KRAJOWA IZBA
RADCÓW PRAWNYCH

CHMURA W KANCELARII PRAWNEJ CZY KANCELARIA PRAWNA W CHMURZE?

PUBLIKACJA PO KONFERENCJI
KRAJOWEJ IZBY RADCÓW PRAWNYCH
20 CZERWCA 2018 R.

Spis treści

Słowo wstępne Macieja Bobrowicza

Prawnicy – radcy prawni i adwokaci, stają dzisiaj przed coraz większymi wyzwaniami związanymi zarówno z rozwojem technologii informatycznych wykorzystywanych w praktyce radcy prawnego i adwokata, jak i związanymi z konkurencyjnością na rynku usług prawnych. Coraz więcej graczy pojawia się na rynku, stąd też wielu z nasz szuka rozwiązań poprawiających naszą ofertę skierowaną do klientów. Takie możliwości stwarzają nowe technologie, zwłaszcza związane z przekazywaniem i przechowywaniem danych. Chmura w kancelarii prawnej to przecież nie tylko poczta, ale również przechowywanie dokumentów dotyczących prowadzonych spraw, billingowanie klientów, czy przesyłanie materiałów i akt.

Jednakże wszystkie te elementy nowoczesnej komunikacji, w przypadku radców prawnych, muszą spełniać również wymogi poufności wynikające z kodeksu etyki oraz muszą spełniać wymogi związane z przepisami prawa powszechnie obowiązującego. Nie wszystkie oferowane na rynku rozwiązania spełniają te wytyczne, dlatego tak ważne jest dogłębne analizowanie oferowanych produktów i wybór tych, które spełniają wszelkie wymagane zasady.

Mam nadzieję, że opracowanie, które właśnie Państwo czytacie, odpowie na wiele pytań związanych ze stosowaniem rozwiązań chmurowych w ramach świadczenia usług prawnych. Z pewnością uzyskacie informację na temat korzyści i ryzyk związanych z wdrożeniem chmury w kancelariach prawnych oraz informację czy warto w każdym przypadku wdrażać chmurę, jak korzystać z rozwiązań w chmurze, czy jest alternatywa dla chmur i jak stosować w praktyce rozwiązania chmurowe.

Dzięki takim konferencjom, jak zorganizowana przez Komisję Rozwoju Zawodowego, poznajemy odpowiedzi na dręczące nas pytania i oferujemy klientom rozwiązania, które wyróżniają nas na rynku. Nas – radców prawnych. To wyróżnia nas wśród prawników. Bo zawód radcy prawnego to profesjonalizm i nowoczesność, również w chmurze.

r. pr. Maciej Bobrowicz
Prezes Krajowej Rady Radców Prawnych

Warszawa, dnia 31 lipca 2018 r.

Coraz więcej graczy pojawia się na rynku, stąd też wielu z nas szuka rozwiązań poprawiających naszą ofertę skierowaną do klientów. Takie możliwości stwarzają nowe technologie, zwłaszcza związane z przekazywaniem i przechowywaniem danych.

Słowo wstępne Włodzimierza Chróścika

Mobilność, dostępność, wysoka jakość, ale przede wszystkim bezpieczeństwo. To cechy, jakie powinna posiadać współczesna Kancelaria, aby zapewnić swoim Klientom odpowiednie bezpieczeństwo prawne i najwyższy poziom świadczonych usług.

Wykonywanie zawodu zaufania publicznego w świecie, w którym książki zastępowane są e-bookami, gazety e-wydaniami, wizytówki stronami internetowymi, a dane przetwarza się w e-rejestrach, nie musi oznaczać ograniczonego zaufania do postępu technologicznego. Ale to właśnie profesjonalni prawnicy powinni zachować szczególną czujność przy wdrażaniu nowoczesnych rozwiązań w procesie pracy.

Z technologii chmury korzystają obecnie zarówno przedsiębiorcy, jak i organy władzy publicznej. Zastosowanie rozwiązań chmurowych pozwala bowiem na radykalne przyspieszenie i usprawnienie realizowanych działań. O ile prościej jest przecież wykonać kilka kliknięć, aby przejrzeć interesujący nas dokument, niż spędzić długie godziny w kolejce do sądowej czytelni akt.

Decyzja o przeniesieniu Kancelarii do chmury musi przede wszystkim uwzględniać zasady etyki zawodowej, które zobowiązują do odpowiedniego zabezpieczenia przed niepowołanym ujawnieniem wszelkich informacji objętych tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia. Powierzenie poufnych danych systemowi informatycznemu może się wiązać z ryzykiem ich nieuprawionego udostępnienia, a co za tym idzie - odpowiedzialnością zawodową radcy prawnego. Dlatego tak istotne jest wyjaśnienie wszystkich wątpliwości, analityczne i szczegółowe rozpoznanie rynku i dostępnych ofert, a także wypracowanie takich standardów zachowań, które usprawnią naszą pracę, nie niosąc za sobą przykrych konsekwencji.

Obawy budzi tylko to, co nieznane. W niniejszej publikacji zostały omówione najistotniejsze kwestie dotyczące działania w chmurze. Zawarte w niej informacje i wskazówki pozwolą Państwu na optymalne wykorzystanie technologi chmury w Kancelarii, przy jednoczesnej minimalizacji związanego z tym ryzyka.

Jak zachować poufność nie stając się niedostępnym? Jak szybko przekazywać dane bez narażenia na ich utratę? Odpowiedzi na te pytania poszukiwała Komisja Wspierania Rozwoju Zawodowego KRRP, organizując w dniu 20 czerwca 2018 r. konferencję dotyczącą korzyści i ryzyk związanych z wdrożeniem chmury w Kancelarii. Dzięki udziałowi w debacie dotyczącej rozwiązań chmurowych, uczestnicy konferencji uzyskali pewność, że Kancelaria w chmurze nie oznacza bujania w obłokach.

r. pr. Włodzimierz Chróścik
Przewodniczący Komisji Wspierania Rozwoju Zawodowego
Krajowej Rady Radców Prawnych

Warszawa, dnia 31 lipca 2018 r.

WPROWADZENIE

Wspomnienie Konferencji

W dniu 20 czerwca 2018 r. w Warszawie odbyła się konferencja pt. „Chmura w kancelarii prawnej czy kancelaria prawna w chmurze?". Konferencja poświęcona była tematyce stosowania rozwiązań chmurowych w świadczeniu usług prawnych.

Organizatorem konferencji była Komisja Wspierania Rozwoju Zawodowego Krajowej Izby Radców Prawnych, której przewodniczącym jest Włodzimierz Chróścik. Konferencję swoim patronatem objął Minister Przedsiębiorczości i Technologii.

Konferencję otworzyli Prezes Krajowej Rady Radców Prawnych Maciej Bobrowicz oraz Przewodniczący Komisji Wspierania Rozwoju Zawodowego Krajowej Izby Radców Prawnych Włodzimierz Chróścik, zapraszając uczestników do debaty.

Konferencję rozpoczęło przemówienie Dominika Wójcickiego, Dyrektora w Departamencie Gospodarki Elektronicznej, Ministerstwa Przedsiębiorczości i Technologii, który podkreślał między innymi rolę technologii w świadczeniu usług oraz wyraził zadowolenie, że radcowie prawni interesują się stosowaniem rozwiązań technologicznych w wykonywaniu zawodu radcy prawnego.

Podczas konferencji wystąpili prelegenci, wśród których byli przedstawiciele dostawców technologii i rozwiązań chmurowych oraz ich użytkownicy, w tym

przedstawiciele kancelarii prawnych, które stosują już rozwiązania chmurowe w świadczeniu usług prawnych. Taki dobór prelegentów zapewnił możliwość pogłębionej analizy tematu rozwiązań chmurowych oraz żywą i merytoryczną debatę już od początku Konferencji.

Zaproszenie do wzięcia udziału w Konferencji w charakterze prelegentów przyjęli (w kolejności wystąpień podczas Konferencji):

- Adam Kotarbiński, Chief Information Officer / Partner, Magnusson
- Wioletta Kulińska, Adwokat / Associate, Magnusson
- Michał Jaworski, Członek Zarządu Microsoft, Dyrektor ds. Innowacji Technologicznych
- Radosław Ochotny, Technology Strategist, Microsoft
- Renata Zalewska, Radca Prawny Microsoft
- Agata Szeliga, Radca Prawny, Partner, Sołtysiński, Kawecki & Szlęzak
- Tomasz Plata, CEO & Co-founder, Autenti
- Michał Tabor, Head of R&D, Autenti
- Łukasz Wachowicz, Head of Sales & Partnerships, Autenti

- Marek Laskowski, Dyrektor Działu IT, Domański Zakrzewski Palinka
- Piotr Marczuk, Dyrektor ds. Polityki Korporacyjnej na region CEE, Microsoft

Konferencja miała formułę debaty, w czasie której radcowie prawni mogli zadawać prelegentom pytania oraz brać czynny udział w dyskusji, z której to możliwości czynnie korzystali, a publiczność żywo reagowała na wystąpienia prelegentów.

Konferencję poprowadziły Joanna Daniłowicz i Aneta Pacek – Łopalewska, radcowie prawni z OIRP Warszawa, od kilku lat angażujący się obok pracy zawodowej w projekty technologiczne oraz zajmujący się wspieraniem prawników we wdrażaniu technologii.

Podczas Konferencji uczestnicy mogli dowiedzieć się, jakie są korzyści i ryzyka związane z wdrożeniem chmury w kancelariach prawnych oraz uzyskać informacje, czy warto wdrażać chmurę, jak z niej korzystać oraz jaka jest alternatywa dla chmur i jak stosować w praktyce te rozwiązania.

Wszystkie zdjęcia z konferencji pochodzą ze strony Krajowej Izby Radców Prawnych.

Autor zdjęć: Piotr Gilarski

Konferencji została poświęcona specjalna strona internetowa (www.konferencja.kirp.pl), na której można znaleźć program konferencji oraz informacje na temat prelegentów. Można również sprawdzić na jakie pytania odpowiadali prelegenci. Każdy radca prawny mógł również włączyć się debaty zadając pytanie

za pośrednictwem specjalnego formularza umieszczonego na stronie. Tą drogą radcowie prawni zadali kilkadziesiąt pytań.

I tak, w kwestii bezpieczeństwo danych kancelarii w chmurze, chcieli wiedzieć np., jakie są podstawowe ryzyka dla bezpieczeństwa danych związane z wdrożeniem rozwiązania chmurowego i jak można zabezpieczyć kancelarię i dane jej klientów w umowie z dostawcą chmury.

W trakcie konferencji radcowie prawni pytali również o to, czy rozwiązania chmurowe są zgodne z RODO, czy wdrażając rozwiązania chmurowe kancelaria zwiększa ryzyko utraty danych i czy wszystkie dane można umieścić w chmurze. W zakresie świadczenia usług z wykorzystaniem chmury pytania dotyczyły m.in. sposobu, w jaki dostawca usługi/rozwiązania wykorzystuje chmurę i w jaki sposób zapewnia dostępność ich klientom.

Nie brakowało też pytań o efektywność rozwiązania chmurowego dla kancelarii, a dokładnie o to, jakie główne argumenty przemówiły za wyborem rozwiązania chmurowego dla kancelarii, do czego kancelaria stosuje chmurę i jak zareagowali klienci – jakie były ich najczęstsze pytania i obawy. W części zaś dotyczącej tego, czy w każdej kancelarii może działać chmura, radcowie prawni pytali o koszty tego rozwiązania i o to od czego one zależą.

Co istotne, o ryzykach, korzyściach, wyzwaniach, kosztach i innych aspektach rozwiązań chmurowych mówili praktycy IT oraz prawnicy, którzy takie rozwiązanie chmurowe wdrożyli i korzystają z niego na co dzień. Odrębnym punktem była dyskusja na niezwykle aktualny i gorący temat bezpieczeństwa i ochrony danych.

Po zakończeniu konferencji, jej uczestnicy potwierdzali, że tematy technologiczne są dla nich interesujące, a na Konferencji o rozwiązaniach chmurowych otrzymali cenną wiedzę od najlepszych specjalistów IT i radców prawnych wdrażających te rozwiązania w swoich kancelariach.

1

ROZDZIAŁ PIERWSZY

CHMURA - PERSPEKTYWA PRAWNIKA


CHMURA

1.1 - Perspektywa prawnika

Zgodnie z definicją Narodowego Instytutu Standardów i Technologii USA (ang. US National Institute of Standards and Technology (NIST)) chmura obliczeniowa daje możliwość wszechobecnego, wygodnego i dostępnego w każdej chwili dostępu sieciowego do współdzielonej puli zasobów komputerowych takich jak: sieci, serwery, pamięci, aplikacje i usługi, które można szybko udostępnić przy minimalnym wysiłku zarządzania i na minimalnym poziomie interwencji reprezentantów usługodawcy [1].

Główny Urząd Statystyczny proponuje zaś jeszcze prostsze poniższe wyjaśnienie chmury obliczeniowej (ang. „cloud computing"):

> *„Usługi chmury obliczeniowej to możliwość korzystania ze skalowalnych usług ICT (pl. „technologie informacyjne i komunikacyjne") przy zastosowaniu Internetu."*[2]

Prawnikowi o nieco bardziej humanistycznym umyśle najprościej jednak możnaby wyjaśnić chmurę obliczeniową jako model przetwarzania danych, który oparty jest o świadczenie usług IT, w szczególności przechowywania, przetwarzania i przesyłania danych przez dostawcę, który zapewnia niezbędną infrastrukturę i oprogramowanie.

