WYTYCZNE RADY ADWOKATUR I STOWARZYSZEŃ PRAWNICZYCH EUROPY W ZAKRESIE KORZYSTANIA PRZEZ PRAWNIKÓW Z USŁUG PRACY W CHMURZE

Conseil des barreaux européens - Council of Bars and Law Societies of Europe - Rada Adwokatur i Stowarzyszeń Prawniczych Europy
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 - B 1040 Brussels - Belgium - Tel.+32 (0)2 234 65 10 - Fax.+32 (0)2 234 65 11/12 - E-mail ccbe@ccbe.eu - www.ccbe.eu

SPIS TREŚCI

Conseil des barreaux européens - Council of Bars and Law Societies of Europe - Rada Adwokatur i Stowarzyszeń Prawniczych Europy
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 - B 1040 Brussels - Belgium - Tel.+32 (0)2 234 65 10 - Fax.+32 (0)2 234 65 11/12 - E-mail ccbe@ccbe.eu - www.ccbe.eu

Wytyczne Rady Adwokatur I Stowarzyszeń Prawniczych Europy w zakresie korzystania przez prawników z usług pracy w chmurze

I. WPROWADZENIE

1 Zakres dokumentu

Ten dokument ma na celu uświadomienie prawnikom różnych rodzajów ryzyka związanych z pracą w chmurze. Stosownie, wytyczne zawarte w drugiej części tego dokumentu są skierowane do samorządów i stowarzyszeń prawniczych należących do Rady Adwokatur i Stowarzyszeń Prawniczych Europy (dalej: Rada) i mają na celu zwrócenie ich uwagi na problemy, które prawdopodobnie napotkają prawnicy, gdy będą podejmować świadome decyzje z zakresu doradzania czy rozważania korzystania z usług pracy w chmurze.

2 Praca w chmurze

Praca w chmurze to termin ogólny, którym określa się infrastrukturę informatyczną, na którą składa się zdalne przechowywanie i przetwarzanie danych oraz oprogramowanie posadowione w centrum danych dostawcy środowiska w chmurze lub w centrach powiązanych, do której dostęp uzyskuje się w ramach usługi poprzez internet. Według Narodowego Instytutu Standardów i Technologii USA (ang. *US National Institute of Standards and Technology (NIST)*) praca w chmurze umożliwia wszechobecny, wygodny i dostępny w każdej chwili dostęp sieciowy do współdzielonej puli możliwych do skonfigurowania zasobów komputerowych takich jak sieci, serwery, pamięci, aplikacje i usługi, które można szybko udostępnić i które wymagają minimalnego wysiłku w zakresie zarządzania czy interakcji z usługodawcą[1].

3 Praca w chmurze na agendzie Komisji Europejskiej

Potrzeba opracowania europejskiej strategii w zakresie pracy w chmurze została zaakcentowana przez Komisję Europejską w Europejskiej agendzie cyfrowej dla Europy. Trzy szerokie obszary do uwzględnienia w tym kontekście w celu zmaksymalizowania korzyści pracy w chmurze dla Europy to:

- Ramy prawne: dotyczy ochrony danych i prywatności, w tym w wymiarze międzynarodowym. Dotyczy to także przepisów prawa i innych reguł związanych z procesem wprowadzenia pracy w chmurze w publicznych i prywatnych organizacjach.
- Podstawowe kwestie techniczne i handlowe: celem jest zwiększenie wsparcia dla badań europejskich i zwrócenie uwagi na kwestie krytyczne np. bezpieczeństwo i dostępność usług pracy w chmurze.

[1] P. Mell and T. Grance, **Definicja pracy w chmurze NIST, amer. Departament Handlu (styczeń 2011 r.) *(ang. The NIST Definition of Cloud Computing*,** National Institute of Standards and Technology, US Department of Commerce (January 2011)).

- Rynek: wsparcie dla projektów pilotażowych ukierunkowanych na wprowadzanie pracy w chmurze. Aby w pełni wykorzystać możliwości procedury udzielania zamówień publicznych, Komisja zaangażuje partnerów z sektora publicznego z państw członkowskich i na poziomie regionalnym do opracowania wspólnego podejścia do pracy w chmurze.

