POLSKA AKADEMIA NAUK
INSTYTUT NAUK PRAWNYCH

PL ISSN 0039-3312

Studia
PRAWNICZE

Zeszyt 2 (210) 2017
Warszawa 2017

Marcin Rojszczak ■

OCHRONA TAJEMNICY ADWOKACKIEJ A USŁUGI ŚWIADCZONE W CHMURZE OBLICZENIOWEJ

Wprowadzenie[1]

Wykonywanie zawodów prawniczych nierozerwalnie wiąże się z obowiązkiem dochowania tajemnicy zawodowej. W szczególności praca adwokata i radcy prawnego, polegająca na świadczeniu pomocy prawnej, wiąże się z podwyższonymi standardami w zakresie ochrony powierzonych informacji.

Podstawę prawną zachowania tajemnicy przez członków korporacji adwokackiej (a więc adwokatów i aplikantów adwokackich) stanowi art. 6 ustawy – Prawo o adwokaturze, zgodnie z którym adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej (art. 6 ust. 1), a obowiązek ten nie może być ograniczony w czasie (art. 6 ust. 2). Dalsze uszczegółowienie zakresu przedmiotowego tajemnicy adwokackiej znalazło rozwinięcie w przepisach Zbioru Zasad Etyki Adwokackiej i Godności Zawodu (dalej: Kodeks), zgodnie z którymi tajemnicą objęte są także wszystkie wiadomości, notatki i dokumenty dotyczące sprawy uzyskane od klienta oraz innych osób, niezależnie od miejsca, w którym się znajdują (§ 19 ust. 3). Należy przy tym zaznaczyć, że zgodnie z wyrokiem NSA z dn. 21 września 1998 roku[2], tajemnicą adwokacką nie są objęte dane personalne klienta

[1] Stan prawny na dzień 1.02.2017; poprawność odnośników internetowych zweryfikowana 25.08.2017.

[2] Wyrok Naczelnego Sądu Administracyjnego z dn. 21 września 1998, sygn. akt: I SA/Ka 2214–2223/96.

i ogólna informacja (wiedza) o rodzaju świadczonej na jego rzecz usługi prawnej. W literaturze przedmiotu wskazuje się ponadto, że konsekwencją nieograniczonego w czasie charakteru tajemnicy adwokackiej jest także uznanie za niedopuszczalne powierzenie archiwizacji dokumentów zewnętrznym wyspecjalizowanym firmom zajmującym się przechowywaniem danych[3].

Adwokat korzystający w pracy zawodowej z komputera lub środków elektronicznego utrwalania danych obowiązany jest przy tym stosować oprogramowanie i inne techniki zabezpieczające dane przed ich niepowołanym ujawnieniem (art. 19 ust. 5 Kodeksu). W przypadku przekazywania informacji objętych tajemnicą zawodową za pomocą elektronicznych środków przekazu wymaga się przy tym zachowania ostrożności i uprzedzenia klienta o ryzykach związanych z zachowaniem poufności przy wykorzystaniu tych środków (art. 19 ust. 6 Kodeksu).

Warto w tym miejscu zaznaczyć, że co do zasady powiadomienie czy nawet uzyskanie zgody klienta w zakresie korzystania z elektronicznych kanałów komunikacji nie ogranicza ani nie zwalnia z odpowiedzialności adwokata za zachowanie tajemnicy zawodowej. Z obowiązku zachowania tajemnicy nie może zwolnić adwokata nawet osoba, której świadczona jest pomoc prawna. Jak słusznie wskazał Sąd Najwyższy w wyroku z dn. 2 czerwca 2011 r., tajemnica zawodowa adwokata czy radcy prawnego wynika z mocy ustawy i ma na celu ochronę nie tylko interesu prywatnego, lecz chroni również interesy danych samorządów zawodowych, a także ma na względzie dobro wymiaru sprawiedliwości. Z tego względu instytucja ta ma charakter *ius cogens*, a nie *ius dispositivum*[4]. W efekcie adwokat, dobierając środki komunikacji elektronicznej, musi rozważyć ryzyka, jakie się z nimi wiążą, i nie rekomendować technik, które nie gwarantują odpowiedniego poziomu poufności przekazywanej informacji.

Ponieważ przepisy ustawy – Prawo o adwokaturze oraz postanowienia kodeksu korporacyjnego w oczywisty sposób nie wiążą co do obowiązku zachowania tajemnicy inne podmioty, niż członkowie adwokatury, w przepisie § 19 ust. 4 doprecyzowano, że adwokat powinien zobowiązać swoich współpracowników i personel oraz wszelkie osoby zatrudnione przez niego podczas wykonywania działalności zawodowej do przestrzegania obowiązku zachowania tajemnicy zawodowej.

---

[3] J. Kurcek, *Tajemnice zawodów prawniczych. Tajemnica adwokacka*, MOP 2013, Nr 23, s. 1278

[4] Postanowienie Sądu Najwyższego z dn. 2 czerwca 2011 r., sygn. akt: SDI 13/11.

Chmura obliczeniowa

W codziennej praktyce większości kancelarii prawnych powszechnie wykorzystywane są nie tylko komputery, ale także komunikacja za pośrednictwem poczty elektronicznej. Informatyzacja pracy prawnika to trend oczywisty, wynikający nie tylko z powszechnych zmian technologicznych – a co za tym idzie z oczekiwań klientów – ale także ze strategii informatyzacji państwa, której częścią jest także cyfryzacja postępowań sądowych. Adwokaci coraz częściej korzystają także z nowoczesnych usług udostępnianych w formie tzw. chmury obliczeniowej.

Przed dalszymi rozważaniami na temat ochrony tajemnicy adwokackiej, konieczne jest odpowiednie zdefiniowanie i przedstawienie modelu funkcjonowania chmury obliczeniowej. Zgodnie z najczęściej przywoływaną w literaturze przedmiotu definicją, wprowadzoną przez amerykański NIST, chmurę obliczeniową można określić jako sposób dostępu poprzez sieć komputerową do współdzielonych i łatwo konfigurowalnych zasobów obliczeniowych (sieci, serwerów, aplikacji czy usług), które na żądanie, dynamicznie mogą być przydzielane i zwalniane, przy równoczesnym minimalnym zaangażowaniu serwisów technicznych[5]. Chmura obliczeniowa jest więc sposobem udostępniania zasobów informatycznych jej użytkownikom.

Rozmawiając o usługach udostępnianych w chmurze obliczeniowej, należy zrozumieć, że termin ten jest wykorzystywany do opisywania całego zbioru technik i technologii. W szczególności wyróżnić można trzy podstawowe modele udostępniania usług za pomocą chmury obliczeniowej[6]:

- *Software as a Service* (SaaS) – w którym użytkownik otrzymuje dostęp do gotowej usługi, uruchomionej i działającej w oparciu o infrastrukturę sprzętowo-programową usługodawcy; w takim przypadku usługobiorca korzysta z udostępnionej mu usługi, a więc funkcjonalności systemu informatycznego na warunkach i w zakresie wynikającym z zaakceptowanego regulaminu,
- *Platform as a Service* (PaaS) – w którym przedmiotem świadczenia usługi jest udostępnienie platformy informatycznej usługodawcy, z wykorzystaniem której klient może tworzyć, rozwijać i eksploatować własne programy użytkowe,

[5] P. Czerwonka, T. Lech, G. Podgórski, *Chmura obliczeniowa*, Acta Universitatis Lodziensis, Folia Oeconomica nr 261/2011.