Celem chmury obliczeniowej jest rezygnacja z modelu utrzymywania własnej dużej infrastruktury informatycznej (np. serwerownie), czy zakup i zarządzanie oprogramowaniem opartym o model licencji, eliminacja konieczności utrzymywania środowiska i ciągłych starań o zapewnienie bezpieczeństwa, aktualizacji i najwyższej jakości. Modele płatności to najczęściej abonament za świadczoną usługę dostępną w modelu chmurowym.

Najczęstsze rodzaje chmury to:

- chmura publiczna – zasoby należące do dostawcy są udostępniane do korzystania przez nieokreśloną grupę odbiorców,

- chmura prywatna – zasoby mogą należeć do dostawcy bądź po ich zorganizowaniu przez dostawcę mogą należeć do użytkownika i są udostępniane do korzystania wyłącznie przez tego jednego użytkownika,

---

1 https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

2 GUS, Pojęcia używane w statystyce publicznej; dziedzina: nauka, technika i społeczeństwo informacyjne; http://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/3086,pojecie.html

- chmura hybrydowa - będąca połączeniem modelu dwóch powyższych lub infrastruktury lokalnej, tj. część danych i aplikacji użytkownika funkcjonuje w chmurze prywatnej a druga część w publicznej lub we własnych serwerowniach lokalnych, przy czym model ten zapewnia pełną kompatybilność i przenoszalność danych wedle uznania użytkownika.

Chmura z punktu widzenia prawnego

Jak wyżej zostało wspomniane, korzystanie z chmury obliczeniowej odbywa się poprzez świadczenie usługi przez dostawcę na rzecz użytkownika. Właściwą umową zatem będzie umowa o świadczenie usług. Przedmiotem umowy może być:

- korzystanie z jakiś konkretnych i gotowych do użycia aplikacji (SaaS czyli oprogramowanie jako usługa),

- udostępnienie platformy, tj. wirtualnego środowiska pracy na serwerach dostawcy gotowego na posadowienie rozwiązań własnych klienta (PaaS czyli platforma jako usługa) bądź

- udostępnienie wyłącznie warstwy sprzętowej i podstawowego oprogramowania jako infrastruktury informatycznej i jej utrzymywanie (IaaS czyli infrastruktura jako usługa).

- Ponadto, nieodłącznym elementem umowy o świadczenie usług chmurowych są postanowienia dotyczące obowiązków dostawcy w zakresie poziomu jakości usług (tzw. SLA - Service Level Agreement), określenie parametrów, dostępności danych, wydajności, i wsparcia w naprawie awarii.

Chmura z punktu widzenia użytkownika

Z punktu widzenia użytkownika chmura to możliwość korzystania z różnych przydanych usług i narzędzi (np. służących komunikacji, rejestrowaniu działań, prowadzeniu spraw), a ponadto jest to bezpieczna przestrzeń, która służy przechowywaniu danych (plików, dokumentów w sposób uporządkowany), tak jak serwer lub dysk.

W szczególności istotne jest, iż pełne korzystanie z zasobów w chmurze, możliwe jest wyłącznie pod warunkiem dostępu do sieci Internetowej choć

obecne rozwiązania dają możliwość używania chmury nawet w modelu nieciągłego dostępu do sieci. Cześć z usług umożliwia pracę również w momentach, kiedy nie mamy dostępu do Internetu. W takich przypadkach dane są synchronizowane automatycznie po odzyskaniu łączności.

Chmura w kancelarii prawnej

„Kancelaria prawna w chmurze czy chmura w kancelarii prawnej", tak brzmiał tytuł konferencji zorganizowanej przez KIRP. Co to tak naprawdę znaczy używać chmury obliczeniowej? Przede wszystkim, jak już wyżej zostało wskazane, chmura obliczeniowa daje dużą elastyczność, zatem to decyzja radcy prawnego prowadzącego kancelarię w jakim zakresie chce korzystać z tych usług.

Możliwych jest kilka sposobów wykorzystania zasobów, poniżej tylko przykładowe z nich:

- Wprowadzenie pełnej digitalizacji dokumentacji i elektronizacja kancelarii, zgodnie z zasadą „biuro bez papieru" (popularne w krajach anglojęzycznych jako „paperless office") - przy czym w Polsce, taki model w kancelarii radcy prawnego dziś właściwie nie jest możliwy, gdyż ze względu na otoczenie biznesowe, praktykę, ale i przepisy prawne nie da się uniknąć prowadzenia akt papierowych.

- Wprowadzenie częściowej digitalizacji lub dualizmu dokumentacji, czyli można powiedzieć, dążenie do modelu „paperless office" – zdaje się być formą najbardziej odpowiednią dla kancelarii prawnej. W tym modelu dokumentacja jest przez radcę przechowywana w formie cyfrowej (skanowanie poczty, skanowanie oryginałów dokumentów otrzymanych od klienta, zapisywanie dokumentów przesłanych przez Klienta e-mailem), a jednocześnie oprócz tego, w przypadku spraw procesowych nadal prowadzona jest dokumentacja papierowa. O ile, w znacznej mierze z klientem stosuje się już korespondencję mailową, możemy korzystać także z kwalifikowanego podpisu elektronicznego,[3] który ma skutek prawny, równoważny podpisowi własnoręcznemu, czynności prawne mogą być dokonywane w formie elektronicznej[4]

3 Kwalifikowany podpis elektroniczny wprowadzony Rozrządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), tzw. Rozporządzenie eIDAS."

4 Zgodnie z art 78 (1) Kodeksu Cywilnego; uwaga forma elektronicz-

i o ile postępowania administracyjne coraz częściej mogą być prowadzone elektronicznie, to co do zasady postępowania sądowe i administracyjnosądowe są nadal (w większości) prowadzone na piśmie. Ewentualnie, w sprawach procesowych bądź sprawach wyjątkowej wagi (np. postępowania karne, bądź inne wyjątkowo wrażliwe sprawy) radca prawny może wybrać prowadzenie wyłącznie dokumentacji papierowej i komunikację osobistą z Klientem.

- Korzystanie z przestrzeni chmury do przechowywania kopii zapasowych danych i archiwum kancelarii – radca prawny ma obowiązek zapewnić dostęp do danych i bezpieczeństwo danych; jedną z form jest tworzenie kopii zapasowych dokumentacji; kopie zapasowe mogą być np. odtworzone w przypadku zagubienia lub zniszczenia komputera, na którym znajdowały się dokumenty istotne dla prowadzonej przez radcę sprawy, przypadkowego usunięcia dokumentu podstawowego, zalania lub pożaru akt papierowych.

- Korzystanie z oprogramowania umieszczonego w chmurze – po pierwsze serwery poczty elektronicznej kancelarii mogą być umieszczone w przestrzeni chmury, a tym samym zwartość skrzynek może automatycznie zapisywać się w chmurze; po drugie dostawcy chmurowi mogą udostępniać także inne funkcjonalne dla prowadzenia biura narzędzia np. komunikatory, telefonię internetową, procesory tekstu, programy do tworzenia grafik i inne. Wszelkie dane powstałe w wyniku używania tych programów lub aplikacji przez kancelarię prawną zapisują się i są przechowywane w przestrzeni chmury obliczeniowej.

Ponadto, co niezwykle istotne, o ile udostępnienie ww. narzędzi odbywać się będzie często poprzez zamówienie tych usług wprost u dostawcy jako właśnie usług dostarczanych w tzw. modelu SaaS (Software as a Service), to jednak należy mieć na uwadze, iż inni producenci specjalistycznego oprogramowania lub aplikacji, z których korzysta radca prawny (np. dostawcy systemów informacji prawnej, księgowość, zarządzanie kancelarią, czy nawet poczta elektroniczna) mogą korzystać z zasobów chmurowych, własnych bądź innych dostawców, co również będzie oznaczać, iż nasze dane przechowywane są w chmurze.

Kluczowym jest zatem, aby wykonawca i dostawca jakichkolwiek usług bądź produktów ICT przedstawił jasną charakterystykę rozwiązania i ewentualnie potwierdził bądź zaprzeczył czy dane umieszczane przez radcę prawnego mogą znajdować się w chmurze obliczeniowej.

---

na, nie postać elektroniczna.

Chmura w kancelarii a główne problemy związane z etyką zawodową

Korzystanie z usług chmurowych jest coraz powszechniejsze w Polsce i to nawet w tych wrażliwych obszarach jak administracja publiczna, sektor ubezpieczeniowy czy bankowy. Można powiedzieć, iż rynek coraz bardziej przekonuje się do rozwiązań chmurowych.

Korzystanie z rozwiązań chmurowych w pracy radcy prawnego lub adwokata pomimo wielu zalet stanowi jednak swoiste wyzwanie z uwagi na obowiązki wynikające z zasad etyki zawodowej, w szczególności kwestie związane z tajemnica zawodową. Należy jednak w tym miejscu wyraźnie podkreślić, iż żadne przepisy prawa polskiego czy uchwał samorządów radcowskich nie zakazują korzystania z rozwiązań chmurowych.

Co więcej, już kilkukrotnie głos w sprawie rozwiązań chmurowych zabierała Rada Adwokatur i Stowarzyszeń Prawniczych Europy (Conseil des barreaux européens, „CCBE"), którego Krajowa Izba Radców Prawnych jest członkiem. CCBE w ramach konsultacji publicznych Komisji Europejskiej, jak i z własnej inicjatywy wydało kilka opinii i wytycznych w tym przedmiocie.

Stanowisko środowisk europejskich jak i pozaeuropejskich jest dość jasne – usługi chmury obliczeniowej do wykorzystania w pracy prawników powinny być dostępne i niosą za sobą wiele korzyści, jednakże decyzja o skorzystaniu z nich powinna być poprzedzona rzetelną analizą samego dostawcy, proponowanych rozwiązań i skonstruowania właściwej umowy z dostawcą. Innymi słowy model chmury obliczeniowej sam w sobie dla zawodów prawniczych nie jest nieodpowiedni, aczkolwiek nie każde rozwiązanie oferowane na rynku będzie dla takiej działalności wystarczająco bezpieczne.[5]

Na radcy prawnym ciąży obowiązek zachowania tajemnicy zawodowej w odniesieniu do wszelkich informacji uzyskanych w ramach świadczenia pomocy prawnej. Tajemnica jest głównym filarem zawodu radcy prawnego, stanowi podstawę zaufania klienta do radcy prawnego i właściwego świadczenia przez niego usług prawnych.[6]

5 CCBE, "Response regarding the European Commission Public Consultation on Cloud Computing" z 9 września 2011 oraz CCBE "Guidelines on the use of cloud computing services by lawyers" z 7 września 2012, wersja polska dostępna pod linkiem http://kirp.pl/wp-content/uploads/2017/08/2012-09-07-wytyczne-ccbe-w-zakresie-korzystania-przez-prawnikow-z-uslug-pracy-w-chmurze.pdf

6 Art. 3 ustawy z dnia 6 lipca 1982 r. o radcach prawnych oraz art. 9 Kodeksu Etyki Radcy Prawnego (dalej „KERP") (zgodnie z Uchwałą Nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22

Zgodnie z przepisami Kodeksu Etyki Radcy Prawnego („KERP")[7], radca prawny ma obowiązek zobowiązać osoby z nim współpracujące przy wykonywaniu czynności zawodowych do zachowania poufności, tj. przykładowo: asystentów, aplikantów, recepcjonistów, informatyków, księgowych.

Organy Krajowej Izby Radców Prawnych uchwalając aktualną treść KERP uznały, iż radca prawny nie jest w stanie w dzisiejszych czasach prowadzić kancelarii i wykonywać czynności zawodowych w pełni samodzielnie, musi współpracować z osobami, wobec których zobowiązanie do zachowania poufności wynikać będzie wyłącznie z zobowiązania kontraktowego.

Obowiązek ten przekłada się na stosunki kancelarii radcy prawnego z podmiotami zewnętrznymi takimi jak wynajmujący powierzchnię biurową dla kancelarii, serwis sprzątający, ochrona, kurierzy, zewnętrzne archiwum akt, itp. Wszystkie te podmioty w wyjątkowych okolicznościach z uwagi na uwarunkowania gospodarcze mogą pod pewnymi ściśle określonymi względami mieć dostęp do zasobów objętych tajemnicą zawodową i muszą być zobowiązane przez radcę prawnego do zachowania poufności w umowie.

Dostawca rozwiązania chmurowego z uwagi na to, iż może pod pewnymi względami również mieć dostęp do danych objętych tajemnicą radcowską i przechowywanych przez radcę w zasobach chmurowych (np. treść poczty czy tworzone pisma procesowe), także powinien być zobowiązany umownie do zachowania poufności i do wymagania, aby osoby pracujące na rzecz dostawcy były zobowiązane do zachowania poufności.