Jak donosi Komisja, w kilku z tych obszarów już rozpoczęto prace, w tym konsultacje publiczne w 2011 r., w których Rada także uczestniczyła[2].

4 Praca w chmurze dla prawników: korzyści i ryzyko

Kancelarie prawne oraz inne firmy korzystają z możliwości pracy w chmurze z wielu powodów. Jeden z nich stanowi możliwość obniżenia kosztów. Praca w chmurze może skutkować redukcją kosztów zakupu serwerów i oprogramowania oraz zatrudnienia pracowników IT do utrzymywania serwerów. Dodatkowo, ponieważ wiele aplikacji pracy w chmurze zapewnia dostęp z dowolnego miejsca, proste ustawienie pracy spoza kancelarii umożliwia zaoszczędzenie na czynszu i kosztach podróży oraz sprzyja współpracy pomiędzy biurami kancelarii prawnych zlokalizowanymi w wielu miejscach.

Ponadto, dla wielu biur kancelarii praca w chmurze może oznaczać uproszczenie prac komputerowych. W przypadku kancelarii posiadających infrastrukturę informatyczną, programy oprogramowania bazującego na chmurze mogą zmniejszyć poziom skomplikowania infrastruktury informatycznej. Podobnie, kancelarie dopiero rozpoczynające działalność, które nie posiadają systemów oprogramowania, mogą za pomocą programów oprogramowania bazującego na chmurze w prosty sposób stworzyć od zera efektywny system zarządzania pracą.

Systemy pracy w chmurze zazwyczaj zapewniają zwiększoną elastyczność dla użytkownika końcowego, ponieważ usługi pracy w chmurze są dostępne za pomocą łącza internetowego zawsze i wszędzie. Dalej, w przeciwieństwie do systemów komputerów biurkowych lub oprogramowania serwerowego, z platform bazujących na chmurze można korzystać na każdym komputerze czy urządzeniu z dostępem do internetu, za pomocą dowolnego systemu operacyjnego. Zawsze gdy użytkownik ma dostęp do internetu, może uzyskać dostęp do plików przechowywanych w chmurze. Dzięki temu praca w chmurze umożliwia prawnikom świadczenie usług w nowoczesny i wydajny sposób, z korzyścią dla klientów.

Jednakże, oprócz wielu istotnych korzyści, praca w chmurze jest też obarczona pewnym ryzykiem i stanowi pewne wyzwanie dla prawników: po pierwsze gdy chodzi o kwestie ochrony danych, po drugie gdy myślimy o zawodowych obowiązkach zachowania poufności i po trzecie w zakresie innych zawodowych i regulacyjnych obowiązków spoczywających na prawnikach. Chociaż pierwszy i drugi z tych obszarów są ze sobą ściśle powiązane, obszary te nie są jednak identyczne. Prawnik musi być także wrażliwy na czysto handlowe ryzyko, na które może być narażony, np. wskutek czasowej niedostępności usługi chmury skutkującej zakłóceniem jego działalności.

Istotą pracy w chmurze jest korzystanie z osoby trzeciej, zdalnego dostawcy usług przetwarzania, w tym usług przechowywania danych, w przeciwieństwie do korzystania z komputerów i serwerów biurowych użytkownika lub w pełni kontrolowanych przez użytkownika. Dostawca usług chmury często jest właścicielem olbrzymich centrów danych lub wynajmuje takie centra od innych dostawców; w przypadku największych dostawców usług chmury centra te mogą być połączone ze sobą tak by tworzyły sieć serwerów, z których niektóre mogą znajdować się poza EOG, na obszarze gdzie mają zastosowanie niższe standardy ochrony danych. W niektórych przypadkach takie centra mogą być zlokalizowane w krajach, które nie w pełni szanują zasady praworządności. Ponadto, w