[6] P . Mell, T . Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Special Publication 800–145, wrzesień 2011.

– *Infrastructure as a Service* (IaaS) – w której użytkownik otrzymuje dostęp do środowiska IT usługodawcy, oferującego uzgodnione wcześniej parametry przetwarzania (np. moc obliczeniową, przepustowość łączy sieciowych, powierzchnię dyskową, ale także np. gwarantowane wskaźniki dostępności itp.).

Ponadto usługi świadczone w modelu chmury obliczeniowej mogą być udostępnione w kilku modelach eksploatacyjnych, z których dwa najważniejsze to chmura prywatna (*private cloud*) oraz chmura publiczna (*public cloud*). W pierwszym podejściu chmura obliczeniowa jest projektowana i eksploatowana przez jeden podmiot na wyłączność. W takim przypadku najczęściej wszystkie elementy implementacyjne rozwiązania (konfiguracja środowiska IT, jego wydajność, ale także lokalizacja geograficzna) jest szczegółowo uzgadniana pomiędzy usługodawcą i usługobiorcą. Rozwiązanie to, ze względu na swoje koszty, znajduje praktyczne zastosowanie do obsługi dużych podmiotów, często korporacji międzynarodowych. Dużo częstszym rozwiązaniem jest korzystanie z chmury publicznej, za pomocą której świadczone są stypizowane usługi dla określonego kręgu odbiorców, zazwyczaj przez publiczną sieć Internet.

Podkreślić należy, że w każdym ze wskazanych wyżej modeli usługowych, użytkownik korzysta z zasobów udostępnionych przez usługodawcę. Fundamentem przetwarzania w chmurze jest przetwarzanie rozproszone, w którym użytkownik nie wie i nie musi wiedzieć ,na jakich konkretnie elementach infrastruktury IT usługodawcy (procesorach, macierzach dyskowych itp.) przetwarzane są jego informacje. Co więcej, normą jest świadczenie tego typu usług z wykorzystaniem zasobów zlokalizowanych w wielu rozproszonych geograficznie centrach przetwarzania. W rezultacie użytkownik korzystający kilkukrotnie z tej samej usługi (np. poczty elektronicznej Google Gmail), może za każdym razem być obsługiwany przez inny serwer zlokalizowany w innym centrum przetwarzania danych, które znajduje się w innym kraju, a nawet na innym kontynencie. Analogicznie, dane użytkownika mogą być automatycznie przenoszone pomiędzy różnymi macierzami dyskowymi, a nawet różnymi centrami przetwarzania danych, aby zoptymalizować użycie całej infrastruktury lub uniknąć problemów wydajnościowych. Co więcej, operatorzy chmur publicznych często rezerwują sobie prawo do korzystania z podwykonawców w celu zapewnienia potrzebnej infrastruktury IT.

Dalsze rozważania na temat zachowania tajemnicy zawodowej w usługach świadczonych z wykorzystaniem chmury obliczeniowej zostaną skoncentrowane na usługach SaaS świadczonych w chmurze publicznej. Do usług tego typu można zaliczyć popularne serwisy poczty elektronicznej (np. Google Gmail, Yahoo Mail czy Microsoft Outlook Web Access), usługi aplikacji

biurowych (np. Microsoft Office 365 czy Google Apps), czy usługi przechowywania i udostępniania plików (np. Dropbox, Google Drive, Microsoft OneDrive). Jest to bez wątpienia przypadek najbardziej częsty, a w efekcie mający największe znaczenie praktyczne.

Dane prawników w chmurze obliczeniowej

Korzystanie z usług świadczonych w chmurze obliczeniowej stało się przedmiotem licznych analiz, z których wiele jest ukierunkowanych na zbadanie technicznych lub ekonomicznych korzyści związanych z nowym modelem przetwarzania danych. W przypadku usług prawniczych, korzystanie z chmury obliczeniowej wiąże się także z fundamentalnymi kwestiami prawnymi, takimi jak zakres i skuteczność prawa do obrony czy kwestia ochrony praw podstawowych w cyfrowym świecie.

Rada Adwokatur i Stowarzyszeń Prawniczych Europy (CCBE) w 2012 roku wydała wytyczne związane z używaniem usług świadczonych w chmurze obliczeniowej przez prawników[7]. W dokumencie nakreślono najważniejsze ryzyka i obszary wymagające indywidualnej weryfikacji, przed podjęciem decyzji o przeniesieniu danych do chmury obliczeniowej. W pierwszej kolejności podkreślono znaczenie wyboru prawa właściwego oraz jurysdykcji obejmującej podmiot świadczący usługi – co jest szczególnie istotne, ponieważ przepisy prawne związane z prywatnością i dostępem do danych stanowiących tajemnicę zawodową różnią się pomiędzy poszczególnymi krajami, zwłaszcza poza obszarem EOG.

Z uwagi na znaczenie firm amerykańskich dla globalnego rynku przetwarzania danych w chmurze, szczególną uwagę należy zwrócić tamtejszej legislacji. Z uwagi na niejednorodny system prawny obowiązujący w Stanach Zjednoczonych, na wstępie należy zaznaczyć, że kwestia ochrony informacji oraz prawa do prywatności jest w większości przypadków obszarem jurysdykcji prawa federalnego. Jakkolwiek ochrona przed bezzasadnym zatrzymaniem i przeszukaniem jest wartością chronioną konstytucyjnie, wskazać należy na liczne przypadki dowodzące funkcjonowania rozbudowanego systemu inwigilacji obywateli przez władze amerykańskie.

Przykładem mogą być ujawnione przez E. Snowdena informacje o *quazi-legalnym* dostępie przez amerykańskie agencje wywiadowcze do danych przetwarzanych przez firmy amerykańskie (w tym największych na świecie dostawców

[7] Council of Bars and Law Societies of Europe, *CCBE Guidelines on the use of cloud computing services by lawyers*, 7 września 2012.

usług chmurowych – takich jak Google czy Amazon). Informacje te wzbudziły uzasadnione obawy co do wiarygodności Stanów Zjednoczonych jako odpowiedzialnego partnera w zakresie ochrony danych osobowych i stały się podstawą do wydania przez Trybunał Sprawiedliwości UE wyroku w sprawie C-362/14, którego konsekwencją było czasowe wstrzymanie transgranicznego przepływu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych[8].

W swojej analizie CCBE wskazuje ponadto na listę elementów, które powinny zostać uwzględnione w umowie z operatorem usługi świadczonej w *cloud computingu* w wykonaniu której przetwarzane będą informacje stanowiące tajemnicę zawodu prawniczego. Poza kwestią wskazania prawa i sądu właściwego do rozstrzygania sporów, w umowie określone powinny zostać między innymi[9]: kwestia własności danych oraz wyłącznego dostępu do nich, zakaz korzystania z podwykonawców bez uzyskania wcześniejszej zgody usługobiorcy, miejsce fizycznej lokalizacji serwerów, prawo do kontroli i audytu przestrzegania zapisów umownych, zasady przetwarzania danych osobowych zgodne z krajowymi wymaganiami obowiązującymi usługobiorcę, kary umowne oraz zakres odpowiedzialności usługodawcy w przypadku naruszenia poufności informacji.

