazuje bowiem, że budowa cyberprzestrzeni odbyła się w zasadzie bez nadzoru i współpracy instytucji państwowych. Również przeważająca większość infrastruktury obsługującej polską cyberprzestrzeń jest w rękach podmiotów komercyjnych (głównie prywatnych), a podmioty te dysponują unikalną wiedzą i przygotowanymi pracownikami.

Moim zdaniem, państwo powinno nie tylko podjąć funkcje koordynacyjne działań administracji i podmiotów prywatnych oraz wymieniać z sektorem prywatnym informacje i narzucać mu standardy w zakresie ochrony cyberprzestrzeni. Konieczne tu jest prawdziwe partnerstwo pomiędzy organami państwa oraz podmiotami prywatnymi, zarówno tymi, które zarządzają infrastrukturą krytyczną, jak i tymi najbardziej narażonymi na cyberataki.

Budowa tego partnerstwa powinna rozpocząć się od wspólnej pracy analitycznej i prawnej nad postulowaną przez NIK nową ustawą, określającą ramy prawne krajowego systemu ochrony cyberprzestrzeni oraz przeglądu istniejących regulacji w zakresie zarządzania kryzysowego, Prawa telekomunikacyjnego i informatyzacji. W proces wypracowania właściwych rozwiązań prawnych należy zaangażować wielu interesariuszy i ekspertów – firmy prywatne i reprezentujące ich organizacje, takie jak Polska Izba Informatyki i Telekomunikacji, przedstawicieli nauki, prawników zajmujących się tą tematyką i organizacje obywatelskie. Nowe rozwiązania i standardy nie mogą zostać narzucone podmiotom prywatnym a muszą być wypracowane w porozumieniu z nimi. W przeciwnym bowiem razie, nowy system nie będzie prawidłowo funkcjonował. Bez pełnego, partnerskiego zaangażowania sektora prywatnego nie da się również zidentyfikować i zinwentaryzować pełnej listy infrastruktury krytycznej, co jest warunkiem koniecznym i wstępnym dla budowy narodowej strategii cyberbezpieczeństwa. Konieczne jest również zaangażowanie istniejących prywatnych zespołów CERT. Właściciele infrastruktury krytycznej i inne podmioty prywatne muszą mieć poczucie współodpowiedzialności za bezpieczeństwo cyberprzestrzeni. Nie da się tego zbudować, nie budując partnerskich relacji.

Nowa rola Administratora Bezpieczeństwa Informacji

Sylwia Kuca | Associate

Po 1 stycznia 2015 r. rola Administratora Bezpieczeństwa Informacji („**ABI**") uległa znacznej zmianie w wyniku wejścia w życie ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej, na podstawie której wprowadzono szereg zmian do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych („**UODO**").[3] ABI, mając znaczący wpływ na zapewnienie bezpieczeństwa przetwarzanych danych, ma możliwość kontroli sposobu przetwarzania danych przy wykorzystaniu cloud computingu.

Nowelizacja UODO poszerzyła m.in. zakres obowiązków ABI, który stał się *wewnętrznym inspektorem* ochrony danych osobowych, do którego obowiązków należy bieżący nadzór na legalnym przetwarzaniem danych osobowych oraz przeprowadzenie sprawdzenia legalności przetwarzania danych (w tym na żądanie Generalnego Inspektora Ochrony Danych Osobowych, GIODO).

W celu zapewnienia ABI swobody w wykonywaniu powierzonych funkcji, przepisy strukturalnie uniezależniły ABI od podmiotu, w którym pełni swoje funkcje (administratora danych), mającego obowiązek zapewnić ABI niezależność organizacyjną (ABI może podlegać jedynie bezpośrednio kierownikowi jednostki organizacyjnej)[4] oraz finansową (poprzez zapewnienie środków na wykonywanie zadań).

---

3 Przepisy UODO zostały uzupełnione przez Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych, Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

4 Zapewnienie niezależności organizacyjnej może mieć formę wyodrębnienia stanowiska ABI wewnątrz struktury organizacyjnej, dopasowanie aktualnego stanowiska osoby pełniącej tej funkcję, outsourcing funkcji na zewnątrz w celu uniezależnienia ABI od przełożonych i poddania ABI wyłącznie zarządowi jako kierownikowi jednostki.

Poniżej przedstawiamy zestawienie zasadniczych zmian dotyczących ABI, wprowadzonych z nowelizacją UODO.

KRYTERIUM	PRZED NOWELIZACJĄ	PO NOWELIZACJI
Powołanie ABI	Obowiązkowe (zgodnie z wyrokiem NSA z dnia 21 lutego 2014 r., I OSK 2445/12)	Fakultatywne
Warunki kwalifikacyjne	Brak	Szczegółowo określone w UODO
Zgłoszenie powołania ABI do rejestru GIODO	Nie	Obowiązkowe
Wpływ powołania oraz zgłoszenia ABI na obowiązek rejestracji zbioru danych w rejestrze prowadzonym przez GIODO	N/A	Zwolnienie z obowiązku rejestracji zbiorów danych w rejestrze prowadzonym przez GIODO z wyjątkami przewidzianymi przez UODO [por. niżej]
Status ABI w relacjach z administratorem danych	Zależność ABI od administratora danych	Bezpośrednia podległość kierownikowi jednostki organizacyjnej (zarządowi), konieczność zapewnienia przez administratora danych niezależności ABI
Zadania ABI	Nadzorowanie zasad przetwarzania danych osobowych	Poszerzenie obowiązków ABI (m.in. zapewnienie przestrzegania przepisów o ochronie danych osobowych oraz prowadzenie rejestru zbiorów danych osobowych)
Kontrola/sprawdzenie zgodności przetwarzania danych osobowych	Kontrola ze strony GIODO	• Sprawdzenie przez ABI dla administratora danych • Sprawdzenie przez ABI na wniosek GIODO • Kontrola ze strony GIODO
Możliwość powołania zastępcy ABI	Brak regulacji	Możliwość wyraźnie przewidziana przez GIODO

Obecnie do zadań ABI należy[5]:

1. zapewnienie przestrzegania przepisów o ochronie danych osobowych, m.in. poprzez nadzorowanie opracowywania i aktualizowania dokumentacji opisującej przetwarzanie danych osobowych oraz stosowane środki zabezpieczeń oraz zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

5 Administrator danych może powierzyć ABI dodatkowe obowiązki, pod warunkiem, że nie naruszy to prawidłowego wykonywania podstawowych zadań ABI.

2. prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez administratora danych, z wyjątkami przewidzianymi przez UODO;
3. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie sprawozdania z przeprowadzonej kontroli[6].

Nadzorowanie opracowywania i aktualizowania dokumentacji opisującej przetwarzanie danych osobowych oraz stosowane środki zabezpieczeń

Nadzór nad opracowywaniem oraz aktualizowaniem dokumentacji opisującej przetwarzanie danych osobowych oraz stosowane środki zabezpieczeń (m.in. Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym) polega m.in. na weryfikacji: opracowania oraz kompletności dokumentacji przetwarzania danych, zgodności przetwarzania danych z obowiązującymi przepisami prawa, stanu faktycznego w zakresie przetwarzania danych, przestrzegania zasad oraz obowiązków określonych w dokumentacji przetwarzania danych.

Zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Jednym ze sposobów zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych są szkolenia oraz webinaria wewnętrzne lub organizowane przez zewnętrzne firmy. Każda osoba, która została zapoznana z przepisami o ochronie danych osobowych, powinna potwierdzić ten fakt, np. w formie pisemnego oświadczenia.

Prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez administratora danych, z wyjątkami przewidzianymi przez UODO

W przypadku powołania ABI oraz zgłoszenia go do rejestru prowadzonego przez GIODO, administrator danych zwolniony jest z obowiązku zgłoszenia zbiorów danych do rejestru GIODO, a także aktualizowania danych dla zbiorów już zarejestrowanych. Zwolnienie to nie dotyczy jednak zbioru obejmującego tzw.

6 Kwestię sprawdzania zgodności przetwarzania danych osobowych oraz nadzorowania opracowywania i aktualizacji dokumentacji opisującej przetwarzanie danych osobowych reguluje Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez ABI.

dane wrażliwe, to jest danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Wynika to ze szczególnego charakteru tych danych.
Rejestr zbiorów danych, prowadzony przez ABI, powinien być jawny, zatem każdemu przysługuje prawo przeglądania rejestru, przy czym administrator danych ma obowiązek zapewnić środki finansowe, pozwalające na realizację opisanej tu zasady jawności.