W istocie, tajemnica zawodowa w przypadku radców i adwokatów jest bezwzględna, wynika z ustawy, jest nieograniczona w czasie i rozległa w swojej materii, gdyż obejmuje wszystkie informacje, których radca dowiedział się w związku z prowadzeniem sprawy i jedynie wyjątkowo, w ściśle określonych sytuacjach może dojść do zwolnienia radcy prawnego z tajemnicy. Nie mniej jednak radca na osoby, z którymi współpracuje może wyłącznie nałożyć zobowiązanie wynikające z umowy. Osoby i podmioty te zawsze powinny być dobierane w sposób staranny przez radcę, jednakże nie ulega wątpliwości, iż takie podmioty trzecie zgodnie z przepisami prawa, zeznające np. jako świadek w sprawie bądź zobowiązane postanowieniem organów publicznych mogą ujawnić te informacje. Tak samo, powinien zostać zobowiązany dostawca chmurowy oraz jego personel, co będzie oznaczać, iż wyłącznie zobowiązanie organu publicznego lub sądu działającego na podstawie przepisów prawa może doprowadzić do ewentualnego ujawnienia danych. Sytuacja taka jednak nie różni się od umownego zobowiązania

listopada 2014 r. w sprawie Kodeksu Etyki Radcy Prawnego).

7 Art. 22 KERP

innych osób i podmiotów z otoczenia radcy prawnego.

Przy tym, istotne jest, aby podmiot ten podlegał prawu polskiemu lub innego kraju europejskiego oraz by dane zlokalizowane były w Unii Europejskiej (bądź ściślej Europejskiego Obszaru Gospodarczego), co wyłączy ewentualność dostępności innych organów z państw niezapewniających odpowiedniego poziomu praworządności bądź nie respektujących umów międzynarodowych do informacji objętych tajemnicą zawodową.

Jednak eliminację ewentualnej hipotetycznej możliwości dostępu dostawcy chmurowego i jego personelu może zapewnić wdrożenie szyfrowania danych. Zatem sorzystanie z rozwiązania szyfrującego zdaje się już w pełni obalać mit, związany z tym, iż chmura obliczeniowa zagraża tajemnicy zawodowej. Warto zatem taką możliwość rozważyć.

Ponadto, zgodnie z art. 23 KERP radca prawny zobowiązany jest przeciwdziałać wszelkim przypadkom niepowołanego ujawnienia informacji objętych tajemnicą zawodową, zniszczenia, zaginięcia lub zniekształcenia nośników tych informacji bądź innego zakłócenia dostępu lub działania tych nośników. W konsekwencji, do obowiązków radcy prawnego należy taki dobór osób i podmiotów zewnętrznych, z którymi współpracuje, aby na każdym etapie wykonywania jego czynności zapewniony był najwyższy poziom bezpieczeństwa dokumentów i nośników danych, rozumianego jako: zapewnienie dostępności, integralności, poufności, przeciwdziałanie wszelkim incydentom.

Konkludując, korzystanie z rozwiązań chmurowych przez radców prawnych i adwokatów nie jest jako takie zabronione. Przy doborze zatem rozwiązania chmurowego należy wziąć pod uwagę wiele czynników: postanowienia umowne jak i pozaumowne takie jak reputacja dostawcy, gwarancje zapewnienia odpowiedniego poziomu bezpieczeństwa.

Jak kancelaria rozwiązała kwestię obowiązków dotyczących sposobu świadczenia usług prawnych i zasad wynikających z etyki zawodowej oraz ustawy o radcach prawnych?

1.2 Odpowiedź na pytanie zadane podczas konferencji

Kancelaria Prawna Magnusson korzysta z rozwiązań chmurowych od 2012 roku, biuro warszawskie zaś wprowadziło rozwiązanie w kolejnych latach, przy czym nadal nie w sposób pełny. Prawnicy kancelarii nadal w sprawach procesowych prowadzą akta papierowe i prowadzą postępowania na piśmie.

Nie wszystkie dokumenty są także przechowywane na dysku chmurowym, a niektóre z dokumentów szczególnie wrażliwych są przechowywane wyłącznie w oryginale w specjalnie przeznaczonych do tego miejscach o podwyższonym stopniu zabezpieczeń i wysoce kontrolowanym dostępie. O ile, dla wspólników kancelarii jest jasnym, iż tajemnica zawodowa rozciąga się na całość dokumentów i informacji w identyczny sposób, to jednak dostrzega się, iż zróżnicowany stopień ryzyka występuje w zależności od:

- rodzaju dokumentów, w posiadanie których wchodzi prawnik,
- charakteru i doniosłości prowadzonych spraw,
- osoby klienta.

Generalnie, korzystanie z rozwiązania chmurowego, oprócz poczty jest postrzegane w kancelarii jako udogodnienie i raczej prawo do skorzystania, aniżeli obowiązek.

Przed wdrożeniem rozwiązania zostały przeprowadzone konsultacje w biurach Magnusson pod kątem możliwości korzystania z usług chmurowych dla zawodów prawniczych. Interpretacje i wytyczne niektórych samorządów europejskich oraz CCBE doprowadziły do przekonania, iż rozwiązanie to nie jest zabronione, a właściwie to dostrzega się wiele zalet. Nie każde jednak rozwiązanie chmurowe dostępne na rynku może być używane przez radców prawnych i adwokatów z różnych przyczyn.

Po zdiagnozowaniu potrzeb naszej kancelarii, rozpoczęliśmy porównywanie ofert różnych dostawców: od niewielkich polskich firm, po duże światowe korporacje. Jasnym było, iż stosowanie takiego rozwiązania stwarzać może pewne ryzyko, jednak celem kancelarii Magnusson było znalezienie kompromisu pomiędzy rozpoczęciem współpracy z podmiotem zewnętrzem, któremu powierzamy część danych kancelarii objętych tajemnicą zawodową, tajemnicą przedsiębiorstwa i stanowiących jednocześnie jedną z najbardziej wartościowych składników przedsiębiorstwa a standardami cyberbezpieczeństwa, zapewnienia ciągłości i dostępności usługi przy zapewnieniu zachowania poufności i kontroli

nad możliwością dostępu do danych.

Po szczegółowej analizie treści umów kilku wytypowanych dostawców, o wyborze jednego z nich przesądziło wreszcie postanowienie dotyczące możliwości wyboru lokalizacji przechowywania danych i możliwość zawężenia wyłącznie do terytorium EOG. Kilka lat temu, w czasie zawierania umowy, był to jedyny dostawca rangi światowej, który oferował takie rozwiązanie. Ponadto, Magnusson upewnił się, iż stroną umowy jest podmiot z siedzibą na terytorium UE, zatem ocenił, iż wszelkie ewentualne próby dostępu do danych przez organy państwa będzie odbywało się zgodnie z przewidywalnymi procedurami na podstawie przepisów prawa. Jednocześnie, umowa w sposób bardzo wyraźny podkreślała, iż właścicielem danym umieszczonych w przestrzeni chmury jest użytkownik i w ramach podstawowego świadczenia usług dostawca nie ma dostępu do danych. Dostawca zobowiązał także siebie i swój personel do zachowania poufności.

Ponadto w zakresie bezpieczeństwa Kancelaria była przekonana, iż nigdy nie będzie w stanie własnymi zasobami stworzyć środowiska zapewniającego poziom jakości usług IT powyżej 99% (SLA). Kancelaria oceniła, iż tak skonstruowana współpraca i wszelkie inne czynniki pozaumowne (reputacja podmiotu, certyfikacje, referencje) przewyższają standard bezpieczeństwa usług IT infrastruktury lokalnej zbudowanych wewnątrz kancelarii bądź świadczony w ramach outsourcingu przez jakikolwiek inny podmiot np. polski i zlokalizowany blisko siedziby kancelarii. Już na tym etapie kancelaria wzięła także pod uwagę skorzystania z rozwiązań szyfrujących dane, co eliminuje możliwość dostępu jakichkolwiek podmiotów trzecich w tym samego dostawcy.

W konsekwencji, usługi prawne świadczone przez Kancelarię przy pomocy rozwiązań chmurowych nie uchybiają żadnym przepisom dotyczącym zawodu radcy prawnego bądź adwokata ani odpowiednio ich zasad etyki zawodowej. Wręcz przeciwnie, Magnusson stoi na stanowisku, iż niektóre rozwiązania zwiększyły bezpieczeństwo przetwarzania danych objętych tajemnicą zawodową oraz znacznie ułatwiły pracę prawnikom.

1.3 Prelegenci i autorzy rozdziału

Wioletta Kulińska

Wioletta Kulińska jest adwokatem pracującym od 2012 roku w warszawskim biurze kancelarii Magnusson jako Associate.

Specjalizuje się w prawie własności intelektualnej, ochronie danych osobowych i nowych technologiach. Wioletta doradza w sprawach dotyczących znaków towarowych, nieuczciwej konkurencji, praw autorskich i nazw domen internetowych, a także w związku z naruszeniami, sporami, transakcjami, badaniami due diligence oraz wdrożeniami strategii dotyczących własności intelektualnej. Udziela klientom bieżących porad w powyższych sferach. Reprezentuje deweloperów i dystrybutorów oprogramowania, dostawców usług hostingowych i firmy outsourcingowe. Negocjuje umowy, przygotowuje propozycje kontraktów na rozwój i wdrażanie oprogramowania i umów typu SLA oraz wspiera klientów w kwestiach związanych z handlem elektronicznym.

Posiada bogate doświadczenie w doradztwie prawnym z zakresu ochrony danych osobowych na rzecz administratorów i podmiotów przetwarzających dane osobowe z różnych branż, reprezentuje klientów przed organami nadzoru i sądami administracyjnymi, przeprowadza audyty ochrony danych osobowych i bezpieczeństwa. Obecnie organizuje szkolenia i prowadzi projekty mające na celu przygotowanie klientów i wdrożenie w organizacjach przepisów tzw. RODO. Jest członkiem IAPP oraz ma uprawnienia CIPP/E (Certified Information Privacy Professional / Europe).

Adam Kotarbiński

Adam Kotarbiński jest menedżerem IT z ponad dwudziestoletnim doświadczeniem w zakresie nowych technologii i informatyki.

Od 2004 r. pełni funkcję Chief Information Officer w międzynarodowej kancelarii prawniczej Magnusson. Wcześniej w latach 2000-2004 kierował działem IT warszawskiego biura kancelarii prawniczej MAQS. Pracował również jako konsultant IT w Agencji Budowy i Eksploatacji Autostrad (obecnie GDDKiA).

Jego praca w Magnusson przypadła na okres dynamicznego rozwoju kancelarii: liczba prawników wzrosła od 50 do ponad 200, a zasięg działalności rozszerzył się z 3 do 12 krajów. Zainicjował oraz przeprowadził migrację struktur IT wszystkich biur kancelarii do modelu chmurowego. Sukces ten został przedstawiony w studium przypadku firmy Microsoft nt. wdrożenia Office 365 i Azure. Prowadzi szereg projektów z zakresu nowych technologii, w tym m.in. rozwiązań sieciowych. Pełni funkcję ABI w Magnusson. Jest członkiem IAPP oraz ma uprawnienia CIPP/E (Certified Information Privacy Professional / Europe).

Posiada wieloletnie doświadczenie w prowadzeniu projektów IT łączących nowoczesne technologie i zagadnienia prawnicze. Jest absolwentem Politechniki Warszawskiej (Wydział Elektroniki i Technik Informacyjnych). Wiedzę techniczną uzupełnił studiami z zakresu zarządzania (Executive MBA, Polska Akademia Nauk) oraz dyplomem magistra finansów i rachunkowości (Akademia Finansów i Biznesu Vistula). Ukończył kilkadziesiąt specjalistycznych szkoleń technicznych z zakresu sieci, serwerów, bezpieczeństwa oraz wdrożeń.

ROZDZIAŁ DRUGI

CHMURA - ASPEKTY TECHNICZNE

2

2.1 – Aspekty techniczne

Technologie informatyczne odgrywają co raz większą rolę w wykonywaniu zawodu radcy prawnego. Każdego dnia korzystamy już z informatycznych systemów dostępu do aktów prawnych, rozstrzygnięć sądowych i orzecznictwa. Monitorujemy status spraw korzystając z dostępu do portali dla pełnomocników, które są udostępniane przez sądy. Wszystkich tych czynności dokonujemy korzystając z różnych urządzeń: smartfonów, tabletów czy laptopów. Wielu radców prawnych korzysta już lub chciałoby skorzystać z rozwiązań chmurowych w ramach swojej praktyki. Oferują one szereg korzyści, takich jak przede wszystkim elastyczność, brak konieczności budowania i utrzymywania własnej infrastruktury IT, atrakcyjny koszt oraz dostęp do najnowszych zabezpieczeń. Z drugiej strony, wiążą się też z ryzykiem utraty kontroli nad przekazywanymi danymi i naruszeniem ich poufności.

Usługi chmurowe (cloud computing) – podstawowe pojęcia

Zgodnie z powszechnie uznawaną definicją National Institute of Standards and Technology (NIST), cloud computing czyli przetwarzanie danych w chmurze obliczeniowej to model umożliwiający dostęp z każdego miejsca, za pośrednictwem sieci i na żądanie, do współdzielonego zbioru konfigurowalnych zasobów komputerowych (np. sieci, serwerów, przechowywania, aplikacji i usług), który może być zapewniony szybko i jest dostępny przy minimalnym zaangażowaniu zarządzających lub interakcji z dostawcą usługi.