[2] Odpowiedź Rady dot. publicznej konsultacji kwestii pracy w chmurze przez Komisję Europejską.

przypadku sieci serwerów w chmurze dane mogą podlegać dezagregacji i mogą być przechowywane na różnych serwerach (nawet w różnych krajach), a nawet stale migrować między tymi serwerami. W większości przypadków administratorzy takich sieci nie będą świadomi, gdzie dokładnie w sieci dany element danych może być przechowywany w danym czasie. Te uwarunkowania jasno pokazują konkretne problemy i potencjalne obawy prawników, gdy chodzi o standardy ochrony danych i potencjalną kradzież, utratę czy ujawnienie informacji poufnych.

Najbardziej widoczne obawy prawników związane z pracą w chmurze to[3]:

Problemy związane z zachowaniem tajemnicy zawodowej i ochroną danych:

- Może zaistnieć potrzeba sprecyzowania zakresu odpowiedzialności prawnika w odniesieniu do niezawodności i bezpieczeństwa Chmury, w której prawnik przechowuje dane swoich klientów.
- Praca w chmurze może wymagać sprecyzowania zakresu w jakim prawnicy potrzebują uzyskać zgodę klienta przed wykorzystaniem usług pracy w chmurze do przechowywania i transmisji informacji poufnych.
- Dane przechowywane w środowisku chmury mogą być narażone na ryzyko nieuprawnionego dostępu czy to fizycznego poprzez nieuprawniony dostęp do obiektu, w którym znajdują się serwery czy też elektronicznego, ze strony pracowników usługodawcy lub jego podwykonawców, przez osoby zewnętrzne, np. hackerów czy przez internet.

Problemy dotyczące eksterytorialności:

- Praca w chmurze może obejmować przetwarzanie danych na serwerach w krajach, które posiadają mniej prawnych mechanizmów ochrony informacji przechowywanej elektronicznie lub których mechanizmy mogą być mniej skuteczne niż te stosowane przez kraje UE/EOG i które nie podlegają systemowi nadzoru UE. Może się zdarzyć, że dostawcy usług pracy w chmurze będą podlegać regulacjom lokalnym zobowiązującym ich do przekazywania danych prawników europejskich przechowywanych na serwerze w chmurze do – jak może się okazać – organów krajowych państw nieczłonkowskich.
- Dodatkowym czynnikiem ryzyka jest rozszerzona legislacja zagraniczna, która może dążyć do nałożenia obowiązku ujawnienia danych na żądanie organów krajowych nie tylko na świadczące usługi pracy w chmurze firmy z państwa macierzystego, ale także na firmy zagraniczne, które ostatecznie pozostają własnością firm z państwa macierzystego. Stosownie, może okazać się, że praca w chmurze podlega niejasnym procedurom regulującym proces zapewnienia lub odmowy zapewnienia przez usługodawcę dostępu do informacji na wniosek administracji rządowej.

Problemy związane z (lokalnymi) wymogami deontologicznymi/regulacyjnymi:

- Problemy mogą pojawić się także wskutek rozbieżnych i/lub sprzecznych wymogów lokalnych krajowych samorządów i stowarzyszeń prawniczych, których prawnicy muszą przestrzegać, gdy chodzi o pracę na danych poufnych.
- Problemy związane z umowami z dostawcami usług pracy w chmurze:

[3] Niektóre z tych problemów zostały już zidentyfikowane w następujących dokumentach: Stowarzyszenie Prawników w Szkocji ***Porady z obszaru pracy w chmurze dla prawników (ang. Cloud Computing - Advice for the profession*** (2012)) i Komisja ds. Etyki amer. Federacji Stowarzyszeń Prawników Grupa Robocza 20/20 ds. skutków korzystania z nowych technologii (ang. *2020 Working Group on the Implications of New Technologies*) – dokument dot. poufności klienta i korzystania z technologii przez prawników (20 września 2010 r.).