Zwolnienie z obowiązku rejestracji zbiorów danych w rejestrze GIODO stosowane jest od momentu zgłoszenia ABI do rejestru prowadzonego przez GIODO. Reguła ta nie dotyczy sytuacji, gdy ABI jest ponownie zgłaszany do rejestru GIODO, po wcześniejszym wykreśleniu go z rejestru przez GIODO działającego z urzędu. W takiej sytuacji, zwolnienie z obowiązku rejestracji zbiorów danych w rejestrze GIODO stosowane jest od momentu wpisania ABI do rejestru.

Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie sprawozdania z przeprowadzonej kontroli

Ta funkcja ABI wzbudza pewne obawy wśród administratorów danych rozważających powołanie ABI. Zgodnie z obowiązującymi przepisami, ABI może dokonać sprawdzenia dla administratora danych oraz na żądanie GIODO.

W pierwszym przypadku, sprawdzenie może mieć charakter planowany (tj. określony w planie sprawdzeń przygotowywanym na okres nie krótszy niż kwartał i nie dłuższy niż rok, przy czym plan sprawdzeń powinien obejmować co najmniej jedno sprawdzenie) oraz doraźny (tj. nieprzewidziany w planie sprawdzeń). Sprawdzenie doraźne powinno być przeprowadzone przez ABI niezwłocznie po powzięciu przezeń wiadomości o naruszeniu lub podejrzeniu naruszenia zasad ochrony danych osobowych.

W przypadku kontroli przeprowadzonej na żądanie GIODO, ABI zawiadamia administratora danych o rozpoczęciu sprawdzenia przed podjęciem pierwszej czynności w toku sprawdzenia. Poza tym, ABI zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed przeprowadzeniem sprawdzenia. W kontekście tych regulacji oraz przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, regulującej m.in. kwestie zawiadomienia o planowanej kontroli, kontrowersje budzi wyjątek od tej zasady, zgodnie z którym, zawiadomienia nie przekazuje się m.in. w przypadku sprawdzenia na żądanie GIODO, jeżeli na takie zawiadomienie nie pozwala termin wyznaczony przez GIODO. Może to mieć miejsce zwłaszcza

w razie powzięcia przez GIODO wiadomości o poważnych nieprawidłowościach w dziedzinie ochrony danych osobowych u konkretnego administratora danych.

Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie z przeprowadzonej kontroli (termin na przygotowanie takiego sprawozdania zależy od rodzaju przeprowadzonej kontroli[7]), które w przypadku kontroli przeprowadzonej na żądanie GIODO, zostaje przekazane GIODO za pośrednictwem administratora danych. Sprawozdanie ABI powinno zawierać m.in. opis stanu faktycznego, stwierdzonego w toku sprawdzenia oraz inne informacje, mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych, jak również stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem.

Na podstawie opisu elementów sprawozdania przygotowanego po przeprowadzonej kontroli, uzasadniony wydaje się wniosek, że nieprawidłowości stwierdzone w trakcie sprawdzenia dokonanego na żądanie GIODO, mogą zostać usunięte przed przygotowaniem przez ABI sprawozdania z wyników kontroli, o ile tylko pozwoli na to czas wyznaczony przez GIODO na przedstawienie sprawozdania. W takiej sytuacji, zgodnie z obowiązującymi przepisami, zalecane jest opisanie w sprawozdaniu stwierdzonych przypadków naruszenia ochrony danych osobowych wraz z podjętymi działaniami przywracającymi stan zgodny z prawem.

Powyższa relacja ABI – GIODO wzbudza pytania o bezstronność i ewentualny konflikt interesów pomiędzy ABI a zatrudniającym go administratorem danych. Instytucja ABI zakłada jednak, że administrator danych powołując ABI, dąży do zagwarantowania w swojej strukturze prawidłowej ochrony danych osobowych, a niezależna i obiektywna opinia leży w interesie przedsiębiorcy i osób, których dane dotyczą. Ustawodawca wprowadzając fakultatywność powołania ABI, pozostawił przy tym w gestii administratora danych podjęcie decyzji o powołaniu w swojej strukturze jednostki odpowiedzialnej za zapewnienie legalnego przetwarzania danych. Z powołaniem oraz zgłoszeniem ABI do rejestru GIODO wiąże się szereg korzyści dla administratora danych, takich jak przeniesienie odpowiedzialności (w tym karnej) za legalne przetwarzanie danych z zarządu na ABI, zwolnienie z obowiązku rejestracji zbiorów danych w rejestrze GIODO oraz zapewnienie stałej kontroli wykwalifikowanej osoby nad legalnym przetwarzaniem danych osobowych, w tym w tzw. chmurach, co ma szczególne znaczenie w kontekście pojawiających się coraz częściej informacji o nielegalnym przetwarzaniu danych umieszczonych w Internecie.

---

7 W przypadku sprawdzenia planowego, termin na przygotowanie sprawozdania wynosi 30 dni od zakończenia sprawdzenia; w przypadku sprawdzenia doraźnego, sprawozdanie powinno zostać przygotowane niezwłocznie po zakończeniu sprawdzenia; w przypadku kontroli przeprowadzonej na żądanie GIODO, termin ten zostaje określony w żądaniu GIODO przeprowadzenia kontroli.

Ochrona danych medycznych w chmurze

Piotr Najbuk | Prawnik, Associate

Dopuszczalność przetwarzania danych medycznych w chmurze

Model usług chmurowych może mieć, i coraz częściej ma, szerokie zastosowanie w usługach medycznych. Może on zostać przykładowo wykorzystany w związku zawarciem umowy powierzenia przetwarzania danych osobowych przez podmiot wykonujący działalność leczniczą a podmiot zewnętrzny (dostawca rozwiązań IT). Rozwiązanie chmurowe może również zostać potencjalnie wykorzystane bez zawierania umowy powierzenia przetwarzania danych osobowych – zgodnie ze stanowiskiem GIODO – „jeżeli podmiot udostępniający system (serwer) nie posiada wiedzy co do rodzaju danych przetwarzanych w tym systemie i nie powierzono mu danych w myśl art. 31 ustawy, to podlega on postanowieniom art. 14 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną i jego odpowiedzialność za przetwarzane dane jest ograniczona zgodnie z art. 12–15 tej ustawy".[8]

Do niedawna dopuszczalność powierzenia przetwarzania danych osobowych medycznych w szczególności tych zawartych w dokumentacji medycznej – była kwestionowana przez GIODO, który wskazywał, że powierzenie przetwarzania danych osobowych medycznych nie jest możliwe w świetle zapisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, stanowi bowiem naruszenie tajemnicy zawodowej osób wykonujących zawód medyczny.

8 GIODO, *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Wydawnictwo Sejmowe, Warszawa 2007

W dniu 9 października 2015 r. Sejm przyjął ustawę o zmianie ustawy o systemie informacji w ochronie zdrowia i niektórych innych ustaw, która wprost dopuściła możliwość powierzenia przetwarzania danych osobowych zgodnie z art. 31 ustawy o ochronie danych osobowych podmiotowi zewnętrznemu, wprowadzając jednocześnie następujące warunki (art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta):

1. zapewnienie ochrony danych osobowych;
2. zapewnienie możliwości kontroli prawidłowego przetwarzania danych osobowych;
3. realizacja umowy powierzenia przetwarzania danych osobowych nie może zakłócać udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia bez zbędnej zwłoki dostępu do danych zawartych w dokumentacji medycznej.

Ustawa o ochronie danych osobowych stanowi, iż warunkiem powierzenia przetwarzania jest m.in. spełnienie wymogów określonych w art. 36–39 ustawy oraz wymogów ustanowionych w rozporządzeniu wydanym na podstawie art. 39a ustawy.