Usługi chmurowe charakteryzują się pięcioma podstawowymi cechami:

1. samoobsługa świadczona na żądanie (on-demand self-service)

użytkownik może w modelu samoobsługowym uzyskać moc obliczeniową, np. możliwość przechowywania w sieci, zgodnie z własnymi potrzebami i bez konieczności kontaktu z przedstawicielem dostawcy usługi

2. szeroki dostęp sieciowy (broad network access)

zasoby są dostępne za pośrednictwem sieci, przy wykorzystaniu standardowych mechanizmów i różnych urządzeń (np. smartfonów, tabletów, laptopów czy stacji roboczych)

3. składanie zasobów (resource pooling)

moce obliczeniowe i inne zasoby dostawcy usługi są dynamicznie przydzielane i zmieniane w zależności od potrzeb klientów

4. szybka elastyczność (rapid elasticity)

moce obliczeniowe i inne zasoby dostawcy usługi mogą być elastycznie przydzielane (zwiększane lub zmniejszane), w niektórych przypadkach automatycznie, aby zapewnić skalowalność odpowiadającą zapotrzebowaniu klientów;

5. mierzalność usługi (measured service)

systemy chmurowe pozwalają na automatyczną kontrolę i optymalizację wykorzystania zasobów poprzez możliwość pomiaru wykorzystania usługi (np. przechowywania, przetwarzania, aktywnych kont użytkowników). Zasoby mogą być monitorowane, kontrolowane i objęte raportowaniem, zapewniając przejrzystość zarówno dla dostawcy, jak i klienta.

Modele usług online

Usługi chmurowe są oferowane w trzech podstawowych modelach świadczenia usług:

IaaS (infrastruktura chmury jako usługa): w ramach tego modelu dostawca usług chmurowych umożliwia użytkownikowi korzystanie ze sprzętu informatycznego (hardware) za pośrednictwem Internetu. Może nim być np. przestrzeń na wirtualnym dysku internetowym przeznaczona do przechowywania danych albo też miejsce na serwerze wydzierżawione w celu wgrania tam własnego oprogramowania .

Przykładem zastosowania takiego modelu jest wykorzystanie wirtualnych serwerów w celu zlokalizowania na nich strony internetowej przygotowanej i obsługiwanej przez klienta. Innym przykładem mogą być wirtualne dyski w chmurze służące do przechowywania i dzielenia się plikami.

W tym modelu, dostawca usług chmurowych zapewnia jedynie infrastrukturę. Wykorzystanie, konfiguracja i obsługa systemów czy aplikacji zainstalowanych na takiej infrastrukturze jest po stronie użytkownika.

SaaS (oprogramowanie chmury jako usługa): w ramach tego modelu użytkownik ma możliwość korzystania z aplikacji udostępnianych przez dostawcę usług chmurowych.

Najczęstszym przykładem modelu SaaS są aplikacje biurowe, obejmujące pocztę elektroniczną, kalendarze, oprogramowanie umożliwiające edycję tekstów, arkusze kalkulacyjne, aplikacje do prowadzenia rozmów lub telekonferencji. Innymi przykładami mogą być specjalistyczne aplikacje do wyszukiwania informacji prawnej czy zarządzania kancelarią.

Ten model opiera się na zapewnianiu przez dostawcę usług chmurowych ciągłości działania usługi oraz ochronie i dostępności do danych, które użytkownicy przekazują do chmury. Dostawca usług chmurowych odpowiada za aktualizacje i rozwój oferowanego oprogramowania. Użytkownik musi zapewnić konfigurację oprogramowania odpowiadającą jego potrzebom (np. co do miejsca przechowywania jego danych, praw dostępu). Użytkownik nie ma kontroli nad systemami operacyjnymi czy serwerami na których uruchamiane są udostępniane mu aplikacje – pozostają one pod kontrolą dostawcy usług chmurowych

PaaS (platforma chmury jako usługa): usługa, w ramach której użytkownik uzyskuje dostęp do infrastruktury, a także do środowiska (w tym często do platformy programistycznej) będącego narzędziem do instalowania, uruchamiania i rozwijania aplikacji przez użytkownika. Użytkownik nie ma dostępu do systemu operacyjnego, na którym jest uruchomiona platforma, ani do przestrzeni dyskowej, na której są składowane dane. Użytkownik ma natomiast dostęp do aplikacji które instaluje, uruchamia czy rozwija oraz do danych zawartych w takich aplikacjach. Dodatkowo, użytkownik może mieć możliwość konfiguracji środowiska, z którego korzysta.

Przykładem modelu PaaS jest stworzenie środowiska testowego dla nowego systemu komputerowego, zainstalowanie na zasobach dostawcy usług

chmurowych systemu do obsługi księgowej przez podmiot świadczący takie usługi lub wykorzystanie platformy do przechowywania i uzyskiwania dostępu do archiwizowania dokumentów klienta.

W tym modelu, dostawca usług chmurowych nie odpowiada za funkcjonowanie i wsparcie rozwiązania, które użytkownik lokalizuje w chmurze. Usługi dotyczące wsparcia, SLA obsługi czy utrzymania systemu lub aplikacji lokalizowanych na platformie należą do użytkownika, a nie dostawcy usług chmurowych. Dostawca odpowiada za funkcjonowanie platformy.

Modele wdrożenia

Wyróżnia się cztery podstawowe modele wdrożenia usług chmurowych:

Chmura prywatna oznacza infrastrukturę informatyczną, która jest przeznaczona dla jednej organizacji. Jest ulokowana na terenie organizacji lub też jej zarządzanie zleca się na zewnątrz osobie trzeciej (zazwyczaj w drodze udostępniania wyspecjalizowanych usług w chmurze), która podlega rygorystycznej kontroli administratora danych.

Chmurę prywatną można porównać do standardowego ośrodka danych, który różni się jedynie tym, że ustalenia dotyczące technologii są wdrażane, by zoptymalizować wykorzystanie dostępnych zasobów i je wzmocnić za pośrednictwem małych inwestycji dokonywanych stopniowo i rozłożonych w czasie.

Chmura publiczna z kolei jest infrastrukturą pozostającą w posiadaniu dostawcy specjalizującego się w świadczeniu usług, który udostępnia, a zatem współdzieli swoje systemy z użytkownikami, podmiotami gospodarczymi lub organami administracji publicznej.

Usługi mogą być udostępnione za pośrednictwem Internetu, co niesie ze sobą przekazanie operacji przetwarzania danych lub samych danych do systemów dostawcy usług. Dostawca usług odgrywa zatem główną rolę pod względem skutecznej ochrony danych powierzonych jego systemom. Wraz z danymi,

użytkownik jest zobowiązany przekazać dużą część swojej kontroli nad tymi danymi .

Chmura hybrydowa, w których usługi są zapewniane przez prywatną infrastrukturę współistniejącą z usługami zakupionymi od chmur publicznych.

Chmura środowiskowa, w których infrastruktura informatyczna jest współdzielona przez kilka organizacji na rzecz społeczności konkretnego użytkownika (np. chmura stworzona i dzielona przez kancelarie prawne).

Wielu radców prawnych korzysta już lub chciałoby skorzystać z rozwiązań chmurowych w ramach swojej praktyki. Oferują one szereg korzyści, takich jak przede wszystkim elastyczność, brak konieczności budowania i utrzymywania własnej infrastruktury IT, atrakcyjny koszt oraz dostęp do najnowszych zabezpieczeń. Z drugiej strony, wiążą się też z ryzykiem utraty kontroli nad przekazywanymi danymi i naruszeniem ich poufności.

2.2 Prelegent i autor rozdziału

Michał Jaworski

Pracownik z najdłuższym stażem polskiego oddziału Microsoft, w którym pracuje od września 1994 roku, obecnie na stanowisku dyrektora ds. strategii technologicznej (ang. National Technology Officer). Pełni jednocześnie funkcję Członka Zarządu Microsoft sp. z o.o. (od 2013). Członek Grupy Roboczej ds. Ochrony Danych Osobowych przy Ministerstwie Cyfryzacji (2018). Przewodniczący Rady Polskiej Izby Informatyki i Telekomunikacji.

Odznaczony Srebrnym Krzyżem Zasługi za działania dla informatyzacji Polski (2012). Członek Rady Narodowego Centrum Badań i Rozwoju (2012-2016). Za popularyzację teleinformatyki i wkład w projekty społeczne nagradzany m.in. wyróżnieniem Prezydenta Aleksandra Kwaśniewskiego (2002), nagrodą “Infostar” (2009). Regularnie publikuje w „IT Professional” i „IT w Administracji”.

Współpracował z Institute for Prospective Technological Studies (IPTS) w Sewilli należącym do Joint Research Centre Komisji Europejskiej. Brał udział w projektach Interkl@asa i “Internet dla Szkół”. Pracował nad stworzeniem Strategii Rozwoju Społeczeństwa Informacyjnego dla Polski.

ROZDZIAŁ TRZECI

WDROŻENIE CHMURY W KANCELARII MAGNUSSON-WNIOSKI

3

3.1 – Efektywność

Efektywne rozwiązanie to takie, które będzie skuteczne, wydajne, niezawodne, szybkie i tanie. W niniejszej części skupimy się na analizie powyższych cech i spróbujemy udzielić odpowiedzi na pytanie: czy praca w chmurze zapewnia i zwiększa efektywność?

Niezwykłą przewagą przechowywania danych osobowych w chmurze jest to, iż dostęp do informacji, które zostały zapisane w chmurze zapewniony jest z każdego dowolnego miejsca na świecie pod warunkiem, połączenia z Internetem. Rozwiązanie chmurowe zapewnia dostęp do zasobów podczas nieobecności w biurze kancelarii, przebywania w delegacji, choroby, urlopu itp. Co więcej, nie jest przeszkodą korzystanie z innego komputera bądź innego urządzania aniżeli biurowy. Daje to zatem możliwość szybkiego rozwiązywania niespodziewanych problemów, zapewnienia ciągłości pracy i przekazywania sobie obowiązków pomiędzy prawnikami czy pracy bez przestojów, co z całą pewnością przekłada się na jakość świadczonej pomocy prawnej.

Ponadto, skuteczność i wysoką produktywność prawników można osiągnąć dzięki niektórym funkcjonalnościom oprogramowania chmurowego, czyli optymalne kosztowo i łatwo dostępne (na żądanie): komunikatory umożliwiające sprawną pracę na odległość, aplikacje do wideokonferencji, możliwość udostępniania plików w czasie rzeczywistym, współdzielenie plików, pracę kilku osób na jednym pliku jednocześnie. Wykorzystywanie tego typu narzędzi z pewnością pozwala oszczędzić czas prawnika, wpływa na zmniejszenie dystansu z klientem poprzez możliwość odbycia wideokonferencji, która coraz bardziej zbliża się do spotkań osobistych, eliminuje do minimum podróże i wyjazdy, a w konsekwencji obniża dodatkowe koszty związane z obsługą spraw. O ile takie same rozwiązania mogłyby być używane przez prawnika nie w formule chmury, a lokalnie, to jednak byłoby to niewydajne kosztowo.

Jeśli chodzi o niezawodność rozwiązań chmurowych, to oczywiście zależy ona od poziomu jakości zapewnianego przez dostawcę (SLA). Poziom ten określa się w procentach, im bliżej 100 % (czy raczej 99,999%) tym lepiej, jednak oczywiście wpływa to na cenę. Co do zasady, prawnicy powinni wybierać wyłącznie takie rozwiązania, które pozwalają im na pracę bez żadnych nieoczekiwanych przerw i awarii. Należy jednak przyznać, że możliwości kancelarii prawnej w zapewnieniu niezawodności systemu teleinformatycznego lokalnego własnymi zasobami i możliwości profesjonalnego dostawcy usług chmurowych są nieporównywalne w tym zakresie. Bezsprzecznie dostawca chmurowy jest w stanie zapewnić o wiele wyższy poziom bezusterkowości, a w konsekwencji efektywności pracy codziennej prawnika.

3.2 Odpowiedzi na pytania zadane podczas konferencji

Jakie główne argumenty przemówiły za wyborem rozwiązania chmurowego dla kancelarii?

Istotną kwestią, która przemówiła za wyborem rozwiązania chmurowego w Kancelarii Magnusson rozwiązań chmurowych jest skalowalność. Oznacza to, że przy rozwiązaniach chmurowych wielkość organizacji zazwyczaj nie ma znaczenia. Typowy model SaaS bazuje na ilości użytkowników i przygotowany jest tak, by działać już od jednego użytkownika. W typowych rozwiązaniach IT klasy enterprise (systemy cechujące się bardzo dużą wydajnością oraz zaawansowanymi funkcjami wspierającymi pracę) dużym problemem jest próg wejścia związany z koniecznością inwestycji początkowych. Klasyczne wdrożenia możliwe są zazwyczaj dopiero od pewnego poziomu wielkości organizacji, ponieważ poniżej tego progu są one nieefektywne lub nieopłacalne. W rozwiązaniach chmurowych otrzymujemy rozwiązanie z pełną funkcjonalnością niezależnie od skali zapotrzebowania. Co więcej, mamy możliwość jego powiększania albo zmniejszania w miarę naszych potrzeb. Możemy po prostu dobierać albo oddawać dostępy dla użytkowników, które są przez dostawce rozliczane zazwyczaj w okresach miesięcznych.