Problem wyboru odpowiedniej jurysdykcji może jednak występować także w obszarze UE oraz EOG. Należy pamiętać, że chociaż państwa Wspólnoty wypracowały wspólne podstawy prawne w zakresie ochrony praw podstawowych, do których należą także dane osobowe, pomiędzy systemami prawnymi istnieją znaczące różnice w zakresie zakresu i granic tajemnic zawodowych, takich jak tajemnica adwokacka. Pomocne w ocenie ryzyk oraz podjęciu decyzji w zakresie skorzystania z konkretnego dostawcy *cloud computingu* może być opublikowana w kwietniu 2014 przez CCBE analiza dotycząca prawnych ram ochrony tajemnicy zawodowej prawników w poszczególnych krajach UE[10]. Jednym z badanych obszarów była ochrona danych przetwarzanych w chmurze, ze szczególnym uwzględnieniem możliwości uzyskania przez władze lub organy ścigania informacji objętych tajemnicą zawodową poprzez zobowiązanie dostawcy usług do ich ujawnienia. Na 18 badanych systemów prawnych, według udzielonych informacji tylko w jednym przypadku – Szwecji – istnieją przepisy, które wymagają przekazania takiego żądania do właściciela informacji, w analizowanym przypadku prawnika – który może odmówić ujawnienia informacji na podstawie przepisów o tajemnicy zawodowej. We wszystkich pozostałych krajach (także

[8] Wyrok Trybunału Sprawiedliwości UE z dn. 6 października 2015, sygn. akt: C–362/14.

[9] Council of Bars and Law Societies of Europe, *CCBE Guidelines*, op. cit., s. 8.

[10] Council of Bars and Law Societies of Europe, *CCBE Comparative Study on Governmental Surveillance of Lawyers' Data in the Cloud*, 04 kwietnia 2014

w Polsce) istniejące prawo nie określa odmiennego statusu firm świadczących usługi *cloud computingu*, w szczególności nie precyzuje, że firmy te nie są właścicielami danych, które przetwarzają i nie powinny być zmuszane do ujawniania/przekazywania tych danych bez zgody czy nawet wiedzy właściciela. CCBE zbadało także, czy dostawcy usług mogą dobrowolnie, bez otrzymania żądania w tym zakresie, ujawnić dane klientów organom ścigania oraz czy w przypadku konieczności ujawnienia informacji (otrzymania skutecznego żądania wydanego w oparciu o przepisy obowiązujące w danym państwie członkowskim), dostawca usług musi poinformować o tym fakcie prawnika, którego dane ujawnia. W każdym z badanych obszarów ujawnione zostały różnice w legislacji poszczególnych państw UE.

Ochrona komunikacji pomiędzy prawnikiem a klientem była także przedmiotem precedensowego wyroku Trybunału Sprawiedliwości w sprawie AM&S Europe przeciwko Komisji, w której Trybunał uznał, że tajemnica komunikacji między adwokatem i jego klientem powinna być chroniona na podstawie prawa Unii w zakresie, w jakim spełnione są dwie przesłanki wskazane w pkt 21 tego wyroku – tj. związana jest z realizacją prawa do obrony oraz jest prowadzona przez adwokata nie będącego pracownikiem klienta[11]. Kwestia ochrony komunikacji prawników świadczących pomoc prawną swoim pracodawcom (tzw. *in-house*) była ponownie przedmiotem analizy w 2010 roku, w wyniku której Trybunał uznał, że sytuacja prawna w państwach członkowskich Unii Europejskiej nie zmieniła się na przestrzeni lat, które upłynęły od wydania wyroku w sprawie AM&S Europe przeciwko Komisji, w zakresie uzasadniającym rozwój orzecznictwa w kierunku przyznania adwokatom wewnętrznym przywileju ochrony tajemnicy w komunikacji z klientem będącym ich pracodawcą[12].

Kancelaria Hogan Lowells w 2012 roku przygotowała podobne do CCBE opracowanie w odniesieniu do Stanów Zjednoczonych i 7 wybranych krajów Ameryki Środkowej i Południowej[13]. Jednakże w tym wypadku celem było przeanalizowanie uprawnień rządu w dostępie do dowolnych danych przetwarzanych w chmurze obliczeniowej – niekoniecznie związanych z wykonywaniem zawodów prawniczych. Jeden z najważniejszych wniosków przedstawionych w raporcie dotyczy wskazania, że w przypadku dostępu agencji rządowych do danych przechowywanych w chmurze istotna nie jest lokalizacja geograficzna serwerów, ale prawo właściwe dla firmy, która jest operatorem usługi świadczonej

[11] Wyrok Trybunału Sprawiedliwości UE z dn. 18 maja 1982, sygn. akt: 155/79

[12] Wyrok Trybunału Sprawiedliwości UE z dn. 14 września 2010, sygn. akt: C–550/07.

[13] C . Wolf, B. Cohen , *Pan-American Governmental Access to Data in the Cloud*, Hogan Lowells White Paper 2014.

z ich wykorzystaniem. Jak wykazano w analizie Hogan Lowells, w przypadku większości z badanych systemów prawnych (w tym Stanów Zjednoczonych, Brazylii czy Meksyku), usługodawcy mogą zostać zobowiązani do ujawnienia danych swoich klientów, także przetwarzanych w innym kraju.

W chwili obecnej, z uwagi na brak szczegółowych regulacji nie tylko na poziomie krajowym, ale także europejskim, skuteczność ochrony danych objętych tajemnicą zawodów prawniczych zależy w dużej mierze od świadomości prawnej pracowników firmy przetwarzającej dane, a także szczegółowych zapisów w umowie regulujących zasady korzystania z usług. Bez wątpienia, niezależnie od rozważenia innych ryzyk, prawnik decydujący się na korzystnie z usług *cloud computingu* powinien przeanalizować gwarancje związane z ochroną tajemnicy zawodowej w jurysdykcji właściwej dla zawartej umowy oraz zadbać, aby w jej zapisach uwzględnić jasną deklarację, że usługa będzie wykorzystywana do przetwarzania informacji stanowiących tajemnicę zawodową.

Ochrona danych osobowych i przekazywanie danych do państwa trzeciego

Należy zwrócić uwagę, że obszarem nierozerwalnie związanym z tajemnicą adwokacką jest także ochrona danych osobowych. Z uwagi na specyfikę pracy adwokata, świadczącego profesjonalną pomoc prawną, dbałość o ochronę informacji dotyczących jego klientów, ale także danych osobowych powierzonych przez klientów czy innych uczestników postępowania wymaga odpowiedniego zrozumienia i stosowania przepisów o ochronie danych osobowych. W szczególności bez trudu można wykazać, że w przypadku niedochowania przez adwokata zobowiązań wynikających z przepisów o ochronie danych osobowych naruszenie tajemnicy zawodowej jest oczywiste.

Problem ten dodatkowo zyskuje na znaczeniu wobec niedawnych doniesień w zakresie kontroli zapowiedzianych przez GIODO w zakresie przestrzegania przepisów związanych z ochroną danych osobowych przez kancelarie prawne z uwzględnieniem zagadnień związanych z przechowywaniem danych w chmurze obliczeniowej[14].

Zgodnie z art. 3 ust. 2 ustawy o ochronie danych osobowych (dalej: uodo), przepisy ustawy stosuje się do osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane

[14] „*NRA uprzedza o kontrolach GIODO*", http://www.prawnik.pl/wiadomosci/adwokaci/artykuly/994314,nra-uprzedza-o-kontrolach-giodo.html

osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Bez wątpienia zatem zakresem podmiotowym regulacji objęte są kancelarie adwokackie (łącznik działalności zarobkowej oraz zawodowej), które zgodnie z terminologią przyjętą w ustawie należy uznać za administratorów danych – a więc podmioty decydujące o celach i środkach przetwarzania danych osobowych.