Rozporządzenie, o którym mowa w punkcie poprzednim, zawiera wymogi istotne z punktu widzenia możliwości wykorzystania rozwiązań chmurowych – w szczególności administrator danych zobowiązany jest do przygotowania i posiadania dokumentu zawierającego politykę bezpieczeństwa, w której znajdować się powinien w szczególności wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykorzystywane oprogramowanie, sposób przepływu danych itp.[9]

Rozporządzenie w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania jest aktem szczególnym, określającym zasady przetwarzania danych medycznych. Zgodnie z § 25.1. zakończoną historię choroby lub kartę noworodka przekazuje się do komórki organizacyjnej właściwej do spraw dokumentacji chorych i statystyki medycznej. § 25 może budzić wątpliwości w kontekście outsourcingu dokumentacji medycznej. Zawiera on bowiem odniesienie do fizycznych miejsc znajdujących się w podmiocie wykonującym działalność leczniczą. Zgodnie z literalnym brzmieniem przepisu, dokumentacja medyczna, w tym także EDM, powinna fizycznie znajdować się w komórkach organizacyjnych wskazanych w tym przepisie.

Przywołane wyżej przepisy nie są precyzyjne, jeśli chodzi o możliwość przetwarzania danych medycznych poza obszarem placówki ochrony zdrowia – wprawdzie nowelizacja z 9 października 2015 r. dopuściła wprost możliwość outsourcingu danych, lecz jednocześnie zapisy innych aktów prawnych wprowadzają istotne ograniczenia w tym zakresie. O ile rozporządzenie w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania może być interpretowane w oparciu o wykładnie celowościową i systemową w sposób , który dopuszcza przetwarzanie danych medycznych poza placówką ochrony zdrowia, o tyle § 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny

9 § 4 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, wymaga bezwzględnie wskazania miejsca i zasobów wykorzystywanych do przetwarzania danych osobowych, co w przypadku chmury publicznej jest często niemożliwe.

Ze względu na wskazany wyżej wymóg, większą kontrolę nad przetwarzaniem danych osobowych i mniejsze ryzyko związane z ujawnieniem bądź utratą danych medycznych, chmura prywatna jest rozwiązaniem z prawnego punktu widzenia bezpieczniejszym i tym samym jest rozwiązaniem rekomendowanym do przetwarzania danych medycznych. Należy również pamiętać, że chmura publiczna może nie zapewnić realizacji podstawowego wymogu dopuszczalności powierzenia przetwarzania danych medycznych, jakim jest zapewnienie stałego dostępu do danych medycznych – w przypadku utraty dostępu do sieci Internet, placówka medyczna może potencjalnie utracić, przynajmniej czasowo, dostęp do danych. Problem ten może być dużo mniej dotkliwy w przypadku korzystania z chmury prywatnej, którą tworzą zasoby znajdujące się wewnątrz organizacji.

Normy ISO

Międzynarodowa Organizacja Normalizacyjna (ISO) opublikowała 1 sierpnia 2014 r. standard ISO/IEC, który ma na celu ujednolicenie standardu bezpieczeństwa usług w chmurach obliczeniowych. W publikacjach dotyczących wykorzystywania chmur obliczeniowych zwraca się uwagę na kilka elementów. Po pierwsze, na różnorodność usług dostarczanych na życzenie użytkownika. Usługi te mogą obejmować dostarczanie oprogramowania, wirtualnego środowiska pracy, sprzętu, świadczenia związane z przechowywaniem danych, tworzeniem ich kopii zapasowych czy kopii bezpieczeństwa. Jednocześnie zwraca się uwagę na kwestie bezpieczeństwa, użyteczności oraz zapewnienia rozliczalności i dostępności danych. Niejednokrotnie bowiem użytkownik usługi nie zna lokalizacji danych ani parametrów sprzętu wykorzystywanego przy przetwarzaniu danych osobowych. Właśnie obawy i ryzyko związane z przetwarzaniem danych w chmurach obliczeniowych legły u podstaw normy ISO/IEC 27018.

Przestrzeganie normy ISO 27018 daje pewność, że poufność danych będzie chroniona na kilka różnych sposobów:

1. **Zachowanie kontroli nad własnymi danymi.** Standard ISO 27018 gwarantuje przetwarzanie danych zgodnie z instrukcją otrzymaną od klienta;
2. **Informacja o przetwarzaniu danych.** Zapewnienie zasad zwrotu, przesyłania i usuwania danych osobowych przechowywanych w centrach danych. Informacja o lokalizacji przechowywania danych oraz wskazywanie podmiotów, które uzyskują prawo dostępu do danych. Informowanie o przypadkach dostępu osób nieupoważnionych do danych osobowych oraz obiektów i sprzętu używanego do przetwarzania danych, jeżeli skutkują one utratą, ujawnieniem lub modyfikacją tych danych.
3. **Skuteczna ochrona danych.** Norma ISO 27018 zapewnia różne istotne środki ochrony. Poprzez ograniczenia sposobów postępowania z danymi osobowymi, w tym ograniczenia ich przesyłania w sieciach publicznych i przechowywania na nośnikach przenośnych. Określone procesy

odzyskiwania i przywracania danych. Standard wyznacza również obowiązek poufności wszystkich osób, które mają styczność z danymi.

4. **Niewykorzystywanie danych osobowych do celów reklamowych.** Wyłączenie możliwości wykorzystywania danych zgromadzonych w chmurze do celów reklamowych.
5. **Informacja o dostępie organów państwowych do danych.** Norma ta, o ile prawo tego nie zabrania, wymaga informowania o wnioskach organów państwowych o ujawnienie danych osobowych.

Chmury obliczeniowe są niewątpliwie rozwiązaniem bardzo atrakcyjnym. Jednocześnie z rozwiązaniami chmurowymi wiąże się szereg ryzyk prawnych. Ze względu na wskazane ryzyka, rekomendowaną technologią do przetwarzania danych medycznych jest technologia chmury prywatnej. Podmiot wykonujący działalność leczniczą, decydujący się na korzystanie z rozwiązań chmurowych, powinien zwracać uwagę na renomę dostawy rozwiązania IT i posiadanie przez niego stosownych norm ISO.

Wiążące reguły korporacyjne (BCR) jako element efektywnej polityki *compliance*

dr Anna Partyka-Opiela | Senior Associate

Czym jest compliance i jakie daje korzyści?

Compliance, czy też zarządzanie zgodnością, to sposób organizacji przedsiębiorstwa, którego celem jest zapewnienie zgodności działań biznesowych z zasadami etyki i przepisami prawa. Wdrożenie systemu zarządzania zgodnością pomaga obniżyć ryzyka prawne, związane z prowadzeniem działalności gospodarczej oraz pozwala skuteczniej ochronić przedsiębiorstwo przed negatywnymi konsekwencjami niezgodnego z prawem zachowania pracowników.

Prawidłowo wdrożony i działający system compliance podnosi wiarygodność organizacji w oczach partnerów biznesowych oraz wpływa na zwiększenie konkurencyjności przedsiębiorstwa na rynku[10]. Jednym z obszarów compliance jest problematyka bezpieczeństwa IT, w tym kwestie związane z outsourcingiem usług informatycznych i ochroną danych osobowych.

Czym są wiążące reguły korporacyjne?

Wiążące reguły korporacyjne regulują kwestie międzynarodowego transferu danych osobowych pomiędzy podmiotami należącymi do jednej grupy kapitałowej. Wyróżnia się reguły przeznaczone dla administratorów danych (ang. *Binding Corporate Rules*) oraz skierowane do przetwarzających dane

10 M. Borowa, *Program compliance – przepis na sukces. Jakie wymagania powinny być spełnione z praktycznego punktu widzenia?*, Dodatek do MoP 23/2013, str. 12.

osobowe na zlecenie (ang. *processor binding corporate rules*). Wiążące reguły korporacyjne przyjmują postać zbioru dokumentów wewnętrznych, których celem jest wprowadzenie jednolitych zasad przetwarzania danych osobowych wewnątrz grupy kapitałowej oraz zapewnienie odpowiedniego poziomu ich ochrony w państwach, które nie gwarantują go na mocy przepisów prawa krajowego.