- Praca w chmurze może podlegać niejasnym politykom z zakresu właścicielstwa przechowywanych danych.
- Dostawcy usług pracy w chmurze mogą nie wykonywać odpowiednich kopii zapasowych danych i/lub nie zapewniać stałej dostępności usług pracy w chmurze.
- Praca w chmurze może być objęta niedostatecznym szyfrowaniem danych.
- Praca w chmurze może podlegać niejasnym politykom z zakresu informowania klientów o przypadkach naruszenia bezpieczeństwa.
- Praca w chmurze może podlegać niejasnym politykom z zakresu okresu przechowywania danych.
- Praca w chmurze może podlegać niejasnym politykom z zakresu niszczenia danych, w sytuacji gdy kancelaria prawna nie chce, aby określone dane były w dalszym ciągu dostępne na serwerze w chmurze lub gdy chce przesłać dane do innej kancelarii prawnej.
- Praca w chmurze może skutkować problemami w obszarze dostępu do danych za pomocą łatwo dostępnego oprogramowania, w sytuacji gdy kancelaria prawna rozwiązuje współpracę z dostawca usług pracy w chmurze lub gdy usługodawca zmienia lub kończy swoją działalność.

5 Wytyczne Rady z zakresu pracy w chmurze

Jak wskazano powyżej, praca w chmurze stanowi dla prawników dobrą alternatywę dla tradycyjnych systemów infrastruktury informatycznej. Jednakże, oprócz wielu istotnych korzyści, praca w chmurze niesie z sobą także pewne ryzyko i wyzwania, gdy chodzi o możliwość wywiązywania się przez prawników z ich obowiązków prawnych jako administratorów danych na mocy Dyrektywy o ochronie danych, stosowania ich zawodowych kodeksów postępowania, zwłaszcza w zakresie obowiązków zachowania poufności w odniesieniu do danych klienta, czy ich odpowiedzialności w ramach systemów nadzoru, którymi są objęci, np. w kwestii prowadzenia ksiąg rachunkowych, które mogą podlegać kontroli przez ich regulatora, czy zapewnienia ciągłości działalności w sytuacji gdy kancelaria prawna nie jest w stanie świadczyć usług.

Rozważając możliwość wdrożenia pracy w chmurze w swojej kancelarii, prawnicy muszą koniecznie przedsięwziąć kroki niezbędne do zapewnienia ochrony danych klienta, zachowania poufności informacji klienta oraz odpowiedniego ustosunkowania się do obaw wskazanych w ust. 2. Pomimo tego, tak jak i inni konsumenci, prawnicy często nie będą dysponowali wystarczającą wiedzą, aby uzyskać pewność, że środki bezpieczeństwa są wystarczające. Mając powyższe na uwadze, Rada opracowała zbiór wytycznych z zakresu korzystania przez prawników z usług pracy w chmurze. Wytyczne mają na celu lepsze uświadomienie prawnikom ryzyka związanego z pracą w chmurze oraz wsparcie prawników w podejmowaniu świadomych decyzji odnośnie do technologii.

II. WYTYCZNE RADY Z ZAKRESU KORZYSTANIA PRZEZ PRAWNIKÓW Z USŁUG PRACY W CHMURZE

Doradzając swoim członkom, którzy rozważają możliwość wdrożenia pracy w chmurze w swoich kancelariach, Krajowe Samorządy i Stowarzyszenia Prawnicze powinny dążyć do skierowania ich uwagi na następujące kwestie:

A. Przepisy z zakresu ochrony danych i zasady dotyczące tajemnicy zawodowej

Z zasady, przepisy z zakresu ochrony danych i zasady dotyczące tajemnicy zawodowej powinny stanowić punkt wyjścia dla prawników w ich rozważaniach na temat możliwości wykorzystania usług pracy w chmurze. W szczególności, prawnicy powinni zweryfikować czy zasady stosowane przez samorządy i stowarzyszenia prawnicze w ich państwie macierzystych dopuszczają przechowywanie danych poza kancelarią prawną i zapewnić, że dostawca usług pracy w chmurze nie podlega rozszerzonej jurysdykcji zobowiązującej go do przekazywania danych prawników europejskich przechowywanych na serwerze w chmurze do – jak może się okazać – organów krajowych państw nieczłonkowskich. Prawnicy mogą chcieć rozważyć czy zważywszy na te obawy, w danym przypadku nie byłoby właściwe skorzystanie z dostawcy usług pracy w chmurze ustanowionego w ramach EOG i (niezależnie od jego lokalizacji) na tyle, na ile to możliwe niepodlegającego takiej rozszerzonej jurysdykcji.