Kolejnym kluczowym atutem rozwiązań chmurowych jest bezpieczeństwo. Nakłady finansowe i osobowe potrzebne w dzisiejszych czasach do zapewniania właściwego poziomu bezpieczeństwa technicznego i sieciowego przerastają nawet duże i prężne organizacje. Dla dostawców usług chmurowych bezpieczeństwo techniczne, organizacyjne i sieciowe to absolutny priorytet, na tym opierają swoją działalność, dlatego też są skłonni ponosić bardzo wysokie koszty związane z gwarantowaniem odpowiednich poziomów zabezpieczeń. Dodatkowo, pomaga im efekt skali, ponieważ zapory i zabezpieczenia służą wielu klientom jednocześnie. Z perspektywy klienta – użytkownika chmury jest to wyjątkowo efektywne, ponieważ otrzymujemy wysoki poziom zabezpieczeń jako dodatek do właściwej usługi, której jesteśmy odbiorcą.

Kolejnym, argumentem przemawiającym za wyborem chmury do pracy w naszej kancelarii była kwestia kosztów, szczególnie analizowanych w stosunku do otrzymywanej jakości usług. W modelu SaaS usługi chmurowe są oferowane w rozwiązaniach abonamentowych bez żadnych opłat początkowych. Konkurencja rynkowa powoduje, że ceny są na akceptowalnym poziomie, a dostawcy usług dają możliwość wypowiedzenia subskrypcji przez klienta w rozsądnym, krótkim terminie.

Nie należy też pomijać kwestii związanej z czasem wdrożenia. W usługach

chmurowych nie ma typowego wdrożenia, usługi chmurowe, dzięki swojej standaryzacji są łatwo implementowane w organizacji. Oznacza to, że szybko i bez dużych nakładów własnych jesteśmy w stanie zacząć korzystać z usługi. Wielu rozwiązań możemy zacząć używać z dnia na dzień, bez wielkich zmian i szkoleń.

Chmura zdejmuje z nas obowiązek dbania o wiele aspektów technicznych, między innymi możemy zazwyczaj zapomnieć o konieczności robienia aktualizacji. Wynika to ze sposobu korzystania z rozwiązania, które powoduje, że obowiązki związane z utrzymaniem oprogramowania są po stronie dostawcy, a użytkownik tylko korzysta z usługi bazującej na tym oprogramowaniu.

Do czego kancelaria stosuje chmurę?

Podstawową usługą, z której korzysta nasza kancelaria w chmurze jest poczta elektroniczna. Jest to bardzo powszechne rozwiązanie. Wiele kancelarii już dzisiaj korzysta z takiego rozwiązania, nawet o tym nie wiedząc. W bardzo dużym uproszczeniu można powiedzieć, że każdy kto nie posiada własnego lokalnego serwera pocztowego, tylko korzysta z poczty u dostawcy usług, stosuje chmurę w swojej działalności.

Następnie, powszechnie wykorzystywaną usługą chmurową są rozwiązania do przechowywania plików. Mogą one mieć różną funkcjonalność, począwszy od osobistych dysków chmurowych, dających komfortowy dostęp do własnych plików z każdego urządzenia, jednocześnie gwarantując wysoki poziom bezpieczeństwa, po zawansowane systemy zarządzania dokumentami.

Specyfika pracy prawnika powoduje, że istotne jest bieżące rejestrowanie aktywności i czasu pracy. W tym zakresie rozwiązania chmurowe też są niezwykle pomoce. Przykładem może być system do wspomagania pracy pod nazwą LEX247 (który Kancelaria Magnusson pomaga współtworzyć i rozwijać), System ten umożliwia prowadzenie dziennika czasu pracy, a na kolejnych etapach raportowanie efektywności pracy i przygotowywanie rozliczeń dla klientów. System wspomaga przechowywanie dokumentów i prowadzenie komunikacji. Natomiast dzięki swojemu chmurowemu charakterowi współpracuje bezproblemowo, transparentnie z innymi usługami, nie komplikując użytkownikowi codziennych działań.

Ponadto, w dużej mierze wykorzystywanymi usługami w kancelarii są rozwiązania do komunikacji głosowej i wideokonferencji. W dzisiejszych czasach daje to niezwykły komfort i szybkość współpracy. Mamy możliwość porozumiewania się wygodnie i tanio. Wideokonferencje możemy prowadzić z komputera, telefonu

komórkowego czy tableta, a w przypadku braku sieci Internet, możemy dołączyć do spotkania przez zwykły telefon. Gdyby nie model chmurowy większość małych i średnich firm nie byłaby w stanie korzystać z tego typu rozwiązań ze względu na bardzo wysoki próg wejścia związany z dużymi inwestycjami początkowymi. Takie rozwiązania wymagają wysokowydajnych serwerów telekomunikacyjnych i zaawansowanej struktury sieciowej. Wdrażanie takiego rozważania lokalnie, w organizacji, która nie ma setek aktywnych użytkowników jest całkowicie nieefektywne. Model chmurowy to zmienia. Możemy mieć pełną funkcjonalność rozwiązania klasy enterprise dla jednego użytkowania przy bardzo niskiej opłacie miesięcznej.

Kolejną rodziną usług chmurowych, z których korzysta praktycznie już każda kancelaria, to systemy informacji prawnej, przy czym mało kto ma tę świadomość. Wchodząc na stronę usługodawcy, logując się do systemu by poszukać ustawy czy sprawdzić komentarze de facto używamy zasobów, które zamieszczone są w modelu chmurowym.

Wreszcie, rozwiązania chmurowe udogodniły w naszej kancelarii pracę grupową. Mamy narzędzia umożliwiające jednoczesne edytowanie dokumentów nie martwiąc się o wersje i kolejność, ponieważ na bieżąco widzimy zmiany innych autorów. Ma to szczególne znaczenie przy pracy na większych dokumentach, szczególnie w wieloosobowych zespołach albo przy pracy z klientem, który oczekuje bieżącego wglądu w pracę.

Zasoby chmurowe są istotnym elementem bezpieczeństwa lokalnej infrastruktury informatycznej, ponieważ stanowią nieskończony, z punku widzenia kancelarii, zasób na kopie awaryjne. Takie wykorzystanie zasobów chmurowych daje nam podniesienie lokalnego bezpieczeństwa dzięki posiadaniu kopii zapasowych w oddzielnej fizycznej lokalizacji dostępnej w szybki i łatwy sposób.

Jak przyjęli rozwiązanie prawnicy? Jakie były ich najczęstsze pytania? Obawy?

Prawnicy w szczególności zwracali uwagę na aspekty etyki zawodowej i wykonywania zawodu. Obawy, w momencie wdrażania rozwiązania w Polsce kilka lat temu dotyczyły bezpieczeństwa, gwarancji jakie dostawca daje w przypadku nieoczekiwanej utraty dokumentów. Ponadto, radcowie i adwokaci potrzebowali zrozumieć, jak działają rozwiązania, których będą używać oraz potrzebowali informacji na temat treści umowy zawieranej z dostawcą. Już na początku rozpoczęcia używania rozwiązań prawnicy dostrzegli ich zalety poczynając

od dostępności dokumentów z różnych urządzeń i także spoza biura, aż po możliwość samodzielnego organizowania i obsługi wideokonferencji z klientem i udostępnianie klientom dużych plików. Prawnicy szybko zauważyli, iż rozwiązania są proste, intuicyjne i faktycznie ułatwiają im pracę i oszczędzają czas. Nigdy też w naszej kancelarii nie mieliśmy żadnego incydentu związanego z bezpieczeństwem czy naruszeniem obowiązków dostawcy, brak jest też dostrzegalnych dla użytkownika przestojów czy awarii, zatem zaufanie do rozwiązania wzrasta.

Jak zareagowali klienci? Jakie były ich najczęstsze pytania? Obawy?

Kancelaria po przeprowadzonej analizie, nie odnotowała obowiązku uprzedniego informowania klientów o zmianie oprogramowania, tak jak nie informuje w szczegółach o zmianie dostawców innych usług czy o stosowanych środkach bezpieczeństwa. Niemniej nigdy tego faktu nie zatajała. Kancelaria pracuje w szczególności z osobami prawnymi i z przedsiębiorcami i raczej odnieść można było wrażenie, iż poprzednio stosowane rozwiązania informatyczne było niekompatybilne z klienckimi, mało elastyczne. Klienci często sami już od dawna korzystali z rozwiązań chmurowych. Nie został odnotowany żaden przypadek jakichkolwiek wątpliwości co do bezpieczeństwa Kancelarii Magnusson czy nadszarpnięcia zaufania do radców i adwokatów pracujących w kancelarii.

Jeśli chodzi o używane przez Kancelarię aplikacje niejednokrotnie klienci dostrzegali zwiększoną szybkość reakcji na zlecenia i zapytania klientów, wysoką dostępność prawników a w szczególności została przez naszych kilku klientów odnotowana redukcja dodatkowych kosztów obsługi (podróże, noclegi itp.).

Czy posiadanie chmury zwiększa przewagę konkurencyjną kancelarii?

Wbrew jeszcze nadal istniejącemu w niektórych kręgach mitowi, iż model chmury obliczeniowej jako takiej nie jest bezpieczny, nasza kancelaria miała zgoła odmienny odbiór zewnętrzny tego rozwiązania.

Coraz częściej zdarza się, iż w ramach procesu ofertowania czy postępowania przetargowego kancelaria jest obowiązana przedłożyć informacje związane ze specyfiką systemu IT oraz poinformować o środkach bezpieczeństwa. Jako, że ciężar niektórych elementów zapewnienia bezpieczeństwa (np. jak odporność

systemów, zapewnienie dostępności i ciągłości usług, poufności, fizyczne zabezpieczenia centrów danych) przeniosła na dostawcę usług chmurowych, to wiarygodność tego dostawcy i stosowany system jest brany pod uwagę podczas wyboru oferty. W jednym z postępowań nasza oferta została zaakceptowana jako ta, która prezentowała m.in. najwyższy poziom bezpieczeństwa, m.in. ze względu na rozwiązania chmurowe.

Na potrzeby przedłużenia polisy ubezpieczeniowej, niedawno ubezpieczyciel wymagał m.in. przedstawienia niektórych danych dotyczących systemu teleinformatycznego i środków zapewniających cyberbezpieczeństwo. W efekcie na plus zostały ocenione przez ubezpieczyciela używane systemy, czym kancelaria podwyższyła swoją wiarygodność i ocenę finalną.

Jakie procesy w kancelarii rozwiązanie chmurowe ułatwiło?

Rozwiązania chmurowe ułatwiają działania w wielu różnych obszarach codziennej pracy w Kancelarii Magnusson. Dostajemy możliwość dostępu do naszych danych z różnych urządzeń. W sposób bezpieczny możemy korzystać z naszych plików nawet na urządzeniach obcych. Usługi chmurowe dają zdecydowanie wygodniejsze możliwości komunikacji, zarówno wewnętrznej, jak i zewnętrznej.

Technologia chmurowa silnie wspiera proces rejestracji czasu pracy, raportowania i rozliczania pracy z klientem. Częściowo również automatyzuje procesy finansowo księgowe.

Mamy dostęp do niezbędnych informacji i baz danych wszędzie tam, gdzie mamy Internet. Możemy zapoznać się albo pobrać dokumenty, zapoznać się z komentarzami, sięgnąć do danych klienta w albo jego statystyk w naszej bazie, czy zrobić szybką weryfikację istnienia potencjalnego konfliktu interesów.

Rozwiązania chmurowe zdejmują z nas też wiele kwestii technicznych, które zajmują czas i zasoby ludzkie Uwalniając te zasoby możemy spokojniej i efektywniej pracować na rzecz klientów. Dopiero patrząc wstecz widzi się jak cześć rozwiązań było nieergonomicznych i jak dużo chmurowych, z pozoru drobnych i prozaicznych usług, dokonało rewolucji na polu efektywności codziennych działań.

Jakie elementy są do poprawy, zwrócenia szczególnej uwagi?

Korzystanie z usług chmurowych od strony organizacyjnej niesie podobne zagrożenia jak każde inne działanie związane z wprowadzaniem rozwiązań informatycznych do codziennej pracy. Należy działać systemowo i konsekwentnie. Praktyka pokazuje, że sprawdza się działanie bez szczegółowego, długoterminowego planowania. Dobre efekty przynosi wytyczanie kierunku zmian i określenie celu jaki chcemy osiągnąć. Następnie należy wprowadzać kolejne usługi, systematycznie, krok po kroku, bez rewolucji. Należy na bieżąco obserwować efekty jakie pojawiają się po uruchomieniu rozwiań i korygować problemy na bieżąco. Istotne jest by nie wprowadzać zbyt wielu nowości i zmian jednocześnie, ponieważ to zniechęca do korzystania z rozwiązania. Takie podejście próbowania i raczej ewolucji dają właśnie rozwiązania chmurowe.

Czy wprowadzenie rozwiązania chmurowego w jakiś sposób wpłynęło na zmianę oferty kancelarii?

Oferta Kancelarii nie zmieniła się znacznie w stosunku do tej sprzed wprowadzenia rozwiązań chmurowych, natomiast poprawiła się efektywność i komfort pracy. Dostrzegalne są oszczędności związane z maksymalnym wykorzystaniem narzędzi do porozumiewania się i pracy na odległość, czy to z klientami z różnych miejsc Polski, czy z zagranicy.