W kontekście *cloud computingu* istotnego znaczenia nabierają reguły przeznaczone dla podmiotów przetwarzających dane na zlecenie (tzw. *processorów)*. Wobec powszechnej praktyki lokowania serwerów w różnych częściach globu oraz swobodnego i nieskrępowanego przepływu powierzonych danych między poszczególnymi lokalizacjami, zapewnienie właściwego i jednolitego poziomu bezpieczeństwa jest niezbędne, szczególnie przy współpracy z administratorami danych mających siedzibę na terenie Polski i innych państw EOG. Zgodnie z opinią Grupy Roboczej Art. 29[11], prawem właściwym dla przetwarzania danych osobowych jest ustawodawstwo ustalone ze względu na siedzibę administratora powierzającego dane[12]. Tym samym, w przypadku naruszenia przepisów o ochronie danych osobowych w toku przetwarzania danych w chmurze, *processor* – oprócz odpowiedzialności kontraktowej wobec administratora – musi liczyć się nawet z koniecznością poniesienia odpowiedzialności karnej na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2014 r. poz. 1182 z późn. zm.) – dalej jako UODO.

Jak wygląda transfer danych osobowych bez wykorzystania wiążących reguł?

Zgodnie z art. 47 ust. 1 UODO, *przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych*. Natomiast zgodnie z art. 48 ust. 1 UODO transfer danych osobowych do państwa niezapewniającego należytej ochrony – o ile nie odbywa się w związku z jednym z wyjątków przewidzianych w art. 47 ust. 2 i 3 UODO – wymaga każdorazowo uzyskania zgody Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Od strony praktycznej, proces transferu danych osobowych do państwa trzeciego (również w ramach tej samej grupy kapitałowej) powinien każdorazowo rozpocząć się od analizy przepisów dot. ochrony danych osobowych obowiązujących w państwie docelowym. W przypadku uznania przez administratora

---

11 Grupa Robocza Art. 29 jest niezależnym ciałem doradczym powołanym na mocy art. 29 Dyrektywy 95/46/WE. W skład grupy wchodzą przedstawiciele organów ochrony danych osobowych z państw członkowskich UE oraz przedstawiciele urzędów UE. Grupa ma charakter niezależny, jednak jej opinie bardzo często stanowią podstawę dla działań państw członkowskich i instytucji UE.

12 *Opinia Grupy Roboczej Art. 29 nr 5/2012 dot. cloud computingu*; dostępna na: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf oraz *Opinia Grupy Roboczej Art. 29 nr 8/2010 o prawie właściwym;* dostępna na: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf

danych, że przepisy te nie zapewniają odpowiedniego (a więc w praktyce przynajmniej zbliżonego do europejskiego) poziomu ochrony danych osobowych, konieczne jest takie uregulowanie transferu w ramach umowy pomiędzy administratorem i odbiorcą danych, aby właściwy poziom zabezpieczeń został zagwarantowany za pomocą zobowiązań kontraktowych.

Ze względu na swoją charakterystykę techniczną, przetwarzanie danych w modelu *cloud computingu* powoduje trudności w ustaleniu państwa, do jakiego dane będą transferowane. Nawet jeśli znane są lokalizacje serwerów, to nie sposób jest przewidzieć, w której z nich powierzone dane będą przetwarzane. Co więcej, w przypadku rozbudowy zaplecza technicznego dostawcy usług, dane mogą zacząć być przetwarzane w lokalizacji, która nie została ustalona w trakcie negocjacji umownych, co może rodzić dodatkowe ryzyka dla administratora danych i processora.

Biorąc pod uwagę, że regulacje dot. ochrony osobowej obowiązują w ok. 50–60 różnych jurysdykcji[13], a powyższy proces powinno się powtórzyć w przypadku każdego transferu danych do państwa trzeciego, nie trudno sobie wyobrazić, że zagwarantowanie właściwego poziomu ochrony w umowie jest stosunkowo trudne. Skomplikowanie regulacji w tym zakresie powoduje również, że skala nielegalnych transferów – a tym samym ryzyko prawne dla administratorów i processorów – jest ogromne[14].

Co daje stosowanie wiążących reguł?

Z punktu widzenia administratora danych, podstawową zaletą wprowadzenia BCR w organizacji jest zwolnienie z obowiązku uzyskiwania zgody GIODO na transfer danych do państwa trzeciego, pod warunkiem wcześniejszego zaakceptowania treści reguł przez organ ochrony danych (art. 48 ust. 2 pkt. 2) UODO). W efekcie, upraszcza się zasady przepływu danych w ramach organizacji oraz unika konieczności zawierania wielu umów transferowych pomiędzy poszczególnymi spółkami, wchodzącymi w skład danej grupy kapitałowej[15]. W przypadku dużych grup kapitałowych ilość dokumentów, które regulują zasady transferu dochodzić może do kilkuset (polityki prywatności i bezpieczeństwa, umowy transferowe, instrukcje, itp.). Znacząca ilość dokumentacji i częsty brak jej wewnętrznej spójności rodzi pole do nadużyć i utrudnia edukację pracowników w tym zakresie. Dzięki zastosowaniu BCR liczba dokumentów ulega znaczącemu zmniejszeniu a pracownikom łatwiej jest zrozumieć i stosować w praktyce zasady regulujące przetwarzanie danych osobowych.

---

13 C. Kuner, *International Legal Framework for Data Protection: Issues and Prospects*, Computer Law & Security Review, Vol. 25, str. 307 I n., 2009. Dostępny na: http://ssrn.com/abstract=1443802

14 W raporcie Komisji Europejskiej dot. wdrożenia Dyrektywy 95/46/WE wskazano, że liczba prawidłowo zgłoszonych transferów danych osobowych jest o wiele niższa od oczekiwań KE. W połączeniu z innymi zgromadzonymi informacjami, KE konkluduje, że na terenie UE dochodzi do bardzo dużej liczby nielegalnych transferów danych do państw niezapewniających odpowiedniego poziomu ich ochrony. Raport dostępny na: http://aei.pitt.edu/45392/1/COM_%282003%29_265_final.pdf

15 J. Byrski, X. Konarski, *Wiążące reguły korporacyjne jako podstawa prawna przekazywania danych osobowych do państwa trzeciego,* [w:] A. Mednis (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym,* Warszawa 2013, str. 93.

Z punktu widzenia dostawcy usług *cloud computingowych*, wprowadzenie wiążących reguł korporacyjnych – oprócz korzyści wspomnianych powyżej – pomaga również znacząco uprościć proces negocjacji umownych z podmiotami zainteresowanymi skorzystaniem z oferowanych usług, a tym samym pozytywnie wpływa na pozycję rynkową przedsiębiorstwa. Dodatkowo, wiążące reguły pomagają uprościć współpracę z podwykonawcami.

Niestety, do dnia dzisiejszego Polska nie przystąpiła do porozumienia dot. automatycznego uznawania wiążących reguł korporacyjnych, zatwierdzonych w innych państwa członkowskich EOG[16]. Oznacza to, że przed wprowadzeniem BCR w ramach podmiotu działającego na terenie RP, konieczne jest jego zaakceptowanie przez GIODO. Zmiany w tym zakresie przyniesie przygotowywane właśnie rozporządzenie ogólne o ochronie danych osobowych (RODO)[17].

Co powinny zawierać BCR?

Brak jest przepisów, które jednoznacznie wskazują jakie konkretnie zapisy powinny znaleźć się w BCR. Kierując się jednak opiniami Grupy Roboczej Art. 29[18] oraz postanowieniami RODO, wyróżnić można treści, które dokument taki powinien zawierać.

BCR powinny określać dokładnie wszystkie podmioty, które wchodzą w skład grupy, w ramach której wprowadza się reguły. Określone powinny zostać rodzaje i kategorie dokonywanych transferów danych oraz państwa, do których dane będą przekazywane. Ponadto, należy opisać zakres przetwarzanych danych oraz określić w sposób ogólny podmioty, których dane dotyczą. W dalszej kolejności należy opisać mechanizmy, które służyć będą egzekucji postanowień BCR w ramach relacji wewnętrznych i zewnętrznych danej grupy. Konieczne jest również wskazanie podstaw prawnych, które legalizują gromadzenie i przetwarzanie danych w ramach grupy kapitałowej. Należy również pamiętać o wskazaniu praw, jakie przysługiwać będą podmiotom danych oraz o wprowadzeniu mechanizmów, które pozwolą na ich skuteczną egzekucję. Dodatkowo, w BCR określić można, jakie wymagania stosowane będą wobec podmiotów spoza grupy, którym udostępnia się dane lub powierza ich przetwarzanie. Ostatecznie konieczne jest wyznaczenie osoby, która będzie odpowiedzialna za monitoring przestrzegania BCR

16 Lista państw, które są stronami porozumienia *mutual recognition* dostępna jest na: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm

17 Rozporządzenie ogólne wprowadzi jednolite przepisy w zakresie ochrony danych osobowych na terenie całej UE. W RODO uregulowane zostaną szczegółowo m.in. kwestie dot. BCR i ich wzajemnej uznawalności. Prace nad rozporządzeniem powinny zakończyć się w grudniu 2015 r. Przepisy RODO wejdą w życie 2 lata po ich oficjalnej publikacji, tj. najprawdopodobniej na początku 2018 r.