B. Wstępna analiza usług pracy w chmurze

Kancelarie prawne niezmienne uczestniczą w przetwarzaniu różnych rodzajów danych, które mogą być objęte różnymi wymogami, gdy chodzi o pracę na tych danych i ich ochronę. Nadrzędnym obowiązkiem dotyczącym wszystkich danych jest jednak obowiązek zachowania ich poufności. Prawnicy rozważający wykorzystanie usług pracy w chmurze powinni przede wszystkim pomyśleć o rodzaju modelu obsługi, który w odpowiedni sposób spełniałby obecne i przyszłe potrzeby kancelarii. Korzystając z oprogramowania chmury jako usługi (ang. *Software as a Service (SaaS)*)[4] lub infrastruktury chmury jako usługi (ang. *Cloud Infrastructure as a Service (IaaS)*)[5] prawnicy będą musieli zapewnić, że obydwie te usługi obejmują przetwarzanie i przechowywanie danych, które mogą obejmować dane osobowe i wrażliwe dane osobowe oraz informacje objęte klauzulą poufności wobec klienta. Toteż prawnicy muszą być informowani i muszą być świadomi tych kwestii, gdy przetwarzają dane w zewnętrznym środowisku. Dodatkowo należy rozważyć wprowadzenie procedur szyfrowania danych podczas transmisji i w trakcie przechowywania danych.

[4] SaaS (Cloud Software as a Service): dostawca dostarcza za pomocą internetu różne usługi aplikacyjne i udostępnia je użytkownikom końcowym. Usługi te często mają na celu zastąpienie konwencjonalnych aplikacji instalowanych przez użytkowników na ich systemach lokalnych; w konsekwencji, od użytkowników ostatecznie oczekuje się wyoutsourcowania ich danych do danego dostawcy usług. Ma to miejsce np. w przypadku typowych biurowych aplikacji webowych np. arkuszy kalkulacyjnych, narzędzi tekstowych, komputerowych rejestrów/ksiąg czy kalendarzy itd.; jednak rzeczone usługi obejmują także oparte na chmurze aplikacje poczty elektronicznej. Źródło: art. 29 Grupy Roboczej ds. ochrony danych, Opinia 05/2012 dot. pracy w chmurze (ang. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*).

[5] IaaS: dostawca użycza infrastruktury technologicznej (tj. wirtualnych serwerów zdalnych), na której użytkownik końcowy może polegać zgodnie z mechanizmami i ustaleniami, dzięki czemu zastąpienie firmowych systemów informatycznych w siedzibie firmy i/lub korzystanie z użyczonej infrastruktury równolegle do systemów firmy okazuje się proste, efektywne i z korzyścią dla użytkownika. Tacy dostawcy są zazwyczaj wyspecjalizowanymi graczami rynkowymi i mogą polegać na fizycznej, skomplikowanej infrastrukturze, która często obejmuje kilka obszarów geograficznych. Źródło: art. 29 Grupy Roboczej ds. ochrony danych, Opinia 05/2012 dot. pracy w chmurze (ang. *Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing*).

W tych warunkach, w sytuacji gdy prawnik rozważa korzystanie z pracy w chmurze, pierwszą decyzją, którą musi podjąć jest ta czy będzie korzystał z modelu usług SaaS czy IaaS.