Takie narzędzia jak wygodne wideokonferencje dające możliwość udostępniania i edytowania plików w czasie rzeczywistym, przeprowadzanie szkoleń na odległość u klientów, udostępnianie dużych, zbyt ciężkich do wysyłki e-mailem plików na zewnątrz w bezpieczny sposób (np. przekazanie akt sprawy innemu prawnikowi w zastępstwie w innym mieście Polski).

Wcześniej koszty w tym zakresie, typu podróże, noclegi, wysyłki kurierów w trybie ekspresowym, były przewidzianym w ofercie kosztem klienta bądź ewentualnym kosztem dodatkowym kancelarii. Obecnie koszty te zostały zredukowane do minimum.

Ile czasu trwało wdrożenie rozwiązania?

W rozwiązaniach chmurowych zazwyczaj nie ma klasycznego wdrożenia, ponieważ usługa jako taka, jest już uruchomiona u dostawcy. Czas technicznego wdrożenia jest pomijalnie mały. Do wykonania pozostaje ustawienie funkcjonalności zgodnie z ustaleniami z dostawcą i wprowadzenie danych początkowych. Całość prac liczona jest w dniach, a czasami wręcz w godzinach. Istotny etap to początkowe testy i próby funkcjonalności usługi, to okresy zazwyczaj liczone w tygodniach. To, co dzisiaj składa się na czas wdrożenia to dwa elementy, analiza dostępnych rozwiązań wraz z wyborem dostawcy zwieńczone dobrą i zrównoważoną, zabezpieczającą interesy radcy prawnego umową oraz jednoczesne wyzwolenie zainteresowania użytkownika usługą, w takim stopniu, by zaczął z niej korzystać. Oczywiście to jest ogólne określenie wdrożenia rozwiązań chmurowych, a wiele zależy do wybranej usługi i dostawcy chmury. Tutaj, jednakże przedstawiamy typowe przypadki.

Ponadto, kolejną kwestią jest rozwój usług. Rozwiązania chmurowe ciągle się rozwijają, a w ślad za tym zaczynamy korzystać z kolejnych rozwiązań. Będąc w chmurze zmieniamy charakter naszego środowiska, stopniowo dostosowujemy i uzupełniamy nasze narzędzia do codziennej pracy w sposób prawie niezauważalny. Mamy efekt stałego rozwoju. Projekty zastępujemy procesem. Chmura staje się

naszym codziennym towarzyszem pracy i jest jak powietrze, niezauważalna, ale absolutnie niezbędna do prawidłowego działania, tak jak powietrze jest niezbędne do życia.

Co trzeba wziąć pod uwagę przy wyborze chmury?

Przede wszystkim warto w pierwszej kolejności sięgnąć do dwóch kluczowych dokumentów wydanych przez CCBE 9 września 2011 CCBE, które pomimo, iż zostały wydane w 2011 i 2012 roku zachowują swoją aktualność i były głównym punktem wyjścia także dla Kancelarii Magnusson. Rekomendujemy, aby procesu zdiagnozowania potrzeb prawnika, który interesuje się rozwiązaniami chmurowymi do wdrożenia we własnej kancelarii, porównania rozwiązań dostępnych na rynku oraz ofert dokonać najpierw ze specjalistą z zakresu IT. Należy biorąc pod uwagę charakter prowadzonych spraw i ewentualne narażenie na ryzyko w zakresie zainteresowania służb państwa bądź organów ścigania jak i koszty, podjąć decyzję czy chcemy wybrać chmurę publiczną, prywatną czy hybrydową.

Należy ponadto zbadać:

- Tożsamość dostawców, pod kątem ich wiarygodności na rynku tj. wypłacalność, polisy OC, czas funkcjonowania na rynku, referencje, posiadanie certyfikacji wynikających z uznawanych norm międzynarodowych (np. ISO) dotyczących zarządzania bezpieczeństwem, zarządzania jakością i zarządzania ryzykiem.

- Kwestie terytorialności, tj. siedzibę dostawcy, lokalizację centrów danych bądź możliwość wyboru tej lokalizacji, jurysdykcję i właściwe prawo w razie sporu z dostawcą,

Postanowienia umowne, a tutaj w szczególności: określenie, iż użytkownik (kancelaria) jest właścicielem danych, zobowiązanie do zachowania poufności przez dostawcę oraz jego personel, wyłączenie możliwości korzystania z podwykonawców bądź kontrola nad doborem podwykonawcy, zasady odpowiedzialności dostawcy za szkody, możliwość przeprowadzenia kontroli i audytu u dostawcy w zakresie stosowania postanowień umowy, sposób wypowiedzenia umowy oraz konsekwencje związane z bezpiecznym zwróceniem lub skasowaniem danych, zawarcie postanowień dotyczących powierzenia przez radcę prawnego jako administratora przetwarzania danych osobowych dostawcy usług chmurowych.

Rozwiązanie chmurowe: największa korzyść i największe ryzyko?

Z perspektywy osoby odpowiedzialnej za IT i bezpieczeństwo w kancelarii prawnej rozwiązania chmurowe radykalnie podnoszą poczucie spokoju i stabilność organizacji. Jest to efektem wysokiego bezpieczeństwa, przewidywalnego i wyważonego budżetu, a także samodzielnych i zadowolonych użytkowników.

Z kolei, prawnik-użytkownik dostrzega przede wszystkim szybkość, wygodę oraz dostępność usług i zasobów z jakiegokolwiek urządzenia i z jakiekolwiek miejsca pod warunkiem połączenia z Internetem, bez uszczerbku dla poszanowania zasad etyki wykonywania zawodu radcy lub adwokata. Kancelaria przy tym, może skupić się na pracy merytorycznej nie zużywając czasu i pieniędzy na kwestie związane z technologią i operacyjnością.

Istotnym zauważalnym ryzykiem jest zaś wybór niewłaściwego dostawcy. Aczkolwiek należy odnotować, iż takie ryzyko wiąże się z wyborem także innych osób współpracujących z radcą prawnym/adwokatem przy wykonywaniu czynności zawodowych.

Prawnicy powinni wybierać wyłącznie takie rozwiązania, które pozwalają im na pracę bez żadnych nieoczekiwanych przerw i awarii. Należy jednak przyznać, że możliwości kancelarii prawnej w zapewnieniu niezawodności systemu teleinformatycznego lokalnego własnymi zasobami i możliwości profesjonalnego dostawcy usług chmurowych są nieporównywalne w tym zakresie. Bezsprzecznie dostawca chmurowy jest w stanie zapewnić o wiele wyższy poziom bezusterkowości, a w konsekwencji efektywności pracy codziennej prawnika.

3.3 Prelegenci i autorzy rozdziału

Wioletta Kulińska

Wioletta Kulińska jest adwokatem pracującym od 2012 roku w warszawskim biurze kancelarii Magnusson jako Associate.

Specjalizuje się w prawie własności intelektualnej, ochronie danych osobowych i nowych technologiach. Wioletta doradza w sprawach dotyczących znaków towarowych, nieuczciwej konkurencji, praw autorskich i nazw domen internetowych, a także w związku z naruszeniami, sporami, transakcjami, badaniami due diligence oraz wdrożeniami strategii dotyczących własności intelektualnej. Udziela klientom bieżących porad w powyższych sferach. Reprezentuje deweloperów i dystrybutorów oprogramowania, dostawców usług hostingowych i firmy outsourcingowe. Negocjuje umowy, przygotowuje propozycje kontraktów na rozwój i wdrażanie oprogramowania i umów typu SLA oraz wspiera klientów w kwestiach związanych z handlem elektronicznym.

Posiada bogate doświadczenie w doradztwie prawnym z zakresu ochrony danych osobowych na rzecz administratorów i podmiotów przetwarzających dane osobowe z różnych branż, reprezentuje klientów przed organami nadzoru i sądami administracyjnymi, przeprowadza audyty ochrony danych osobowych i bezpieczeństwa. Obecnie organizuje szkolenia i prowadzi projekty mające na celu przygotowanie klientów i wdrożenie w organizacjach przepisów tzw. RODO. Jest członkiem IAPP oraz ma uprawnienia CIPP/E (Certified Information Privacy Professional / Europe).

Adam Kotarbiński

Adam Kotarbiński jest menedżerem IT z ponad dwudziestoletnim doświadczeniem w zakresie nowych technologii i informatyki.

Od 2004 r. pełni funkcję Chief Information Officer w międzynarodowej kancelarii prawniczej Magnusson. Wcześniej w latach 2000-2004 kierował działem IT warszawskiego biura kancelarii prawniczej MAQS. Pracował również jako konsultant IT w Agencji Budowy i Eksploatacji Autostrad (obecnie GDDKiA).

Jego praca w Magnusson przypadła na okres dynamicznego rozwoju kancelarii: liczba prawników wzrosła od 50 do ponad 200, a zasięg działalności rozszerzył się z 3 do 12 krajów. Zainicjował oraz przeprowadził migrację struktur IT wszystkich biur kancelarii do modelu chmurowego. Sukces ten został przedstawiony w studium przypadku firmy Microsoft nt. wdrożenia Office 365 i Azure. Prowadzi szereg projektów z zakresu nowych technologii, w tym m.in. rozwiązań sieciowych. Pełni funkcję ABI w Magnusson. Jest członkiem IAPP oraz ma uprawnienia CIPP/E (Certified Information Privacy Professional / Europe).

Posiada wieloletnie doświadczenie w prowadzeniu projektów IT łączących nowoczesne technologie i zagadnienia prawnicze. Jest absolwentem Politechniki Warszawskiej (Wydział Elektroniki i Technik Informacyjnych). Wiedzę techniczną uzupełnił studiami z zakresu zarządzania (Executive MBA, Polska Akademia Nauk) oraz dyplomem magistra finansów i rachunkowości (Akademia Finansów i Biznesu Vistula). Ukończył kilkadziesiąt specjalistycznych szkoleń technicznych z zakresu sieci, serwerów, bezpieczeństwa oraz wdrożeń.

O Z D Z I A Ł C Z W A R T Y

KORZYSTANIE Z CHMURY PRZEZ PRAWNIKÓW - KWESTIE PODSTAWOWE


CHMURA

4.1 Korzyści i ryzyka

Każda technologia niesie ze sobą korzyści, ale staje się źródłem zagrożeń. Nawet przy stosowaniu typowych rozwiązań informatycznych, prawnicy byli i są narażeni na ataki z użyciem złośliwego oprogramowania czy utratę poufności danych. Rozwiązania chmurowe oferują prawnikom szereg korzyści, ale jak każde rozwiązanie informatyczne, wiążą się też z określonymi ryzykami.

Do najczęściej wskazywanych korzyści korzystania z usług chmurowych zalicza się:

- możliwość skalowania zasobów na żądanie
- efektywność kosztową
- dostęp do najnowszych wersji oprogramowania, automatyczne aktualizacje i usuwanie usterek
- brak konieczności inwestycji w sprzęt (hardware)
- bezpieczeństwo (rozproszenie danych, zarządzanie aktualizacjami, bezpieczeństwo fizyczne, kopie danych)
- niezwłoczna dostępność do rozwiązań oferowanych globalnie (brak „zacofania technologicznego) - dostęp do usług o wysokiej jakości
- współdzielenie odpowiedzialności z dostawcą usług chmurowych, np. przy przetwarzaniu danych osobowych

Wśród najczęstszych ryzyk związanych z korzystaniem z usług chmurowych wymienia się:

- ryzyko naruszenia tajemnicy radcowskiej
- nieuprawniony dostęp organów państwowych (w tym państw trzecich) do danych przechowywanych w chmurze
- silne związanie się z dostawcą usługi
- brak dostępu do danych (przerwy w ciągłości działania)
- utratę kontroli nad danymi i zarządzaniem aplikacjami w modelu SaaS
- brak kontroli nad rozwojem oprogramowania w modelu SaaS.

Poniżej przedstawimy okoliczności, które warto rozważyć przy dokonywaniu oceny technologii chmurowych aby doprowadzić do zmniejszenia ryzyk i w maksymalny sposób wykorzystać zalety chmury obliczeniowej.

4.2 Obowiązki radcy prawnego w zakresie zachowania tajemnicy zawodowej

Wszystkie opisane poniżej obowiązki radcy prawnego pozostają w mocy bez względu na rodzaj wykorzystywanej technologii IT.

Zachowanie odpowiedniego poziomu staranności

Radca prawny ma obowiązek wykonywania czynności zawodowych sumiennie oraz z należytą starannością uwzględniającą profesjonalny charakter działania

Tajemnica radcowska

Obowiązek zachowania tajemnicy zawodowej przez radcę prawnego stanowi fundament relacji między radcą prawnym a klientem.

Zgodnie z art. 3 ust. 3 ustawy z dnia 6 lipca 1982 o radcach prawnych („Ustawa o Radcach Prawnych”)[1], radca prawny jest zobowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Obowiązek ten nie może być ograniczony w czasie i istnieje również po zaprzestaniu wykonywania zawodu.