Warto w tym momencie zwrócić uwagę na przepis art. 43 ust. 1 pkt 5 uodo, zgodnie z którym administratorzy danych zwolnieni są z obowiązku rejestracji zbioru danych dotyczących osób korzystających z obsługi adwokackiej. Przepis ten wyłącza zatem obowiązek rejestracji zbioru danych osobowych, o którym mowa w art. 40, w zakresie zbioru danych klientów kancelarii. Nie wyłącza jednak co do zasady obowiązku stosowania szczegółowych rozwiązań przewidzianych w ustawie do ochrony tego zbioru, w szczególności konieczności opracowania i wdrożenia polityki bezpieczeństwa, nadania upoważnień osobom dopuszczonym do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych.

Przepisy ustawy w art. 27 ust. 1 wprowadzają ponadto odrębną definicję tzw. danych wrażliwych – do których zaliczone zostają m.in. informacje dotyczące stanu zdrowia, nałogach lub życiu seksualnym oraz dane związane ze skazaniami, orzeczeniami o ukaraniu i mandatach karnych, a także związane z innymi orzeczeniami wydanymi w postępowaniu sądowym lub administracyjnym. Nierzadko zatem teczki prowadzonych spraw w kancelarii prawnej będą zawierały dane osobowe szczególnie wrażliwe. W tym miejscu warto zauważyć, że chociaż przepis art. 27 ust. 1 uodo wprowadza ogólny zakaz przetwarzania takich informacji, to zgodnie z art. 27 ust. 2 pkt 5 uodo przetwarzanie to jest dopuszczalne, jeżeli dotyczy danych, które są niezbędne do dochodzenia praw przed sądem. Jak wskazał WSA w Warszawie w wyroku z dn. 5 sierpnia 2005 roku, w przypadku udostępniania przez adwokata informacji stanowiących dane wrażliwe w celu przygotowania pozaprocesowej opinii nie dochodzi do naruszenia przepisów ustawy o ochrony danych osobowych, bowiem czynność taka służy realizacji prawa do obrony osoby oskarżonej w postępowaniu sądowym i znajduje swoje oparcie w przepisie art. 27 ust. 2 pkt 5 ustawy o ochronie danych osobowych. Sąd ponadto podkreślił, że obowiązek zachowania przez adwokata tajemnicy zawodowej nie oznacza, iż adwokat będący obrońcą w procesie karnym, nie jest uprawniony i zobowiązany do podejmowania działań mających na celu obronę oskarżonego[15]. Należy jednak zauważyć, że o ile udostępnienie

[15] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dn. 5 sierpnia 2005, sygn. akt: II SA/Wa 564/05.

danych osobowych – w tym danych wrażliwych – innym uczestnikom postępowania znajduje oparcie w obowiązujących przepisach, to już sposób udostępnienia tych informacji powinien zostać przeprowadzony zgodnie z reżimem ustawy. W szczególności skorzystanie ze środków komunikacji elektronicznej (np. poczty elektronicznej lub usługi przechowywania i udostępniania plików) oznacza, że dane te są przetwarzane nie tylko przez uprawnionego uczestnika postępowania – ale również przez usługodawcę internetowego.

Zgodnie z art. 31 uodo administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Zgodnie z definicją przedstawioną w ustawie, przetwarzaniem danych jest także ich przechowywanie – zwłaszcza, jeżeli wykorzystuje się do tego systemy informatyczne. Nie ma zatem wątpliwości, że skorzystanie przez administratora danych z usługi informatycznej, która wiąże się z przechowywaniem informacji zawierających dane osobowe w systemach informatycznych usługodawcy – jest w świetle przepisów ustawy powierzeniem przetwarzania danych osobowych.

W literaturze przedmiotu wskazuje się, że umowa o powierzenie przetwarzania danych osobowych najczęściej będzie miała postać umowy o świadczenie usług, do której na podstawie art. 750 kc stosuje się przepisy o zleceniu[16]. Brak zachowania formy pisemnej nie będzie wywierał skutku nieważności umowy (art. 73 § 1 kc). Usługi związane z przetwarzaniem danych w chmurze obliczeniowej najczęściej są zawierane na odległość, bez fizycznej obecności obu stron – często z wykorzystaniem gotowych wzorców umów i regulaminów, które są akceptowane przez użytkownika podczas rejestracji usługi. W takim wypadku praktyczne zastosowanie mogą znaleźć znowelizowane przepisy Kodeksu cywilnego, wprowadzające od 8 września 2016 do porządku prawnego formę dokumentowej czynności prawnej. Zgodnie z art. 77^2 kc, do jej zachowania wystarczy złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie, przy czym dokumentem może być także nośnik informacji umożliwiający zapoznanie się z jej treścią (art. 77^3 kc). Zaktualizowane przepisy cały czas wymagają w celu zachowania elektronicznej formy czynności prawnej opatrzenia oświadczenia woli kwalifikowanym podpisem elektronicznym – co w przypadku usług świadczonych w chmurze jest rozwiązaniem niespotykanym. Należy jednak zwrócić uwagę, że zachowanie formy dokumentowej nie jest równoważne zachowaniu formy pisemnej (por. art. 78^1 ust. 2 kc) – a na taką wskazuje wprost aktualna redakcja art. 31 uodo. Nie zasługuje przy tym na aprobatę pogląd wyrażony przez P. Barta, jakoby zawarcie

[16] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, art. 31, Wydanie 4, C. H. Beck 2016.

umowy powierzenia przetwarzania danych osobowych w formie dokumentowej było dopuszczalne już w obecnym reżimie prawnym, w związku z czym nowelizacja art. 31 nie jest konieczna[17]. P. Barta dokonuje błędnego podziału formy pisemnej na dokumentową oraz elektroniczną, podczas gdy oczywistym zamiarem ustawodawcy było dodanie nowej – obok istniejących wcześniej – formy szczególnej składania oświadczeń woli[18].

W piśmiennictwie wskazuje się na niewielkie praktyczne zastosowanie formy dokumentowej w obecnym kształcie przepisów prawa cywilnego[19]. Podnosi się także argument, że wprowadzanie oddzielnej formy czynności prawnej nie znajduje uzasadnienia w sytuacji, gdy to od woli stron zależy, jaki sposób wyrażenia woli uznają za wystarczający w łączącym je stosunku (swoboda formy)[20]. Należy jednak podkreślić, że obszar przetwarzania danych osobowych jest dobrym przykładem możliwości praktycznego zastosowania nowych przepisów. Zasada swobody formy nie może mieć bowiem zastosowania w sytuacji, gdy przepis szczegółowy wiąże określone skutki z zachowaniem odpowiedniej formy. Natomiast skutki zawarcia umowy o powierzenie przetwarzania danych osobowych obejmują nie tylko jej strony, ale także – a może przede wszystkim – osoby, których dane będą przetwarzane w wyniku wykonania umowy. Dlatego, z punktu widzenia administratora danych oraz określenia granic jego odpowiedzialności za ew. naruszenia przepisów o ochronie danych osobowych, szczególnie ważne wydaje się dochowanie reżimowi zawarcia umowy powierzenia w sposób nie budzący wątpliwości interpretacyjnych.