Ponadto, usługi pracy w chmurze mogą być dostarczane przez dostawcę usług chmury publicznej lub dostawcę usług chmury prywatnej. Dostawca usług chmury publicznej to dostawca, który oferuje swoje usługi wszystkim, podczas gdy dostawca usług chmury prywatnej stanowi zazwyczaj własność i/lub jest kontrolowany przez małą grupę. Np. w niektórych państwach członkowskich prawnicy zorganizowali się i stworzyli chmury prywatne. Rozróżnienie pomiędzy chmurą publiczną i prywatną może mieć duże znaczenie dla oceny, który dostawca usług stanowi mniejsze ryzyko, np. gdy chodzi o możliwość przechowywania danych na serwerach posadowionych poza EOG lub danych, które mogą podlegać rozszerzonej jurysdykcji. Korzystanie z publicznej chmury nie zawsze powinno być postrzegane jako niewłaściwe, pod warunkiem że prawnik przeprowadził najpierw analizę *due diligence* samego dostawcy, bezpieczeństwa centrum danych wykorzystywanego przez dostawcę oraz w zakresie szczegółowości zapisów umowy o świadczenie usług (ang. Service Level Agreement, SLA). Gdy analiza due diligence wykaże kwestie problematyczne, może okazać się, że dostawcy (zwłaszcza małe i średnie firmy) będą gotowi dopasować swoje usługi i/lub negocjować warunki umowne tak by uwzględnić te kwestie.

Przed zawarciem umowy prawnik jako użytkownik końcowy usługi pracy w chmurze, powinien zweryfikować:

[a] doświadczenie,

[b] reputację,

[c] specjalizację,

[d] adres rejestrowy i lokalizację dostawcy usług pracy w chmurze.

Dodatkowo, osobno należy zweryfikować:

[a] wypłacalność, rzetelność, właścicielstwo i adekwatność kapitałową dostawców usług,

[b] potencjalne konflikty interesów,

[c] ryzyko niewłaściwego wykorzystania przechowywanych informacji,

[d] dokładne posadowienie serwerów wykorzystywanych do przechowywania danych,

[e] na tyle na ile to możliwe, bezpieczeństwo zarówno fizyczne, jak i elektroniczne serwerów i centrum danych, w których się znajdują,

[f] właściwe przepisy prawa cywilnego, karnego i publicznego oraz regulacje.

C. Uprzednia ocena wrażliwości danych

Kancelarie prawne niezmienne uczestniczą w przetwarzaniu różnych rodzajów danych, które mogą być objęte różnymi wymogami, gdy chodzi o pracę na tych danych i ich ochronę. Każdej decyzji dotyczącej przechowywania informacji na serwerze w chmurze powinna koniecznie towarzyszyć analiza w zakresie rodzaju informacji (dane pracowników, dane karne, ogólne archiwa prawnicze itd.) i poziomu zabezpieczeń, które muszą zostać zastosowane.

D. Ocena zabezpieczeń

Każda ocena dostawców usług pracy w chmurze obejmuje ocenę zastosowanych zabezpieczeń technicznych, fizycznych i organizacyjnych zgodnie z krajowymi i międzynarodowymi standardami zarządzania ryzykiem IT, np. normą ISO 27001:2005

(zarządzanie bezpieczeństwem) i ISO 9001 (zarządzanie jakością). Certyfikaty wydane przez uznanych audytorów IT także mogą służyć jako kryterium testowe.

Tam gdzie to właściwe, prawnik musiałby także ocenić niezawodność jego własnych standardów bezpieczeństwa poprzez ustanowienie zasad w obszarze technologii informacyjno-komunikacyjnych, zapewnienie informacji oraz przeszkolenie pracowników. Ponieważ kancelarie prawne rzadko posiadają skuteczny całościowy proces zarządzania hasłami, należy rozważyć tokenizację lub wprowadzenie elektronicznej rejestracji przy biurku za pomocą kart identyfikacyjnych pracowników.

Ogólnie rzecz biorąc, prawnik powinien zawsze rozważyć uzyskanie profesjonalnego wsparcia i porady w procesie wybierania i monitorowania dostawców usług pracy w chmurze.