Kodeks Etyki Radcy Prawnego, który stanowi załącznik do uchwały nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców prawnych z dnia 22 listopada 2014 r. („Kodeks Etyki”), stanowi, że:

- radca prawny powinien zachować w tajemnicy wszystkie informacje dotyczące klienta i jego spraw, ujawnione radcy prawnemu przez klienta bądź uzyskane w związku z wykonywaniem przez niego jakichkolwiek czynności zawodowych, niezależnie od źródła tych informacji oraz formy i sposobu ich utrwalenia (art. 15 ust. 1;

- tajemnica zawodowa obejmuje również wszelkie tworzone przez radcę prawnego dokumenty oraz korespondencję radcy prawnego z klientem i osobami uczestniczącymi w prowadzeniu sprawy - powstałe dla celów związanych ze świadczeniem pomocy prawnej (art. 15 ust. 2)

1 T. j. Dz. U. z 2017 r. poz. 922

- obowiązek zachowania tajemnicy obejmuje zakaz ujawniania informacji i dokumentów, oraz zakaz korzystania z nich w interesie własnym lub innej osoby, chyba że przepisy prawa lub Kodeksu stanowią inaczej (art. 16).

Z obowiązku zachowania tajemnicy zawodowej, wynikają dodatkowe zobowiązania radcy prawnego dotyczące:

- zobowiązania osób współpracujących z nim przy wykonywaniu czynności zawodowych do zachowania poufności w zakresie objętym jego tajemnicą zawodową (art. 22) oraz

- obowiązek zabezpieczenia przed niepowołanym ujawnieniem wszelkich informacji objętych tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia. Dokumenty i nośniki zawierające informacje poufne należy przechowywać w sposób chroniący je przed zniszczeniem, zniekształceniem lub zaginięciem. Dokumenty i nośniki przechowywane w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych. Radca prawny powinien kontrolować dostęp osób współpracujących do takich dokumentów i nośników (art. 23).

Dodatkowo, w przypadku wykonywania zawodu, pozyskiwania klientów czy wykonywania czynności zawodowych drogą elektroniczną, radca prawny powinien:

- zabezpieczać poprzez okresową archiwizacją i dbać o dostępność danych przetwarzanych drogą elektroniczną (art. 35 pkt. 6);

- chronić tajemnicę zawodową, informując w treści korespondencji elektronicznej o jej poufnym charakterze; zabezpieczenie uznaje się za należyte jeśli klient po uprzednim poinformowaniu go o zagrożeniach związanych z korzystaniem z drogi elektronicznej, domyślnie lub wyraźnie zaakceptował stosowane w komunikacji z nim środki, techniki, sposoby, systemy lub standardy komunikacji elektronicznej (art. 35 pkt 7).

4.3 Obowiązki radcy prawnego w zakresie ochrony danych osobowych

Zakres praw i obowiązków radcy prawnego w procesie przetwarzania danych osobowych zależy od jego roli w tym procesie. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO")2 wyróżnia dwa główne typy podmiotów zaangażowanych w operacje dokonywane na danych osobowych: administratora i podmiot przetwarzający. Administratora i przetwarzającego wyróżniała również ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, której wskazane przepisy nadal obowiązują w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady 2016/681 z 27 kwietnia 2016 r[3].

Administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Podmiotem przetwarzającym jest natomiast osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO).

> *Radca prawny (kancelaria) jest bez wątpienia administratorem danych swoich pracowników, które przetwarza w celach związanych ze stosunkiem pracy, w tym wypłaty wynagrodzeń czy przeprowadzanych ocen pracownika. Radca prawny jest też administratorem danych osobowych swoich klientów, które przetwarza co do zasady w celu wykonania umowy. Takie dane mogą być też przetwarzane w innych celach, w tym w celach informacyjnych (np. w przypadku przesyłania newsletterów, zaproszeń na organizowane konferencje lub informacji o zmianach w przepisach).*

Natomiast rola radcy prawnego w procesie przetwarzania danych osobowych pozyskiwanych od klienta lub w związku z doradztwem dla klienta

2 Dz. U. UE L 119 z 4.5.2016, s. 1

3 Zob. art. 175 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 poz. 1000)

budziła w przeszłości pewne kontrowersje. Wynikały one przede wszystkim z niejasnych decyzji Generalnego Inspektora Ochrony Danych Osobowych z 2005 r., które z jednej strony wskazywały że jest on przetwarzającym, a z drugiej – odwoływały się do podstaw przetwarzania danych przez radcę prawnego jako administratora i określały go terminem „odbiorcy danych"[4].

Na gruncie tych decyzji oraz Ustawy o ochronie danych osobowych z 1997 r. część doktryny prezentowała stanowisko, że status radcy prawnego z perspektywy przepisów o ochronie danych osobowych zależał od okoliczności sprawy[5]. Jeżeli radca prawny albo kancelaria prowadzili dla klienta postępowanie sądowe lub uczestniczyli w badaniu prawnym i w ramach tych działań sami podejmowali decyzje o celach i środkach przetwarzania danych osobowych (np. pozyskiwali dane potencjalnych świadków oraz określali, w jaki sposób i kiedy je wykorzystać), to byli administratorem danych. Jeżeli natomiast przetwarzali dane osobowe przekazane przez klienta wyłącznie w ramach jego instrukcji (np. w celu przygotowania opinii prawnej w oparciu o dane klienta), wówczas pełnili rolę przetwarzającego.

Obecnie, na gruncie RODO, powyższe wątpliwości zostały jednak rozstrzygnięte na rzecz stanowiska, że kancelaria radcy prawnego ma status administratora danych z uwagi na swoją niezależność przy świadczeniu usług prawnych oraz obowiązek zachowania tajemnicy zawodowej.

Jak wynika z poniżej wskazanych dokumentów, powyższą konkluzję podzieliła zarówno Grupa Robocza Art. 29, organy ochrony danych osobowych i samorządu radców prawnych oraz polski ustawodawca:

- ze stanowiska Grupy Roboczej Art. 29 (Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of „controller" and „processor" adopted on 16 February 2010 (WP 169)) oraz stanowiska brytyjskiego Information Commissioner's Office[6] wynika, że prawnicy powinni być kwalifikowani jako administratorzy danych, ze względu na specyfikę świadczonych przez nich usług obsługi prawnej. Specyfika ta wynika przede wszystkich z niezależności prawników oraz z tego, że prawnicy podejmują decyzje, jakie informacje są im potrzebne do

4 Decyzja z dnia 2 sierpnia 2005 r. (GI-DEC-DS.-233/05)

5 J. Barta, Ustawa o ochronie danych osobowych. Komentarz do art. 31, 2016, Legalis; P. Poniatowski, Ochrona danych osobowych przetwarzanych przez adwokatów, Studia Iuridica Lublinensia, vol. XXVI, 2, 2017, s.89-91.

6 https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

wykonania usługi oraz są odpowiedzialni za treść porady;

- z zestawienia wyników kontroli, które GIODO przeprowadził w 2016 r. w wybranych dziesięciu kancelariach prawnych, w tym w jednej, korzystającej z usług przetwarzania w chmurze obliczeniowej, wynika, że radcowie prawni przetwarzają dane osobowe na podstawie bezwzględnie obowiązujących przepisów prawa (Ustawa o Radcach Prawnych) oraz na podstawie przepisów korporacyjnych[7], co wskazuje na zakwalifikowanie ich jako administratorów danych osobowych;

- z przewodnika dla radców prawnych i adwokatów opublikowanego przez organy samorządu radców prawnych i adwokatów wynika, że radcy prawni i adwokaci wykonujący zawód w kancelariach są administratorami danych niezależnie od rodzaju zlecenia, natomiast w przypadku adwokatów i radców wykonujących zawód spółkach np. komandytowych, partnerskich, administratorami danych są spółki[8];

- również z aktualnego projektu ustawy wprowadzającej ustawę o ochronie danych osobowych, która wprowadza zmiany do ustawy z dnia 6 lipca 1982 r. o radcach prawnych oraz ustawy z 26 maja 1982 r. o adwokaturze wyłączające niektóre uprawnienia osób, których dane dotyczą w odniesieniu do przetwarzania ich danych przez radców prawnych i adwokatów[9] wynika wprost, że polski ustawodawca traktuje kancelarie jako administratora danych.

---

7 Zestawienie wyników kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzonych w kancelariach prawnych, Warszawa, 2017, http://www.giodo.gov.pl/pl/1520291/9847

8 http://www.adwokatura.pl/admin/wgrane_pliki/file-poradnik--dla-radcow-prawnych-i-adwokatow-ogolne-rozporzadzenie-o-ochronie--danych-rodo-22897.pdf. , s. 27-30

9 https://legislacja.rcl.gov.pl/projekt/12302951/katalog/12457737#12457737

Powyższe oznacza to że kancelaria będzie administratorem danych w odniesieniu do wszelkich danych pozyskanych w ramach współpracy z Klientem, niezależnie od tego czy otrzymuje dane od Klienta w ramach zlecenia czy zbiera takie dane samodzielnie na zlecenie Klienta. Warto zwrócić uwagę, że w przypadku powierzenia przetwarzania danych, podmiot przetwarzający jest związany instrukcjami administratora. Z taką sytuacją nie mamy do czynienia w przypadku kancelarii prawnej. Kancelaria prawna jest niezależna w swojej ocenie i nie jest związana instrukcjami administratora. Nie ma zatem wątpliwości, że nie przetwarza ona danych osobowych w imieniu i zgodnie z instrukcjami Klienta, ale jest odrębnym administratorem danych osobowych przetwarzanych w związku ze świadczeniem usług prawnych na rzecz Klienta.

Należy zwrócić też szczególną uwagę na relację między przepisami o ochronie danych osobowych i dotyczącymi obowiązku zachowania tajemnicy zawodowej.

Zgodnie z art. 5 Ustawy o ochronie danych osobowych z 1997 r.[10], jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw. W związku z powyższym, w zakresie w jakim ustawa o radcach prawnych lub Kodeks Etyki przewiduje dalej idącą ochronę danych osobowych klientów (tj. w zakresie dotyczącym zachowania tajemnicy zawodowej) pierwszeństwo mają przepisy ustawy o radcach prawnych i Kodeks Etyki. W zakresie nie uregulowanym przez te regulacje, należy stosować przepisy o ochronie danych osobowych. Dotyczy to w szczególności, kwestii powierzania przetwarzania danych osobowych[11].

10 Zob. również motyw (164) i art. 90 RODO, który przewiduje, że w zakresie uprawnień kontrolnych organów nadzorczych ochrony danych osobowych, państwa członkowskie mogą przyjąć przepisy szczegółowe mające chronić obowiązek zachowania tajemnicy zawodowej, o ile jest to niezbędne by pogodzić prawo do ochrony danych osobowych z obowiązkiem zachowania tajemnicy zawodowej.

11 J. Barta, jw.

Ustawa o radcach prawnych oraz Kodeks Etyki zobowiązują radców prawnych do ochrony informacji stanowiących tajemnicę radcowską. Niniejsze wskazówki mają pomóc radcom prawnym przy podejmowaniu decyzji o korzystaniu z usług chmurowych. Taką decyzję radca prawny musi jednak podjąć samodzielnie, po przeanalizowaniu wszystkich zalet i wad takiego rozwiązania w jego konkretnej sytuacji.

4.4 RODO

Wymogi wynikające z RODO oraz polskich przepisów uzupełniających RODO (ustawy o ochronie danych osobowych oraz przepisów wprowadzających) mogą być pewnym wyzwaniem dla radców prawnych. Do maja 2018 r. wiele podmiotów koncentrowało się na dostosowaniu do tych regulacji, przesyłając informacje o przetwarzaniu danych lub weryfikując własne procesy przetwarzania i bazy danych. Należy jednak pamiętać, że zapewnianie zgodności z RODO jest procesem ciągłym i nie kończy się w momencie przyjęcia procedur czy dostosowania istniejących operacji przetwarzania danych do RODO w chwili jego wejścia w życie.

O RODO często wspomina się w kontekście kar finansowych i odpowiedzialności karnej jakie mogą grozić za naruszenie jego przepisów. Należy jednak pamiętać, że celem RODO jest zapewnienie wysokiego i spójnego stopnia ochrony osób fizycznych oraz usunięcie przeszkód w przepływie danych osobowych w Unii. Osiągnięcie tych celów niewątpliwie będzie korzystne dla radców prawnych, czy to z perspektywy możliwości świadczenia przez niego usług prawnych, jak i zaufania klientów do radców chroniących ich dane osobowe. Radca prawny powinien zatem w toku całej swojej działalności brać pod uwagę cele i zasady wynikające z RODO.