Przepisy ustawy co do zasady przypisują odpowiedzialność za zgodne z ustawą przetwarzanie informacji administratorowi danych, także w przypadku gdy dane zostały powierzone do przetwarzania podmiotowi zewnętrznemu. Z uwagi na niewystarczająco precyzyjną redakcję przepisów art. 31 ust. 3 i 4 uodo, w doktrynie trwa dyskusja na temat zakresu tej odpowiedzialności w odniesieniu do działań podmiotu zewnętrznego[21]. W szczególności art. 31 ust. 4 uodo stanowi, że odpowiedzialność za przestrzeganie przepisów ustawy

---

[17] Komentarz do art. 31, Nb 9 [w:] **P. Barta, L. Litwiński,** *Ustawa o ochronie danych osobowych. Komentarz*, wyd. 4, Warszawa 2016.

[18] Por. uzasadnienie do projektu ustawy o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (druk 2678), pkt II.2.

[19] J. **Grykiel,** *Kilka uwag o nowej definicji dokumentu i formie dokumentowej,* MOP 5/2016

[20] Por. komentarz do art. 77^2, Nb 2 [w:] **M. Gutowski, (red.),** *Kodeks cywilny. Tom I. Komentarz. Art. 1–449^{11}*, Warszawa 2016.

[21] Por. rozważania na tle art. 31 uodo w: **P. Barta, P. Litwiński, Us***tawa o ochronie danych osobowych. Komentarz,* wyd. 4, C. H. Beck 2016

spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niegodnie z umową. Jak wskazał jednak Sąd Apelacyjny w Warszawie w wyroku z dn. 23 września 2015, w cytowanym przepisie nie chodzi o odpowiedzialność cywilną, ale o odpowiedzialność w zakresie wypełnienia obowiązków ustawy przed Generalnym Inspektorem Ochrony Danych Osobowych[22]. Natomiast do rozstrzygnięcia zakresu odpowiedzialności administratora danych za szkodę wyrządzoną osobie trzeciej przez podmiot przetwarzający dane na zlecenie należy posłużyć się normą przewidzianą w art. 429 kc.

Dotrzymanie rygorów ustawy w zakresie powierzenia przetwarzania danych osobowych to nie jedyny obowiązek ciążący na administratorze danych, który chce przetwarzać informacje z wykorzystaniem usług dostępnych w chmurze obliczeniowej. W praktyce dużo większe problemy mogą wiązać się z faktem przetwarzania informacji za granicą, a często także braku możliwości dokładnego wskazania, gdzie dokładnie dane są przetwarzane. Najwięksi dostawcy usług *cloud computingu* dysponują kilkunastoma centrami przetwarzania danych rozlokowanymi na całym świecie.

Ustawa o ochronie danych osobowych szczegółowo reguluje warunki i tryb, w jakim dane osobowe mogą zostać przekazane do państwa trzeciego. W dalszych rozważaniach pod pojęciem państwa trzeciego będzie rozumiany kraj nie należący do Unii Europejskiej ani nie będący stroną umowy o Europejskim Obszarze Gospodarczym. Podstawową regulację w tym zakresie stanowi art. 47 ust. 1, zgodnie z którym przekazanie danych może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych – przy czym odpowiedni poziom jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe. W zakresie transgranicznego przepływu danych krajowa ustawa o ochronie danych osobowych implementuje przepisy unijnej dyrektywy 95/46 z 1995 roku[23].

W praktyce obecne regulacje przewidują trzy najważniejsze tryby, w jakich dane mogą zostać przekazane do państwa trzeciego:

[22] Wyrok Sądu Apelacyjnego w Warszawie z dn. 23 września 2015 r., sygn. akt: VI ACa 1357/14 05.

[23] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dn. 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz.UE.L Nr 281, s. 31)

- bez indywidualnej decyzji GIODO, jeżeli przekazanie następuje do państwa, które zostało uznane za spełniające kryteria przewidziane w art. 47 ust. 1 uodo oraz art. 25 dyrektywy 95/46 przez GIODO lub Komisję Europejską,
- bez indywidualnej decyzji GIODO w trybie art. 48 ust. 2 pkt 1 uodo, jeżeli przekazanie następuje do państwa, które nie zostało uznane za spełniające kryteria przewidziane w art. 47 ust. 1 uodo oraz art. 25 dyrektywy 95/46, ale administrator danych zaleci stosowanie adekwatnych zabezpieczeń odnośnie ochrony prywatności oraz podstawowych praw i wolności osoby – poprzez zastosowanie odpowiednich klauzul umownych zatwierdzonych przez Komisję Europejską,
- na podstawie indywidualnej decyzji GIODO wydanej na podstawie art. 48 ust. 1 uodo, jeżeli przekazanie następuje do państwa, które nie zostało uznane za spełniające kryteria przewidziane w art. 47 ust. 1 uodo oraz art. 25 dyrektywy 95/46, a administrator danych nie zawarł z podmiotem przetwarzającym odpowiedniej umowy zgodnej z klauzulami umownymi zatwierdzonymi przez Komisję Europejską.

Pierwszy z przedstawionych trybów przewidziany jest dla sytuacji, w której Komisja Europejska wydała decyzję o adekwatności poziomu ochrony danych osobowych w państwie trzecim do obowiązującego na terytorium UE. Lista takich decyzji jest dostępna publicznie na stronie internetowej Komisji[24]. Według stanu na 31 grudnia 2016 roku wydano 12 tego typu decyzji, w tym dotyczącą USA – będącą konsekwencją zawarcia umowy Tarcza Prywatności. Jeżeli dane osobowe mają być przetwarzane w kraju objętym decyzją Komisji, nie jest konieczne wdrażanie żadnych dodatkowych zabezpieczeń ze strony administratora danych[25]. Pogląd ten jest jednak dyskutowany w literaturze przedmiotu. W szczególności wątpliwości dotyczą pewności, jaką administrator danych może wiązać z procesem tzw. samocertyfikacji, będącej podstawą programu „Tarcza Prywatności" oraz – nieobowiązującego już – programu „Bezpieczna przystań". Jak wskazuje Grupa robocza art. 29, spółki eksportujące dane nie powinny opierać się tylko na deklaracji importera o zgodności z zasadami programu „Bezpieczna przystań"[26]. Powinny natomiast uzyskać dowody, że autocertyfikacja w ramach programu „Bezpieczna przystań" istnieje i domagać się dowodów

[24] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[25] P. Drobek, *Międzynarodowe transfery danych osobowych w świetle praktyki Generalnego Inspektora Ochrony Danych Osobowych – zagadnienia wybrane*, MOP 8/2013.

[26] Grupa Robocza art. 29 ds. Ochrony Danych, „*Opinia 05/2012 na temat przetwarzania danych w chmurze obliczeniowej*", rozdział 3.5.1.

wykazujących, że przestrzegane są jej zasady. Chociaż pogląd ten został wyrażony w odniesieniu do programu „Bezpieczna przystań, schemat autocertyfikacji pozostał niezmieniony także obecnie i stanowi podstawę programu „Tarcza prywatności". Dlatego należy uznać że rekomendacja ta pozostaje nadal aktualna i ma zastosowanie w sytuacji eksportu danych osobowych do Stanów Zjednoczonych. Dalej idący pogląd – wprowadzający możliwość podważenia na drodze sądowej przez krajowy organ ochrony danych osobowych każdej decyzji o adekwatności zabezpieczeń wydanej przez KE – został wyrażony przez Trybunał Sprawiedliwości UE w sprawie C-362/14[27].