18 *Working Document 02/2012 setting up a table with the elements to be found in Processor Binding Corporate Rules*, dostępny na: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf oraz *Working Document setting up a framework for the structure of Binding Corporate Rules (WP 154)*, dostępny na: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf

w ramach grupy oraz wskazanie sposobu, w jakim wiążące reguły będą udostępniane podmiotom danych i organom ochrony danych osobowych.

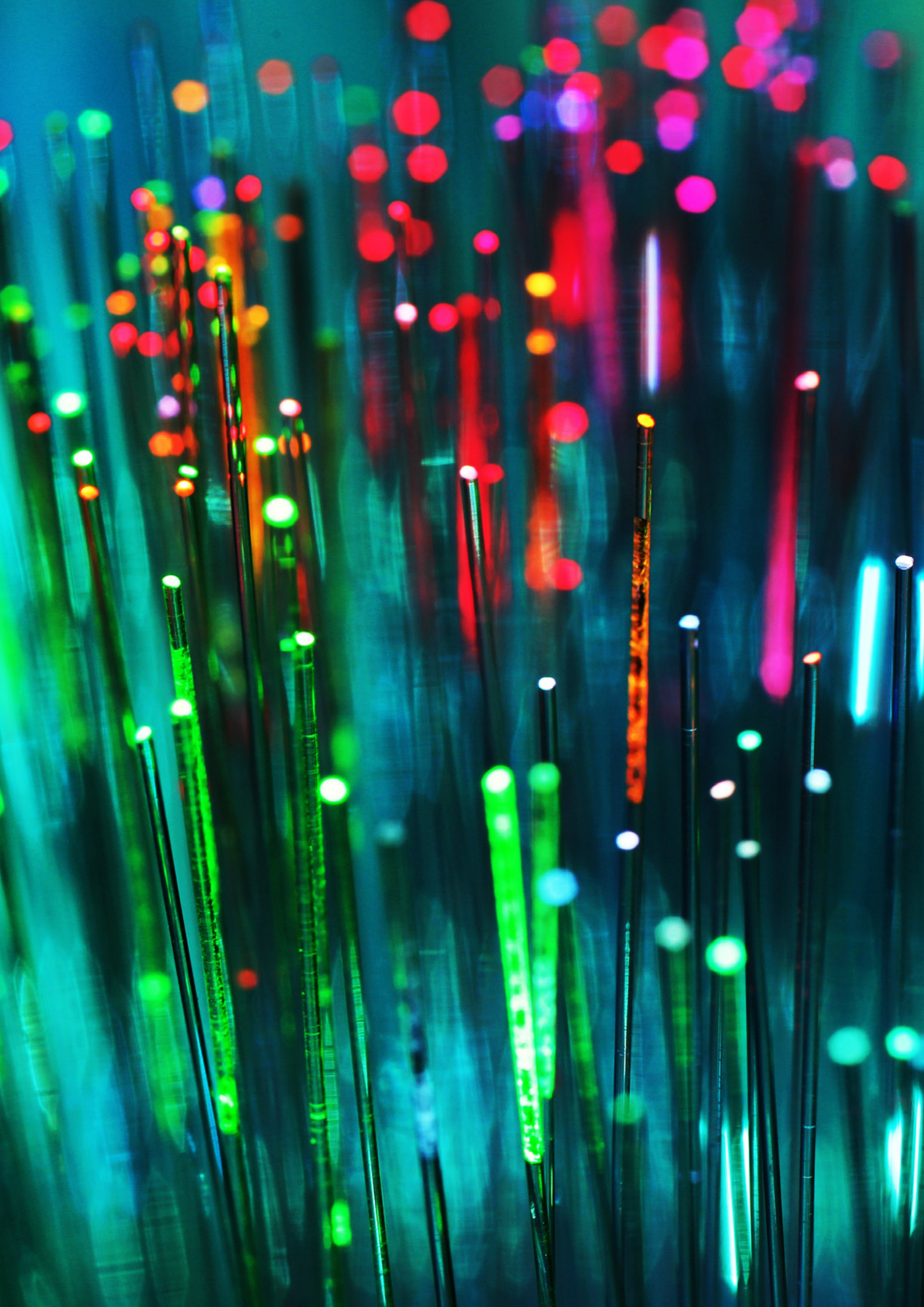
Jakie mechanizmy pomogą egzekwować postanowienia BCR ?

Zarówno ogólne zasady compliance, jak i opinie Grupy Roboczej ds. Art. 29, jednoznacznie potwierdzają, że samo wdrożenie BCR nie zapewni jego skuteczności. W tym celu konieczne jest wprowadzenie mechanizmów pozwalających na skuteczną egzekucję wprowadzonych regulacji. Do działań takich zalicza się m.in.:

1. regularna ocena poziomu zaangażowania pracowników w przestrzeganie norm wewnętrznych organizacji oraz uwzględnianie postaw etycznych w ramach mechanizmów cyklicznej oceny personelu;
2. przejrzysta komunikacja wewnętrzna (tzw. *plain language*) oraz regularne szkolenia dla pracowników w zakresie istniejących standardów i procedur postępowania;
3. wdrożenie procedur raportowania wewnętrznego i controllingu, w tym zapewnienie możliwości anonimowego zgłaszania naruszeń (tzw. *whistleblowing*);
4. cykliczne audyty zgodności, których wyniki przekazywane są do kadry zarządzającej najwyższego szczebla;
5. informowanie opinii publicznej o podjętych działaniach i wynikach kontroli, np. w formie informacji zamieszczanych na stronach internetowych organizacji[19].

Wskazane powyżej działania nie są charakterystyczne tylko dla BCR, ale stanowią trzon systemów zarządzania zgodnością w przedsiębiorstwach. Oznacza to, że wymienione mechanizmy powinny funkcjonować w odniesieniu do każdego rodzaju polityki prawnej lub etycznej, która wdrażana jest w ramach organizacji. Można zatem uznać, że wdrożenie BCR w przedsiębiorstwach, które nie korzystały dotychczas z tego rozwiązania, ale mają stworzone skuteczne systemy zarządzania zgodnością w odniesieniu do innych aspektów swojej działalności, nie powinno stanowić dużego wyzwania a może przynieść wymierne korzyści, w postaci zapewnienia zgodności działań grupy kapitałowej z przepisami o ochronie danych osobowych i obniżyć ryzyko odpowiedzialności z tego tytułu.

19 Ch. Parker, *Meta-regulation: legal accountability for corporate social responsibility*, str. 15 i n., dostępne na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=942157



Prawa autorskie a usługi chmurowe

Jakub Kubalski | Associate

Truizmem jest stwierdzenie, iż prawo nie nadąża za rozwojem techniki. Ludzka inwencja jest oczywistym motorem gospodarki światowej. Na forpoczcie tych innowacji są technologie informatyczne. Ostatnimi laty coraz większą popularność zdobywają usługi przetwarzania w chmurze. Niektóre modele *cloud computingu*, 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, pomimo tego, że usługobiorca ma dostęp do korzystania z danego oprogramowania, to samo oprogramowanie nie jest odtwarzane ani uruchamiane, ani w większości przypadków nie znajduje się nawet w pamięciach urządzeń usługobiorcy.

Niemniej jednak, intuicyjnie wydawałoby się, że usługobiorca **korzysta** z danego oprogramowania w usługach SaaS i PaaS. Skoro zatem może mieć miejsce korzystanie, to czy podmiot uprawniony z tytułu autorskich praw majątkowych nie powinien otrzymywać wynagrodzenia za takie korzystanie? Te wątpliwości obracają się wokół tytułowego pytania niniejszego wpisu, a mianowicie, czy można traktować *cloud computing* jako korzystanie z autorskich praw majątkowych w ramach pól eksploatacji, zapisanych w ustawie o prawie autorskim i prawach pokrewnych?