E. Porównanie istniejącej własnej infrastruktury informatycznej z usługami pracy w chmurze

W ramach oceny usług pracy w chmurze, prawnicy powinni porównać te usługi z ich obecną infrastrukturą informatyczną. Taka ocena pozwoli kancelarii prawnej podjąć decyzję czy przejście na osobne środowisko usługi pracy w chmurze będzie skutkowało obniżeniem czy podwyższeniem ryzyka.

F. Ocena możliwości odzyskania danych w sytuacji awarii po stronie dostawcy usług pracy w chmurze, awarii w kancelarii prawnej lub sporu umownego pomiędzy dostawcą usług i kancelarią prawną

Prawnik nie będzie chciał, aby działalność jego kancelarii została zakłócona w sytuacji wystąpienia awarii po stronie dostawcy usług pracy w chmurze. Dodatkowo, w wielu jurysdykcjach, prawnicy są zobowiązani zawodowo i regulacyjnie do zapewnienia dostępności do danych klienta i innych materiałów, które nie muszą stanowić danych osobowych czy danych klienta (np. ich zapisy księgowe) do celów kontroli przez właściwe organy zawodowe i krajowe organy nadzoru. Gdy takie materiały nie mogą zostać udostępnione na żądanie tych organów, czy to z powodu awarii po stronie dostawcy usług pracy w chmurze, awarii w kancelarii prawnika (skutkującej naruszeniem lub rozwiązaniem umowy z dostawcą usług pracy w chmurze) czy też w wyniku sporu umownego z dostawcą usług pracy w chmurze, który może skutkować zajęciem lub prawem retencji do danych prawnika po stronie usługodawcy, prawnik może narazić się na stwierdzenie w odniesieniu do jego osoby zachowania niezgodnego z etyką zawodową lub popełnienie czynu zabronionego wskutek niemożności przedstawienia danych lub innych materiałów. Taki czyn zabroniony lub zachowanie niezgodne z etyką zawodową może utrzymywać się tak długo jak długo prawnik nie jest w stanie przedstawić materiałów.

Toteż, w trakcie oceny dostawcy usług pracy w chmurze, prawnik powinien ocenić jego stopień narażenia na negatywne konsekwencje zawodowe lub prawne związane z taką niedostępnością danych. Prawnik powinien rozważyć czy konieczne jest wynegocjowanie odpowiednich warunków umownych w celu zapewnienia stałej dostępności, nawet w sytuacji zaistnienia sporu umownego czy awarii po stronie usługodawcy, czy jego własnej kancelarii prawnej. Prawnik może także chcieć ocenić czy konieczne jest skorzystanie ze środków technicznych w celu opanowania takiej sytuacji niedostępności. Przykładowo: umowne prawo do odzyskania danych może mieć ograniczone zastosowanie, gdy dane występują w formie niełatwej do odczytania. Może okazać się konieczne zapewnienie stałej dostępności oprogramowania potrzebnego do odczytu danych, np. w formie licencji na dane oprogramowanie stale przechowywanej w depozycie na rzecz prawnika.

G. Zabezpieczenia umowne

Ważne jest, aby rozważyć przynajmniej następujące aspekty:

[a] zakres usługi,

[b] dostępność systemu,

[c] terminy wyprowadzania błędów i usuwania awarii,

[d] kary umowne za niewykonanie lub opóźnienie wykonania (gdy egzekwowalne na mocy właściwych krajowych przepisów prawa),

[e] zmiany w wymogach serwisowych,

[f] zobowiązanie usługodawcy do dostosowania systemu w zakresie wymaganym przez zmiany regulacyjne lub legislacyjne,

[g] wyłączenie możliwości podzlecania bez uprzedniej zgody,

[h] licencje, zwłaszcza zapewnienie, że usługodawca posiada odpowiednie licencje na wykorzystywane przez niego oprogramowanie,

[i] właścicielstwo przechowywanych danych i wyłączne prawo dostępu,

[j] umowy dot. ochrony danych, w szczególności gdy wymagane przez i w zakresie wymaganym przez właściwe krajowe przepisy prawa,