Wydanie decyzji Komisji o adekwatności poziomu ochrony nie wyłącza konieczności wdrożenia pozostałych przepisów prawnych związanych z ochroną danych osobowych – w szczególności zawarcia umowy o powierzenie przetwarzania danych osobowych. Podkreślić należy, że umowa o powierzenie przewarzania danych osobowych powinna być zawarta w każdym przypadku, gdy administrator danych zleca przetwarzanie informacji podmiotowi zewnętrznemu, niezależnie czy jest to podmiot krajowy, posiadający siedzibę w państwie członkowskim UE lub stronie układu EOG, czy będący państwem trzecim[28].

W przypadku drugiego z przedstawionych trybów, tj. zastosowania tzw. klauzul umownych, konieczne jest zawarcie dodatkowej umowy z podmiotem przetwarzającym, nazywanej w literaturze przedmiotu umową transferową[29]. Administrator danych powinien w tym celu skorzystać z jednego z zatwierdzonych przez Komisję Europejską wzorców umownych. Do chwili obecnej Komisja przyjęła trzy takie wzorce – dwa przeznaczone dla sformalizowania relacji pomiędzy administratorem danych a zagranicznym kontrolerem (decyzje Komisji Europejskiej 2001/497/EC oraz 2004/915/EC) oraz jeden zawierający klauzule umowne do kontraktu pomiędzy administratorem danych a zagranicznym procesorem (decyzja Komisji Europejskiej 2010/87/EU). W prawie unijnym pod pojęciem kontrolera należy rozumieć podmiot przetwarzający dane i kontrolujący sposób ich przetwarzania (np. podejmujący decyzję co do wykorzystanych środków przetwarzania, celów przetwarzania, retencji danych itp.). Natomiast pod pojęciem procesora należy rozumieć podmiot, który przetwarza dane na zlecenie, ale nie decydujący o sposobie czy zakresie przetwarzania. Zderzając te definicje z wcześniejszymi rozważaniami, należy zauważyć, że w przypadku usług świadczonych w chmurze obliczeniowej zastosowanie powinny znaleźć

[27] Wyrok Trybunału Sprawiedliwości UE z dn. 6 października 2015, sygn. akt: C–362/14.

[28] Por. odpowiedź na pytanie 10 w załączniku II do decyzji KE 2000/520/WE.

[29] D. Karwala, *Wiążące reguły korporacyjne dla przetwarzających dane osobowe (processor binding corporate rules)*, Monitor Prawniczy 13/2014.

klauzule właściwe dla relacji z procesorem informacji, a więc wynikające z decyzji 2010/87/EU. Dlatego, jeżeli administrator danych planuje skorzystać z usług przetwarzania w chmurze, a usługodawca jest podmiotem świadczącym usługi w kraju, co do którego nie wydano decyzji o adekwatności poziomu ochrony, umowa transferowa zawarta pomiędzy stronami powinna zostać uzupełniona o zapisy umowne wynikające z decyzji 2010/87/EU[30].

W praktyce powszechne stosowanie klauzul umownych w odniesieniu do usług świadczonych w chmurze obliczeniowej napotyka na trudność związaną ze wskazaniem prawa właściwego dla umowy transferu. We wszystkich wzorcach przyjętych przez Komisję Europejską wymaga się, aby było to prawo państwa członkowskiego właściwe dla administratora danych.

W decyzjach GIODO podkreśla się, że pomimo zwolnienia administratorów danych stosujących standardowe klauzule umowne z konieczności uzyskania indywidualnej zgody organu nadzoru na przekazanie danych do państwa trzeciego są oni obowiązani spełnić wszystkie wymogi decyzji Komisji oraz ustawy odnoszące się do planowanego transferu danych[31]. W szczególności wypełnienie obowiązków wynikających z art. 47 i 48 uodo nie wyłącza zastosowania w takich wypadkach pozostałych przepisów ustawy, do których przestrzegania zobowiązany jest administrator danych.

W sytuacji, w której transfer danych ma odbyć się do kraju nie objętego decyzją KE o adekwatności poziomu ochrony oraz brak jest możliwości zastosowania standardowych klauzul umownych zatwierdzonych przez Komisję, administrator danych może uzgodnić treść umowy transferu we własnym zakresie i wystąpić do GIODO o wydanie zgody na przekazywanie danych do państwa trzeciego. Należy zauważyć, że zgoda GIODO – wydana w formie decyzji po przeprowadzeniu postępowania administracyjnego – warunkuje rozpoczęcie transferu danych. W szczególności GIODO wielokrotnie podkreślał[32], że wydanie decyzji w przedmiocie wyrażenia zgody na przekazanie danych osobowych do państwa trzeciego nie legalizuje wcześniejszego przekazania danych osobowych do państwa trzeciego, które ewentualnie miałoby miejsce przed datą wydania decyzji w sprawie. Niewątpliwie z uwagi na charakter usług *cloud computingu*, powiązanie rozpoczęcia korzystania z usługi z koniecznością wcześniejszego uzyskania formalnej zgody GIODO jest praktycznie niemożliwe do realizacji.

---

[30] Grupa Robocza art. 29 ds. Ochrony Danych, *Opinia 05/2012 na temat przetwarzania danych w chmurze obliczeniowej, rozdział 3.5.3: Standardowe klauzule umowne.*

[31] Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dn. 13 lutego 2015, sygn. akt: DESiWM/DEC-108/15.

[32] Por. np. decyzja GIODO nr DESiWM/DEC-902/13 z dn. 3 września 2013, nr DESiWM/DEC-1207/14 z dn. 22 grudnia 2014.

Jak wskazano wcześniej, umowy zawierane z usługodawcami mają zazwyczaj postać wzorców akceptowanych elektronicznie w trakcie procesu rejestracji (umowy adhezyjne).

Analiza przypadków

Uzupełniając rozważania teoretyczne związane z formalną stroną powierzenia przetwarzania tajemnic zawodowych oraz danych osobowych, warto przeanalizować regulaminy usług oraz wzorce umowne oferowane przez liderów rynku. W przypadku wyboru firmy krajowej nie powinny występować dwie trudności: inna niż polska jurysdykcja oraz konieczność transferu danych za granicę. Warto jednak zwrócić uwagę, że wiele firm działających w Polsce oferuje swoje usługi przez polskie oddziały lub z wykorzystaniem podwykonawców będących zagranicznymi centrami przetwarzania informacji. Największe polskie firmy hostingowe – tj. spółki AZ.pl Sp. z o.o. (operator serwisu az.pl), nazwa.pl Sp. z o.o. (operator serwisu nazwa.pl) oraz home.pl S.A. (operator serwisu home.pl) zgodnie podkreślają w udostępnionych regulaminach usług, że prawem obowiązującym dla relacji umownych jest prawo polskie. Wszystkie trzy firmy jednocześnie zapewniają, że ich centra przetwarzania danych są zlokalizowane w Polsce, przy czym informacja na ten temat nie wynika wprost z regulaminów, a publikowanych materiałów prasowych[33]. Ponadto spółka Home.pl oferuje możliwość podpisania umowy o powierzenie danych osobowych, której wzór udostępnia na swojej stronie internetowej[34]. Umowa wprost odwołuje się do krajowych przepisów, precyzyjnie wskazując na zobowiązania usługobiorcy związane z wypełnieniem zobowiązań ustawowych.