Utwór a program komputerowy

Program komputerowy, zgodnie z ustawą o prawie autorskim i prawach pokrewnych jest chroniony jak utwory literackie. Nie należy jednak zapominać, iż oprogramowanie wykonalne zawiera nie tylko program komputerowy, lecz z reguły również inne utwory – tekst, grafikę, niekiedy utwory muzyczne i audiowizualne. W wyroku z dnia 22 grudnia 2010 r., w sprawie *Bezpečnostní softwarová asociace* C393/09, Trybunał Sprawiedliwości UE stwierdził, iż:

[…] *graficzny interfejs użytkownika nie pozwala na powielanie tego programu komputerowego, lecz stanowi po prostu element tego programu, za pomocą którego użytkownicy wykorzystują właściwości omawianego programu*.

Trybunał jednocześnie zaznaczył, iż pomimo tego, że graficzny interfejs użytkownika – GUI – nie podlega ochronie prawno-autorskiej jako program komputerowy, to z powodzeniem może podlegać ochronie przewidzianej w ogólnych przepisach prawa autorskiego.

Zgodnie z powołanym wyżej orzecznictwem, kod źródłowy i wynikowy programu komputerowego będzie podlegał ochronie prawno-autorskiej jako program komputerowy, gdyż jest on formą wyrażenia takiego programu. Inne elementy, jeżeli spełniają generalne warunki do uznania ich za utwory w rozumieniu prawa autorskiego, podlegają ogólnej ochronie prawno-autorskiej, vide: GUI.

Przesłanki uznania korzystania w ramach istniejących lub nowych pól eksploatacji

Z koncepcji monopolu autorskiego wynika, iż jeśli w przyszłości pojawią się nowe techniczne sposoby korzystania z utworu, to zostaną objęte treścią majątkowego prawa autorskiego, chyba że ustawa postanowi inaczej. Wyrazem tego jest redakcja przepisu art. 50 ustawy, która zawiera otwarty katalog pól eksploatacji, poprzez wyrażenie „w szczególności".

Modele PaaS i SaaS zapewniają usługobiorcy dostęp do oprogramowania (samego systemu operacyjnego lub łącznie z pakietem aplikacji) poprzez zapewnienie zasobów IT na żądanie użytkowników, z wykorzystaniem infrastruktury usługodawcy.

Wydaje się, że takie korzystanie z oprogramowania, jakie ma miejsce w modelu SaaS i PaaS *cloud computingu*, ma odmienny charakter niż dotychczasowe sposoby dystrybucji i odtwarzania programu komputerowego. Ponadto, tworzony jest nowy, odmienny rynek rozpowszechniania produktów IT, które są dedykowane do usług przetwarzania w chmurze. Przykładowo, podmiot zwlekający z wdrożeniem konkretnego systemu informatycznego, z racji wysokich kosztów zakupu infrastruktury, obecnie może wdrożyć taki system na sprzęcie dostawcy usług przetwarzania w chmurze.

Odtwarzanie w chmurze programów komputerowych ma podobny charakter, co usługi telewizji *Video on Demand*. Wielu użytkowników VoD bowiem nie kupiłoby kopii DVD czy Blu-ray danego filmu, lecz swobodny i łatwy dostęp do różnych mediów powoduje, iż tworzony jest nowy rynek dla materiałów audiowizualnych i poprzez to, odrębne ekonomiczne znaczenie określonego sposobu użycia[20].

Można postulować wszakże, że korzystanie z usług *cloud computing* w większości przypadków będzie równoznaczne z korzystaniem z praw majątkowych do programu komputerowego i korzystaniem z autorskich praw majątkowych do innych utworów, w ramach obecnie istniejących pól eksploatacji, określonych w art. 50 pkt. 3) bądź art. 74 ust. 4 pkt. 1) lub 3) ustawy o prawie autorskim i prawach pokrewnych, tj.:

---

20 Postulat uznania VoD jako nowego pola eksploatacji jest zasugerowany przez E. Traple w: *System Prawa Prywatnego – Prawo autorskie*, pod red. J. Barty, tom 13, Warszawa 2007, s. 150.

1. w zakresie autorskich praw majątkowych do twórczych elementów oprogramowania nie będącego programem komputerowym (np. GUI) – publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym (art. 50 pkt. 3);
2. w zakresie praw majątkowych do programu komputerowego:
   a) trwałe lub czasowe zwielokrotnienia programu komputerowego w całości lub w części **jakimikolwiek środkami i w jakiejkolwiek formie**[21] **(art. 74 ust. 4 pkt.1), lub**
   b) rozpowszechniania, w tym użyczenia lub najmu, programu komputerowego lub jego kopii (art. 74 ust. 4 pkt. 3).

Kto korzysta z oprogramowania w chmurze?

Niezależnie jednak od kwestii, czy przetwarzanie w chmurze stanowi nowe formy eksploatacji programów komputerowych, czy też zawiera się w ramach obecnie funkcjonujących pól eksploatacji, korzystanie z usług przetwarzania w chmurze, może oznaczać korzystanie z praw majątkowych do programu komputerowego, jak również autorskich praw majątkowych do innych twórczych elementów programu komputerowego (np. GUI).

W stosunku prawnym, przedmiotem, którego jest usługa SaaS lub PaaS, korzystającym z oprogramowania, niewątpliwie jest usługobiorca. Trudno bowiem uznać, by korzystał z tego oprogramowania inny podmiot, gdyż to właśnie usługobiorca ma możliwość zapoznawania się i czerpania korzyści z programu komputerowego, udostępnionego mu za pośrednictwem chmury obliczeniowej.

Zatem świadczenie usług przetwarzania w chmurze, w ramach których uruchamiane jest oprogramowanie na rzecz usługobiorcy, będzie wymagało określenie uprawnień licencyjnych dla usługobiorcy.

W celu realizacji zamierzeń biznesowych usługodawcy *cloud computingu* należy prawidłowo określić zakres, treść, rodzaj takiej licencji dla użytkownika, na podstawie charakterystyki konkretnej usługi przetwarzania w chmurze.

---

[21] W literaturze spotykana jest opinia, iż jeżeli nie jest dokonywana czynność zwielokrotnienia programu komputerowego w ramach infrastruktury sprzętowej usługobiorcy, to nie można mówić o korzystaniu z praw majątkowych do programu komputerowego. Sądzę, że należy jednak zwrócić uwagę na pełną redakcję tego przepisu, tj. *„zwielokrotniania programu komputerowego* […] *jakimikolwiek środkami i w jakiejkolwiek formie"*. Moim zdaniem, usługi przetwarzania w chmurze w modelu SaaS oraz PaaS w istocie polegają na zwielokrotnieniu programu w infrastrukturze usługodawcy (uruchomienie wielu kopii, lub udostępnienie kopii wielu usługobiorcom). Należy zwrócić uwagę, iż ustawa nie uzależnia prawa do zwielokrotniania od tego, gdzie takie zwielokrotnianie się odbywa. Zob. także: E. Molenda-Kropielnicka, *Cloud computing – zagadnienia prawne,* ZNUJ 2013, z. 119, str. 109 i n.

Charakter odróżniający znaków towarowych zawierających element „cloud”

Monika Gebel | Associate

Dotychczasowe próby rejestracji oznaczenia

Posługiwanie się oznaczeniem odróżniającym, zawierającym słowo „cloud”, dla działalności związanej ze świadczeniem usług w chmurze, stanowi atrakcyjną możliwość dla przedsiębiorców. Pozwala na czytelne wskazanie charakteru prowadzonej działalności i szybkie dotarcie do właściwego kręgu odbiorców. Oznaczenie to cieszy się już od kilku lat dużą popularnością, wyrażającą się między innymi w licznych próbach rejestracji w charakterze znaku towarowego – tylko pomiędzy 2007 a 2011 rokiem do amerykańskiego urzędu patentowego (USPTO) skierowano około 500 zgłoszeń znaków towarowych zawierających wspomniane słowo.