[k] zabezpieczenia i odpowiedzialność,

[l] zobowiązanie do zachowania poufności,

[m] monitoring i sprawozdawczość,

[n] dokumentacja techniczna, dokumentacja procesu i dokumentacja administratora systemu/użytkownika,

[o] prawo do kontroli i audytu, w tym standardowe certyfikacje,

[p] kopie zapasowe, plan awaryjny,

[q] dostarczenie kodu źródłowego (ang. usługa *Software-ESCROW*) w sytuacji niewypłacalności lub niezdolności biznesowej usługodawcy do świadczenia usług,

[r] posadowienie serwerów – w kraju, w ramach EOG lub poza EOG, ale z zachowaniem standardów europejskich w zakresie ochrony prywatności i poufności,

[s] ubezpieczenie, gwarancje, rękojmie i odszkodowanie,

[t] okres, sposób wypowiedzenia usługi,

[u] koniec usługi i postanowienia dotyczące rozwiązania umowy, w tym z zakresu przekazania i kasowania danych,

[v] procedury mediacyjne, zawierania ugody i/lub arbitrażowe,

[w] właściwe przepisy prawa i jurysdykcja.

H. Czynniki losowe

Należy zwrócić uwagę na fakt, że dostępność usługi pracy w chmurze zależy od nieprzerwanego połączenia sieciowego. Prawnik powinien rozważyć czy nie ma potrzeby posiadania alternatywnego lub zapasowego połączenia z internetem w sytuacji awarii podstawowego połączenia.

I. Przejrzystość

Aby zapewnić przejrzystość usług prawniczych, prawnik może rozważyć poinformowanie przyszłych klientów, że kancelaria prawna korzysta z usług pracy w chmurze. Można to zrobić poprzez umieszczenie informacji w ogólnych warunkach każdej umowy o świadczenie obsługi prawnej. Informacja ta będzie podlegała zmianie stosownie do wyników negocjacji z poszczególnymi klientami. Ta formuła pozwoliłaby podawać szczegółowe informacje na temat pracy w chmurze wyłącznie na prośbę danego klienta. Należy zauważyć, że mogą istnieć jurysdykcje, które wymagają zgody klienta w tym zakresie.

Umieszczenie informacji w ogólnych warunkach każdej umowy o świadczenie obsługi prawnej byłoby wskazane zwłaszcza w sytuacji gdy kancelaria prawna korzysta z usług dostawcy usług pracy w chmurze na serwerze posadowionym w innej jurysdykcji. W takim przypadku prawnik może potrzebować świadomej zgody klienta na przechowywanie danych poufnych na takich serwerach. Klientowi należy dostarczyć informacje na temat dostawcy usług pracy w chmurze oraz prawnych standardów ochrony danych, przepisów dotyczących ochrony prywatności i zasad poufności obowiązujących prawników w kraju posadowienia serwerów.

J. Kwestia ogólna

Praca w chmurze jest obarczona wieloma rodzajami ryzyka i rodzi problemy opisane w tych wytycznych, zwłaszcza gdy chodzi o poufność/ tajemnicę adwokacką/radcowską i retencję danych. Rada Adwokatur i Stowarzyszeń Prawniczych Europy zachęca samorządy i stowarzyszenia prawnicze do zwiększenia świadomości ich członków w zakresie konieczności wykazywania większej czujności oraz stosowania zabezpieczeń wysokiego poziomu. Zabezpieczenia prawne i techniczne powinny zostać zapewnione prawnikom przez dostawców usług pracy w chmurze (np. gwarancja tworzenia długoterminowych kopii zapasowych dla danych itd.).

W praktyce, prawnicy nie zawsze mają możliwość spełnić wszystkie te wymagania. Toteż, samorządy i stowarzyszenia prawnicze zachęca się do określenia mechanizmów, które ułatwią prawnikom zastosowanie się do tych wytycznych, np. poprzez tworzenie własnych infrastruktur pracy w chmurze przy uwzględnieniu kwestii wskazanych powyżej. W takiej sytuacji mogą życzyć sobie przeprowadzenia oceny skutków.