Sytuacja wygląda odmiennie w przypadku największych globalnych firm dostarczających powszechne usługi SaaS – takie jak poczta elektroniczna czy przechowywanie plików. Klienci usług bezpłatnych, udostępnianych przez firmę Google, takich jak Gmail (poczta elektroniczna) czy Drive (repozytorium plików) są zobowiązani do zaakceptowania dokumentu Warunki świadczenia usług[35], w którym wskazano jako prawo właściwe prawo stanu Kalifornia

[33] Por. np.: komunikat prasowy firmy Nazwa.pl – https://www.nazwa.pl/o-firmie/biuro-prasowe/serwery-nazwapl-w-polcom-data-center/, komunikat prasowy firmy Home.pl: https://home.pl/firma/datacenter

[34] https://pomoc.home.pl/baza-wiedzy/umowa-na-hosting-wirtualny-z-zapisami-giodo/

[35] https://www.google.com/policies/terms/

w Stanach Zjednoczonych. Częścią warunków jest także Polityka prywatności[36], w której z kolei doprecyzowano, że firma Google ma prawo do stosowania mechanizmów automatycznego skanowania danych zamieszczonych przez użytkowników (w tym np. treści wiadomości e-mail) do celów reklamowych. Ponadto operator wprost wskazuje, że przetwarza dane osobowe na serwerach w wielu krajach na całym świecie – przy czym może się to odbywać także poza krajem zamieszkania użytkownika. Przetwarzanie realizowane jest także z wykorzystaniem podmiotów zewnętrznych, nazywanych w dokumencie podmiotami stowarzyszonymi, które zgodnie z definicją zawartą w Polityce są podmiotami należącymi do grupy firm Google. Użytkownik nie jest poinformowany, którym konkretnie podmiotom udostępnione są jego dane, ani w jakich lokalizacjach geograficznych są one przetwarzane. Firma Google rezerwuje sobie także prawo do udostępnienia danych osobowych firmom, organizacjom i osobom trzecim, jeśli w dobrej wierze uzna, że udostępnienie, wykorzystanie, zachowanie lub ujawnienie danych jest uzasadnione. W efekcie nie ma wątpliwości, że warunki te znacząco odbierają od wymaganych przez prawo krajowe i europejskie w odniesieniu do przetwarzania danych osobowych.

Firma Google oferuje także usługi komercyjne pod nazwą Google Apps (dla klientów komercyjnych nazywany także jako G Suite dla Firm), w których te same produkty udostępniane są na odmiennych warunkach handlowych, a także formalno-prawnych. W punkcie 14.10 regulaminu korzystania z usługi G Suite[37] wskazano – podobnie jak w przypadku usług bezpłatnych Google – na jurysdykcję prawa właściwego dla stanu Kalifornia w Stanach Zjednoczonych, wskazując ponadto, że wszelkie spory wynikające z umowy będą rozstrzygane wyłącznie przez sądy hrabstwa Santa Clara w stanie Kalifornia. Użytkownicy G Suite otrzymują jednak możliwość zawarcia załącznika do głównej umowy, regulującego zasady powierzenia przetwarzania danych osobowych[38]. Załącznik ten w punkcie 4 określa jako prawo właściwe w przypadku rozstrzygania sporów dotyczących przetwarzania danych osobowych, prawo właściwe dla państwa członkowskiego usługobiorcy. Treść umowy jest udostępniona online, a jej zawarcie odbywa się poprzez formularz elektroniczny. Taki sposób zawarcia umowy może budzić wątpliwości w zakresie zachowania formy pisemnej, wymaganej art. 31 ust. 1 uodo. Ponadto załącznik wyłącza możliwość przetwarzania danych przez Google w innym celu niż w zakresie określonym przez usługobiorcę (pkt 5.3) oraz zawiera dodatkową gwarancję, że dane udostępnione przez usługobiorcę nie będą przetwarzane do celów reklamowych (pkt 5.4). Firma wskazuje także

[36] https://www.google.com/policies/privacy/
[37] https://gsuite.google.com/intl/pl/terms/2013/1/premier_terms.html
[38] https://gsuite.google.com/terms/dpa_terms.html

listę podwykonawców (firm należących do grupy Google), które mogą wykonywać w jej imieniu umowę[39]. Ponadto Google oferuje zawarcie dodatkowego porozumienia[40] zgodnego ze standardowymi klauzulami umownymi, ustalonymi decyzją Komisji Europejskiej 2010/87/EU. Zgodnie z art. 9 porozumienia, prawem właściwym dla tej umowy jest prawo państwa członkowskiego, w którym zarejestrowany został podmiot przekazujący dane. Podobnie jak aneks dotyczący powierzenia przetwarzania danych osobowych, także to porozumienie jest akceptowane w postaci elektronicznej poprzez zaznaczenie odpowiedniej opcji w serwisie internetowym.

Firma Google informuje, że usługa G Suite umożliwia klientom spełnienie wymagań związanych z ochroną danych zgodnie z przepisami Unii Europejskiej[41]. Niezależnie od tej deklaracji, uzasadnione wątpliwości w stosowaniu usługi G Suite w kancelarii prawnej budzić może brak wpływu usługobiorcy na miejsce przetwarzania informacji (serwerownie Google zlokalizowane są na całym świecie), a także stosowanie prawa stanu Kalifornia w obszarach innych niż regulowane przepisami EU w zakresie danych osobowych. Warto podkreślić, że takim obszarem jest chociażby kwestia ochrony tajemnicy zawodowej.

Problem jurysdykcji kraju nienależącego do Unii Europejskiej nie będzie występował w przypadku korzystania z usług świadczonych przez firmę Microsoft. Firma ta dostarcza szereg usług świadczonych w chmurze obliczeniowej, w tym usługę poczty elektronicznej (Outlook) oraz przechowywania i udostępniania plików (OneDrive) – stanowiące część produktu Office 365. Zgodnie z treścią punktu 7.h umowy subskrypcyjnej dotyczącej usług online firmy Microsoft[42], prawem właściwym dla zobowiązań umownych jest prawo irlandzkie. Ponadto w celu wyegzekwowania postanowień umownych Microsoft jest zobowiązany do wytoczenia powództwa przed sądem właściwym dla siedziby klienta. Firma ponadto deklaruje gotowość zawierania dodatkowych umów o przetwarzaniu danych zgodnych ze standardowymi klauzulami umownymi UE z każdym klientem korzystającym z Office 365, niezależnie od wielkości jego firmy i wartości umowy dotyczącej korzystania z usługi[43]. Na tym tle należy

[39] https://gsuite.google.com/terms/subprocessors.html

[40] https://admin.google.com/terms/apps/1/4/en/mcc_terms.html

[41] „*Najczęstsze pytania o bezpieczeństwo G Suite*", https://gsuite.google.com/faq/security/

[42] *Umowa subskrypcyjna dotycząca usług online firmy Microsoft*, wrzesień 2016, https://azure.microsoft.com/pl-pl/support/legal/subscription-agreement/

[43] Klauzule modelu UE – często zadawane pytania, https://products.office.com/pl-pl/business/office-365-trust-center-eu-model-clauses-faq

przypomnieć jednak nakaz sądu federalnego USA z 25 kwietnia 2014 roku[44], w którym Microsoft został zobowiązany do wydania kopii nośników elektronicznych, zawierających dane swojego klienta. Dane te były składowane w centrum przetwarzania w Irlandii, którym zarządzał podmiot zależny firmy Microsoft, zarejestrowany w Irlandii i podlegający prawu UE. Amerykański sąd zobowiązał zatem Microsoft do wydania informacji przechowywanych w innym kraju, bazując przy tym wyłącznie na przepisach prawa federalnego USA. Wyrok ten został zaskarżony i uchylony w 2016 roku w wyniku skutecznej apelacji Microsoft[45]. W uzasadnieniu wyroku sądu apelacyjnego podkreślono, że zobowiązanie skarżącego do wydania informacji przechowywanych w innym kraju doprowadziłoby do faktycznego transgranicznego przepływu informacji z pominięciem przepisów prawa irlandzkiego[46]. Sprawa nie jest jednak ostatecznie rozstrzygnięta, ponieważ prokurator skorzystał z instytucji ponownego wysłuchania, przewidzianego w prawie amerykańskim[47].