Jedną z pierwszych decyzji, w których odniesiono się do tych prób, była decyzja USPTO w sprawie słownego znaku towarowego „cloud computing”. Znak zgłosiła spółka Dell dla usług takich, jak m.in. produkcja sprzętu komputerowego do wykorzystania w centrach przetwarzania danych oraz projektowanie i rozwój sieci do wykorzystania w centrach przetwarzania danych. Należy zauważyć, że po zgłoszeniu przez Dell ,oznaczenie zostało zarejestrowane jako słowny znak towarowy i dopiero w późniejszej decyzji z 12 sierpnia 2008 r. USPTO stwierdził, iż oznaczenie „cloud computing” nie może być przedmiotem prawa wyłącznego na znak towarowy ze względu na jego opisowy charakter dla usług, dla których zostało zarejestrowane. USPTO uzasadnił swoją decyzję między innymi tym, iż oznaczenie,

które próbował zarejestrować Dell, opisuje jedynie cechę charakteryzującą usługę świadczoną przez zgłaszającego (*feature and characteristic of applicant's services*). Jak wskazał USPTO, oznaczenie ma charakter jedynie opisowy, gdy opisuje składnik, właściwość lub funkcję dóbr czy usług. USPTO, powołując się na słownikowe znaczenie terminu *cloud computing* uznał, że jest ono w analizowanej sprawie opisowe dla usług zgłaszającego, na które składają się m.in. produkcja sprzętu komputerowego, ponieważ przeciętny przyszły konsument usług tego rodzaju, zobaczywszy znak towarowy „cloud computing" w połączeniu z działalnością zgłaszającego, natychmiast spostrzeże cechę tych usług.

Opisowość oznaczenia i jej konsekwencje

Podobnie, jak amerykański Trademark Act[22], również krajowy system rejestracji znaków towarowych oraz istotny dla polskich przedsiębiorców system rejestracji znaków wspólnotowych, podlegających ochronie we wszystkich krajach UE, znają pojęcie opisowości znaku towarowego.
Zgodnie z polską ustawą – prawo własności przemysłowej[23] – oznaczenie o opisowym charakterze pozbawione jest zdolności odróżniającej. Znak opisowy jedynie opisuje zgłoszone towary lub usługi – składa się wyłącznie, zgodnie z przykładowym katalogiem sformułowanym w p.w.p., *z elementów mogących służyć w obrocie do wskazania w szczególności rodzaju towaru, jego pochodzenia, jakości, ilości, wartości, przeznaczenia, sposobu wytwarzania czy funkcji*. Co za tym idzie, zgodnie z art. 129 ust. 2 pkt 2 p.w.p. oznaczenie takie nie podlega ochronie.

Jak wskazuje się w orzecznictwie, opisowy charakter znaku można odróżnić od nieopisowego w ten sposób, że na opisowy charakter znaku wskazuje okoliczność, iż jedyną i bezpośrednio przekazywaną informacją jest ta, która wskazuje na cechę towaru, zaś opisowego charakteru nie mają te znaki, które dopiero drogą pośredniego wnioskowania mogą stanowić oznaczenie takich cech[24].

Należy zauważyć, że ocena opisowego charakteru oznaczenia jest dokonywana, podobnie jak wskazano na to w decyzji USPTO, z perspektywy odbiorcy danych usług czy towarów – osoby, do której są one kierowane. Opisowymi słownymi znakami towarowymi będą zatem dla przykładu znak „chmura" dla usług związanych z cloud computingiem czy też znak słowny „szybkiewifi" dla usług związanych z bezprzewodowym Internetem.

Warto zauważyć, że chociażby minimalnie opisowy charakter zarejestrowanego już znaku, stanowi również ograniczenie zakresu ochrony znaku towarowego – zgodnie z art. 156 ust. 1 pkt 2 p.w.p. uprawniony ze znaku towarowego nie może zakazać używania przez inne osoby w obrocie oznaczeń wskazujących w szczególności na cechy i charakterystykę towarów, ich rodzaj, ilość, jakość, przeznaczenie, pochodzenie czy datę wytworzenia lub okres przydatności.

---

22 US Trademark Law, section 2 (e)(1), http://www.uspto.gov/sites/default/files/trademarks/law/Trademark_Statutes.pdf

23 Ustawa z dnia 30 czerwca 2000 r. (Dz. U. 2001 nr 49 poz. 508).

24 Por. wyrok Naczelnego Sądu Administracyjnego z dnia z dnia 16 grudnia 2009 r., sygn. II GSK 214/09.

Opisowość oznaczenia stanowi również przeszkodę w jego rejestracji na gruncie rozporządzenia o wspólnotowym znaku towarowym[25]. Zgodnie z art. 7 pkt 1 c i d rozporządzenia, nie są rejestrowane takie znaki towarowe, które *składają się wyłącznie z oznaczeń lub wskazówek mogących służyć w obrocie do oznaczania rodzaju, jakości, ilości, przeznaczenia, wartości, pochodzenia geograficznego lub czasu produkcji towaru lub świadczenia usługi, lub innych właściwości towarów lub usług* oraz takie, które *składają się wyłącznie z oznaczeń lub wskazówek, które weszły do języka potocznego lub są zwyczajowo używane w uczciwych i utrwalonych praktykach handlowych.*

Również w tym przypadku opisowość oznaczenia oceniana jest z punktu widzenia odbiorców danych usług (*relevant public*). Co istotne, jak wskazuje Urząd Harmonizacji Rynku Wewnętrznego w Alicante (OHIM) w metodologii oceny znaku, znaki nie podlegają rejestracji, jeżeli są opisowe w którymkolwiek z oficjalnych języków Unii Europejskiej, niezależnie od rozmiaru kraju bądź liczby jego ludności. Niezależnie od tego, OHIM wskazuje również, iż w wypadku przekonywujących dowodów na to, iż dane oznaczenie posiada opisowy charakter również w języku innym niż jeden z oficjalnych języków UE, również takie oznaczenie nie zostanie zarejestrowane.

Dla przykładu, oznaczeniem wskazanym przez OHIM jako opisowe ze względu na wskazywanie celu i funkcji jest oznaczenie słowne „TRUSTEDLINK", które próbowano zarejestrować dla dóbr i usług w sektorze IT, w tym m.in. dla oprogramowania dla e-commerce[26]. Innym oznaczeniem, którego ochrony ze względu na opisowy charakter odmówił OHIM, jest oznaczenie „CLEARWIFI", które zgłoszono dla usług telekomunikacyjnych, w tym w szczególności szybkiego dostępu do sieci komputerowych i komunikacyjnych[27].

Jakie rozwiązanie wybrać, jeżeli chcemy, aby w naszym oznaczeniu mimo wszystko znalazło się wyrażenie „cloud", „cloud computing" lub ich polskie odpowiedniki?

Mimo faktu, iż decyzji o treści podobnej do omówionej wyżej decyzji USPTO w sprawie oznaczenia Dell, można spodziewać się w przypadku próby zgłoszenia oznaczenia „cloud computing" (lub też samego oznaczenia „cloud") dla usług świadczonych w podobnym zakresie w Urzędzie Harmonizacji Rynku Wewnętrznego w Alicante (OHIM) lub też w Urzędzie Patentowym RP, w wypadku woli używania

któregoś z tych oznaczeń w obrocie, możliwe jest dokonanie takiej zmiany zgłaszanego oznaczenia, która pozwoli na jego rejestrację.

---

25 Rozporządzenie Rady nr 207/2009 z dnia 26 lutego 2009 r.

26 Por. wyrok Sądu Pierwszej Instancji w sprawie T-345/99 „TRUSTEDLINK z 26 października 2000 r.

27 Por. wyrok Sądu Pierwszej Instancji w sprawie T-399/08 „CLEARWIFI" z 19 listopada 2009 r.

Istnieje szereg działań polegających na odpowiedniej modyfikacji oznaczenia, które mogą doprowadzić do uznania, iż znak posiada odróżniający charakter. Pierwszym z zabiegów, który może nadać oznaczeniu opisowemu zdolność odróżniającą, jest umieszczenie opisowego wyrażenia w odpowiednim kontekście i stworzenie tzw. znaku złożonego. Taki znak można utworzyć m.in. poprzez:

1. dodanie do elementu opisowego dodatkowych słów – modyfikację znaku, np. poprzez dodanie do słowa opisowego np. firmy zgłaszającego, pod warunkiem, że nie jest ona również wyrażeniem opisowym dla danej klasy towarów lub usług;
2. dodanie do elementu opisowego elementów graficznych, takich jak np. krój czcionki, kolor czy dodatkowy rysunek, a tym samym stworzenie znaku słowno-graficznego zawierającego interesujący nas element.

Jak wskazuje się w doktrynie, o zdolności odróżniającej znaku, w skład którego wchodzi takie opisowe wyrażenie, będą decydować pozostałe oznaczenia słowne lub graficzne. Element opisowy ogólno-informacyjny nawet w takiej sytuacji nie będzie mógł uzyskać samodzielnie odróżniającego charakteru[28]. Należy jednak zauważyć, że nawet złożony znak może zostać uznany za opisowy w sytuacji, w której składa się na niego kilka opisowych wyrażeń. Nie będzie on natomiast uznany za opisowy, gdy występujące w nim dodatkowe elementy będą miały charakter dystynktywny i pozwolą na uznanie go za oznaczenie odróżniające. Należy pamiętać o tym, iż znak towarowy badany jest w sposób całościowy – nie ocenia się osobno każdego z elementów składających się na oznaczenie, lecz wszystkie te elementy łącznie. Powyższe dotyczy zarówno oznaczeń zawierających wyłącznie wyrażenia w języku polskim, jak i wyrażenia w różnych językach.

Zabiegiem, który można zastosować, aby nadać danemu oznaczeniu charakter odróżniający jest również stworzenie neologizmu – nowego wyrazu jedynie pośrednio wskazującego na charakter świadczonych usług. Dla przykładu, OHIM nie zarejestrował wspomnianego wcześniej znaku „TRUSTEDLINK", zarejestrował jednak znak towarowy „LINQ" m.in. dla usług telekomunikacyjnych. Różnica zdaje się być niewielka, jednak w uzasadnieniu OHIM wskazał, że oznaczenie to ma zdolność odróżniającą i może stanowić znak towarowy, ponieważ jest wymyślone, nie jest dostępne w żadnym ze słowników i nie stanowi popularnego błędu ortograficznego.

Mimo wypracowania w doktrynie i orzecznictwie pewnych standardów oceny znaków oraz metod oceny ich charakteru odróżniającego, każdy przypadek – zgłaszane oznaczenie – powinien być oceniany indywidualnie dla klas produktów, dla których ma zostać zarejestrowany oraz z perspektywy odbiorcy, do którego te dobra i usługi są kierowane. Jak wspomniano, oznaczenie oceniane jest w sposób całościowy, a zatem to, czy szereg słów zarejestrowanych dla danych klas towarów bądź usług, będzie miało charakter odróżniający, będzie zależało od wielu czynników, z których najistotniejsze zostały wskazane w niniejszym artykule.

---

28 Por. P. Kostański, *Prawo własności przemysłowej,* Warszawa 2014.

Zespół kancelarii Domański Zakrzewski Palinka

Praktyka IP&TMT

Praktyka IP&TMT to zespół doświadczonych ekspertów, który doradza w dziedzinach związanych z prawami na dobrach niematerialnych. Posiadamy wieloletnie doświadczenie w zakresie prawa autorskiego i praw pokrewnych, prawa własności przemysłowej, ochrony dóbr osobistych i ochrony baz danych. Nasi eksperci doradzają również w kwestiach prawnych związanych z IT. Doświadczenie w zakresie sporządzania i negocjowania umów IT oraz gałęzi prawa powiązanych z tą tematyką, pozwala nam sprostać wyzwaniom na rynku usług IT, m.in. kwestiom prawnym związanym z usługami cloud computing. Nasze usługi skupiają się również na dynamicznie rozwijającym się rynku gier wideo. Pracujemy także z międzynarodowymi i polskimi firmami z branży telekomunikacyjnej, świadcząc usługi doradcze związane z różnymi aspektami ich obecności na rynku, m.in. rozwiązywaniem sporów regulacyjnych, negocjacjami i przygotowaniem umów operatorskich, dystrybucyjnych i innych. Praktyka IP&TMT otrzymała rekomendacje Media Law International oraz dziennika Rzeczpospolita, zostaliśmy również wyróżnieni w rankingu WTR 1000 2015.

Zespół ds. Ochrony Danych Osobowych

Zespół doradza wiodącym krajowym i zagranicznym przedsiębiorstwom działającym w sektorach: bankowym i finansowym, motoryzacyjnym, farmaceutycznym, sprzedaży wysyłkowej, FMCG, turystyki i hotelarstwa, energetycznym i paliwowym, reklamowym i public relations. Nasi eksperci posiadają wieloletnie doświadczenie, zdobywane od chwili wdrożenia regulacji dotyczących ochrony danych osobowych w Polsce. Prawnicy systematycznie monitorują ustawodawstwo i rozwijające się praktyki w Polsce, Unii Europejskiej i krajach spoza UE. Biorą też udział w tworzeniu dobrych praktyk w zakresie

ochrony danych oraz uczestniczą w debacie publicznej nad ochroną danych osobowych w Polsce. Oferujemy kompleksowe doradztwo w zakresie wdrażania rozwiązań Ochrony Danych Osobowych oraz prowadzenie postępowań przed GIODO, WSA i NSA, a także zajmujemy się zleceniami typu compliance (zapewnienie zgodności dokumentów o międzynarodowym zakresie obowiązywania z przepisami polskimi i unijnymi).

Interdyscyplinarny Zespół Compliance

Każdy z obszarów działalności przedsiębiorstwa jest obarczony ryzykiem braku zgodności. W związku z tym przedsiębiorcy zwracają coraz większą uwagę na budowanie skutecznych systemów compliance. Naszym klientom oferujemy doradztwo w ramach aż 12 specjalizacji prawa dla firm reprezentujących większość branż. W zakres naszego doradztwa wchodzą m.in. analiza compliance – identyfikacja ryzyk, zdefiniowanie środków zaradczych, poprawa środowiska etycznego w organizacji; budowa systemów compliance – wdrażanie nowych systemów, aktualizacja i uzupełnienie procedur wewnętrznych; edukacja i prewencja oraz prowadzenie postępowań karnych i administracyjnych m.in. w zakresie: korupcji gospodarczej lub urzędniczej, ustawiania przetargów publicznych, prania brudnych pieniędzy, odpowiedzialności za naruszenie zasad prawa antymonopolowego.

White-collar crimes, czyli przestępstwa „białych kołnierzyków"

Od wielu lat doradzamy w sytuacjach kryzysowych w zakresie ograniczenia ryzyka przestępstw gospodarczych, m.in.: nadużyć gospodarczych i finansowych, nieuczciwości pracowników, osób zarządzających i współpracowników firmy, odpowiedzialności karnej członków organów spółek kapitałowych, problemów związanych z nierzetelnym prowadzeniem dokumentacji, przypadków nadużycia zaufania i konfliktu interesów, korupcji gospodarczej i urzędniczej, przeciwdziałaniu praniu brudnych pieniędzy.

Compliance w ochronie zdrowia

Tworzymy największy i najbardziej wszechstronny zespół doradców dla sektora ochrony zdrowia w Polsce. Zapewniamy kompleksową obsługę podmiotów wykonujących działalność leczniczą, a także firm zewnętrznych bezpośrednio lub pośrednio zaangażowanych w tą działalność. W skład zespołu wchodzą prawnicy, ekonomiści, lekarze, a także eksperci z zakresu ekonomiki ochrony zdrowia. W ramach usług compliance w ochronie zdrowia przeprowadzamy audyty placówek medycznych, przygotowujemy standardowe procedury działania placówek medycznych – SOP's, szkolimy lekarzy i pielęgniarki (m.in. w zakresie błędów w sztuce, zapobieganie korupcji, preskrypcji produktów refundowanych).

DZP

Domański Zakrzewski Palinka sp.k.

Rondo ONZ 1 | 00-124 Warszawa
T: +48 22 557 76 00
F: +48 22 557 76 01

ul. Paderewskiego 8 | 61-770 Poznań
T: +48 61 642 49 00
F: +48 61 642 49 50

ul. Gwiaździsta 66 | 53-413 Wrocław
T: +48 71 712 47 00
F: +48 71 712 47 50

www.dzp.pl