Sprawa ta wskazuje jednak na uzasadnioną wątpliwość co do skuteczności gwarancji kontraktowych zawartych w umowach z firmami posiadającymi siedzibę w USA w zakresie ochrony tajemnic zawodowych, w tym powierzonych danych osobowych.

Podsumowanie

Ochrona informacji przetwarzanych z wykorzystaniem chmury obliczeniowej to problem stosunkowo nowy, którego specyfika jest często niewystarczająco uwzględniona w istniejących przepisach prawnych. Państwa członkowskie UE ustanowiły skuteczny i spójny system ochrony danych osobowych, a Komisja Europejska podjęła znaczny wysiłek w celu zapewnienia, że dane

[44] United States District Court Southern District of New York, postanowienie z dn. 25 kwietnia 2014, sygn. akt: 13 Mag. 2814, https://assets.documentcloud.org/documents/1149373/in-re-matter-of-warrant.pdf

[45] United States Court of Appeals for the Second Circuit, wyrok w sprawie Microsoft v Stany Zjednoczone z dn. 14 lipca 2016, sygn.: 829 F.3d 197 (2016), https://www.justice.gov/opa/blog-entry/file/937006/download. Szersze omówienie wyroku i jego implikacji z punktu widzenia prawodawstwa amerykańskiego także w: Harvard Law Review t. 130 (2016), s. 769-776.

[46] Ibidem., s. 42.

[47] United States Court of Appeals for the Second Circuit, sygn. akt: 14–2985, Petition for Rehearing and Rehearing En Blanc", 13 października 2016, https://www.justsecurity.org/wp-content/uploads/2016/10/Microsoft_14-2985-United-States-Appellee-Petition.pdf

obywateli UE będą przetwarzane w sposób zgodny z tym systemem także poza granicami Wspólnoty. Reżim ustanowiony dla przetwarzania danych osobowych może być jednak niewystarczający dla zapewnienia adekwatnej ochrony prawnie chronionych tajemnic zawodowych, w szczególności tajemnicy adwokackiej. Brak ustandaryzowania w ramach UE definicji, zakresu stosowania i mechanizmów ochrony tajemnicy zawodów prawniczych powoduje, że prawnik decydujący się na korzystanie z usług świadczących w chmurze obliczeniowej za każdym razem musi wnikliwie przeanalizować nie tylko regulamin usługi, z której zamierza skorzystać – ale także przepisy krajowe państwa, w którym zlokalizowane jest centrum przetwarzania danych, oraz państwa, w którym siedzibę posiada usługodawca. W przypadku przekazywania danych poza granice UE dodatkowo rozważenia wymaga problem odpowiedniego transferu danych osobowych, w sposób zgodny z przepisami wspólnotowymi oraz krajowymi. Z pewnością pomocne przy podjęciu tej decyzji mogą być analizy i publikacje CCBE[48] czy GIODO[49], wskazujące na listę najważniejszych elementów, które powinny być brane pod uwagę przy weryfikacji i wyborze usług świadczonej w chmurze obliczeniowej.

Podsumowując rozważania na temat prawnych aspektów udostępniania i przetwarzania tajemnic zawodowych (w szczególności tajemnicy zawodów prawniczych) w chmurze obliczeniowej, zasadne wydaje się sformułowanie – jako postulatu *de lege ferenda* – potrzeby nowelizacji istniejących przepisów, dostosowujących zasady ochrony tajemnic zawodowych do współczesnych zagrożeń wynikających z nowoczesnych środków przetwarzania informacji. W szczególności zasadne wydaje się wprowadzenie na poziomie prawa wspólnotowego prawnej definicji tajemnicy zawodu prawniczego oraz mechanizmów zapewniających możliwość jej egzekwowania na jednakowym poziomie we wszystkich państwach UE.

Rozwiązania te mogą bazować na prawnym rozdzieleniu obowiązków właściciela informacji oraz firmy przetwarzającej informacje na jego zlecenie (np. firmy hostingowej, dostawcy usług chmury publicznej, ale także archiwum dokumentów czy firmy świadczącej usługi digitalizacji dokumentów). W takim przypadku żądania ze strony uprawnionych organów powinny być kierowane do firmy przetwarzającej dane, ale adresowane do właściciela informacji. Zatem firma przetwarzająca dane przekazywałaby takie żądanie do właściciela informacji, który byłby zobowiązany do wykonania żądania, ale miałby także realną

[48] Council of Bars and Law Societies of Europe, *CCBE Guidelines on the use of cloud computing services by lawyers*, 7 września 2012.

[49] Generalny Inspektor Ochrony Danych Osobowych, *Deklalog Chmuroluba*, http://www.giodo.gov.pl/259/id_art/6271/j/pl

możliwość powołania się na przepisy nakładające szczególny rygor poufności, np. związany z tajemnicą zawodów prawniczych. Należy podkreślić, że zastosowanie takiego podejścia nie utrudniłoby działania organom wymiaru sprawiedliwości, a jednocześnie umożliwiło prawnikom (oraz przedstawicielom innych zawodów przetwarzających informacje prawnie chronione) podjęcie skutecznych działań zmierzających do ochrony danych przed niepowołanym dostępem.

Niezależnie, czy na poziomie UE wypracowane zostanie wspólne podejście do ochrony tajemnic zawodowych przetwarzanych w rozproszonych sieciach informatycznych, słusznym wydaje się także, aby działania legislacyjne w tym zakresie zostały podjęte przez krajowego prawodawcę. Doprecyzowanie na gruncie ustawowym kręgu podmiotów zobowiązanych do zachowania tajemnicy zawodowej oraz zasad związanych z jej ochroną przez podwykonawców niewątpliwie przyczyniłoby się do zwiększenia gwarancji związanych z zachowaniem tajemnic zawodów prawniczych (w tym tajemnicy obrończej).

PROTECTION OF LEGAL PRIVILEGE IN THE CLOUD COMPUTING

The article presents most important issues related to cross-border processing of lawyers data containing professional secrets, including the processing of personal data. Author discusses risks associated with the lack of standardization in the area of protection of legal priviledge in cloud computing services in different jurisdictions, also between EU Member States.

Article is supplemented by an analysis of terms of service and privacy policies of the largest providers of services in the public cloud (Google, Microsoft) in the context of the fulfillment of the legal requirements for the protection of personal data and the professional secrecy.

Keywords: legal privilege, entrusting the processing of personal data, standard contractual clauses, cloud computing.