Z perspektywy codziennej praktyki, w szczególności następujące działania mogą ułatwić radcom prawnym zgodne z RODO przetwarzanie danych osobowych:

- przeprowadzenie oceny jakie dane osobowe są przetwarzane przez radcę prawnego lub będą przez niego przetwarzane i w jakim charakterze (administrator/przetwarzający);

- ustalenie właściwych podstaw przetwarzania danych osobowych – jako administrator, radca prawny nie może dowolnie zmieniać podstaw przetwarzania danych, dlatego ustalenie właściwej podstawy prawnej na początku przetwarzania jest niezwykle istotne. Przykładowo, jeżeli radca prawny przetwarza dane na podstawie zgody, osoby której dane dotyczą, po odwołaniu tej zgody nie może zdecydować, że przetwarza dalej dane tej osoby w celu wykonania umowy zawartej z taką osobą;

- dokonanie przeglądu i weryfikacji danych przetwarzanych w celach marketingowych np. ustalenie czy w świetle pozyskanych zgód oraz przekazanych informacji nadal może wysyłać newslettery lub inne materiały marketingowe, czy też konieczne jest dokonanie dodatkowych czynności (np. uzyskanie zgody, przekazanie uzupełniających informacji itp.);

- dokonanie przeglądu papierowych baz danych osobowych oraz rozwiązań IT w których przetwarzane są dane pod kątem spełniania wymogów RODO, w tym w zakresie ochrony danych;

- przygotowanie klauzul informacyjnych dotyczących przetwarzania danych np. do umów z pracownikami i współpracownikami, do umów z klientami czy na stronę internetową (w zakresie nie objętym wyłączeniami);

- przygotowanie się do realizacji wniosków osób, których dane dotyczą;

- przygotowanie się do ewentualnego zgłaszania naruszenia ochrony danych osobowych;

- przygotowanie wewnętrznych rejestrów czynności przetwarzania danych;

- podjęcie decyzji, czy powoływać inspektora ochrony danych osobowych;

- przeszkolenie pracowników i współpracowników;

- przeanalizowanie, czy dane są przekazywane poza Unię Europejską i jeśli tak, czy wdrożone zostały środki ochrony danych;

- przeprowadzenie oceny, czy w przypadku powierzania przetwarzania danych osobowych przez lub do radcy prawnego zostały zawarte umowy o powierzeniu przetwarzania zgodne z RODO;

- opracowanie zasad usuwania danych osobowych.

Radcowie prawni działają w różnych organizacjach i w różnej skali, w tym jako prawnicy w przedsiębiorstwach lub organach administracji, jednoosobowych lub niewielkich kancelariach po kilkudziesięcioosobowe kancelarie. W przypadku mniejszych organizacji, może być podnoszony argument, że zakres obowiązków nakładanych przez RODO jest nieproporcjonalnie wysoki. Należy jednak pamiętać, że często w takim przypadku przetwarza się mniej danych oraz korzysta z mniejszej ilości systemów IT. Wybór właściwego rozwiązania IT w powiązaniu ze świadomością spoczywających na radcy prawnym obowiązków pozwoli nawet takim niewielkim organizacjom na przetwarzanie danych zgodnie z RODO.

4.5 Wytyczne Rady Adwokatur i Stowarzyszeń Prawniczych Europy

Korzystanie z usług dostępnych w chmurze obliczeniowej było i jest ciągle przedmiotem wielu analiz organizacji zrzeszających prawników. Na gruncie europejskim warto zwrócić uwagę na następujące dokumenty wydane przez Radę Adwokatur i Stowarzyszeń Prawniczych Europy (CCBE):

- wytyczne w zakresie korzystania przez prawników z usług pracy w chmurze z dnia 7 września 2012 r.[12], oraz

- praktyczne wskazówki w zakresie poprawy bezpieczeństwa teleinformatycznego prawników przed bezprawnym nadzorem opublikowane w maju 2016 r.[13]

Wytyczne CCBE dotyczące usług chmurowych zostały opublikowane przeszło pięć lat temu, co w dobie dynamicznie rozwijających się technologii jest bardzo długim okresem. W wielu obszarach, takich jak konieczność ustalenia wiarygodności dostawcy, wrażliwości danych, wybrania modelu usługi pozostają one w dużej części aktualne. Szerszego spojrzenia wymagać mogą jednak pewne aspekty umowne wskazywane przez CCBE. Tytułem przykładu, oczekiwanie aby umowa regulowała dostarczenie kodu źródłowego oprogramowania chmurowego (software escrow) w sytuacji niewypłacalności lub niezdolności biznesowej usługodawcy do świadczonych usług będzie trudne do spełnienia w przypadku standardowego, masowo stosowanego oprogramowania chmurowego oferowanego przez największe firmy informatyczne i niewielkich, często jednoosobowych, kancelarii prawnych, które chciałyby z nich korzystać. Rygorystyczne przestrzeganie tej rekomendacji mogłoby całkowicie zablokować korzystnie ze standardowych aplikacji chmurowych. Alternatywą dla takiego wymogu będzie zweryfikowanie wiarygodności dostawcy oraz zapewnienie sobie możliwości zwrotu danych po zakończeniu korzystania z usługi.

12 https://www.oirpwarszawa.pl/wytyczne-ccbe-w-zakresie-korzystania-przez-prawnikow-z-uslug-pracy-w-chmurze/
13 http://www.oirpwarszawa.pl/bezpieczenstwo-teleinformatyczne--prawnikow/

O RODO często wspomina się w kontekście kar finansowych i odpowiedzialności karnej, jakie mogą grozić za naruszenie jego przepisów. Należy jednak pamiętać, że celem RODO jest zapewnienie wysokiego i spójnego stopnia ochrony osób fizycznych oraz usunięcie przeszkód w przepływie danych osobowych w Unii. Osiągnięcie tych celów niewątpliwie będzie korzystne dla radców prawnych, czy to z perspektywy możliwości świadczenia przez niego usług prawnych, jak i zaufania klientów do radców chroniących ich dane osobowe.

4.6 Prelegenci i autorzy rozdziału

Agata Szeliga

Agata Szeliga jest radcą prawnym a od 2009 r. partnerem w kancelarii Sołtysiński Kawecki & Szlęzak.

Kieruje praktykami zajmującymi się prawem ochrony danych i prywatności oraz pomocy publicznej i zamówień publicznych. Reprezentuje klientów zarówno przed organami polskimi (sądami, organami administracji, w tym przed regulatorami – UODO i jego poprzednikiem GIODO oraz UKE), jak i przed Komisją Europejską.

W ramach praktyki prawa ochrony danych osobowych i prywatności zajmuje się w szczególności, przygotowywaniem umów i innych dokumentów w zakresie danych osobowych, analizą struktur biznesowych pod kątem zgodności z przepisami dotyczącymi ochrony danych osobowych, reprezentowaniem w postępowaniach dotyczących danych osobowych.

Realizowała również szereg projektów doradczych w zakresie licencjonowania i wdrażania oprogramowania oraz świadczenia usług związanych z oprogramowaniem, w tym dotyczących „cloud computing" oraz blockchain.

Renata Zalewska

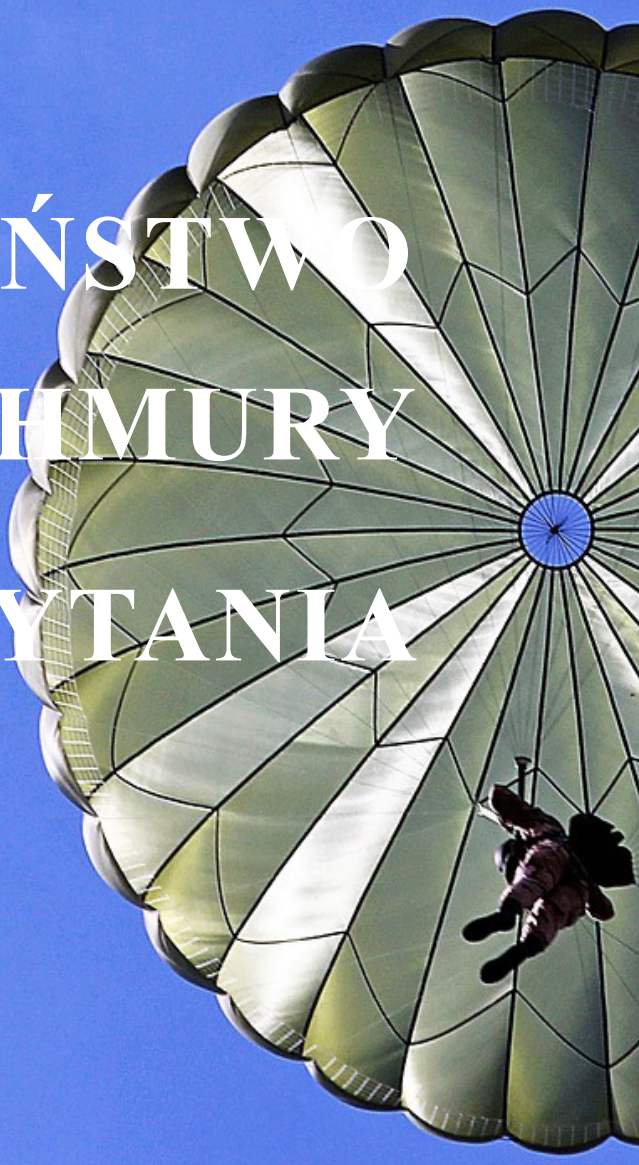
Renata Zalewska jako radca prawny Microsoft w swojej praktyce zawodowej zajmuje się kwestiami prawnymi dotyczącymi ochrony danych osobowych, prywatności, cyberbezpieczeństwa, usług IT w tym usług cloud computing z uwzględnieniem regulacji sektorowych.

Wcześniej Renata Zalewska była radcą prawnym takich firm z sektora IT jak: Dell Sp. z o.o. oraz Dell Products Poland Sp. z o.o., wspierając ich działalność sprzedażową w Warszawie i produkcyjną w rozwijającej się fabryce Della w Łodzi. Pełniła także regionalną funkcję Radcy Prawnego CA Technologies Sp. z o.o. („CA") koordynując wsparcie prawne spółek CA z obszaru Europy Środkowo-Wschodniej. Renata Zalewska rozpoczynała swoją karierę zawodową jako prawnik spółki Softbank S.A.

Renata Zalewska jest członkiem Okręgowej Izby Radców Prawnych w Warszawie, a także członkiem – założycielem Polskiego Stowarzyszenia Prawników Przedsiębiorstw.

ROZDZIAŁ PIĄTY

BEZPIECZEŃSTWO CHMURY - WAŻNE PYTANIA



5.1 Bezpieczeństwo chmury

Określenie czym jest bezpieczeństwo rozwiązań „chmurowych" w kontekście biznesowym jaki realizują kancelarie prawne stanowi zadanie nietrywialne.

Aby odpowiedzieć na tak postawione pytanie, należy jako pierwsze znaleźć odpowiedź na pytanie, co jest kluczowym elementem biznesowym w doradztwie prawnym, poza oczywiście takimi aspektami jak jakość, dostępność, wiarygodność itp. Moim zdaniem jest nim zaufanie jakie prawnik, kancelaria jest w stanie zbudować pomiędzy sobą, a klientem.

Mając świadomość istotności, wrażliwości i sensytywności informacji, które klient powierza kancelariom i faktu, że obecnie praktycznie 100% tych informacji ma postać cyfrową, bezpieczeństwo staje się podstawą biznesu.

Kancelaria, jak każdy inny podmiot gospodarczy są zmuszone do podejmowania szeregu działań zmierzających do ograniczenia ryzyka utraty informacji. Również w tym aspekcie napotykamy wiele problemów zmierzających do postawienia kolejnego pytania, w jaki sposób niewielkie ale również duże kancelarie prawne, są w stanie adekwatnie odpowiedzieć na cyberzagrożenia z jakimi się stykają lub na pewno zetkną (utrata danych, zaawansowane rozłożone w czasie zaawansowane ataki socjotechniczne itp.).

Problem podejmowania adekwatnych reakcji jest z perspektywy kancelarii warunkowany m.in. możliwościami inwestycyjnymi, eksperckimi ale również edukacją i świadomością ryzyka wśród prawników. W tak rozumianym kontekście rozwiązania chmurowe dostarczane przez liczących się dostawców „chmury" zapewniają kancelariom adekwatną odpowiedź na szereg ryzyk związanych z bezpieczeństwem, znosząc lub przynajmniej istotnie ograniczając barierę w postępowaniu z nimi.

Z perspektywy bezpieczeństwa korzystanie z rozwiązań „chmurowych" dla kancelarii to dostęp do metod i środków technicznych umożliwiających redukcję ryzyka niedostępny w inny sposób. Przekłada się to znacząco na podniesienie bezpieczeństwa danych klienta kancelarii i wiarygodność świadczonych usług.

Tak jak wspomniałem, technologia to nie wszystko, a „chmura" z perspektywy bezpieczeństwa nie jest panaceum na zapewnienie 100% bezpieczeństwa kancelarii. Świadomość ryzyk, edukacja technologiczna prawników stanowi niezbędne uzupełnienie całego łańcucha działań wpływających na osiągnięcie

akceptowalnego cyberbezpieczeństwa kancelarii.

Czym zatem jest cyberbezpieczeństwo? Jest wiele definicji funkcjonujących w powszechnym obiegu, na potrzeby niniejszej publikacji chciałbym zaproponować jednak nieco inną autorską definicję:

> *Bezpieczeństwo chmury to: suma nakładów (finansowych, technologicznych i organizacyjnych) związanych z bezpieczeństwem jakie jest zdolny ponosić dostawca „chmury" oraz dojrzałość i świadomość ryzyk w organizacji, która z chmury korzysta.*

Czynnik percepcji ryzyka przez organizację w połączeniu z poziomem świadomości cyberzagrożeń oraz możliwości inwestycyjne i eksperckie, determinują naszą osobistą percepcję i postrzeganie nas na rynku jako firmę, kancelarię „cyberbezpieczną" lub też nie.

„Chmura" w istotny sposób, wskazane czynniki przenosi na nieporównywalnie wyższy poziom i to również w perspektywie małych kancelarii.

Na co dzień rozmawiając o bezpieczeństwie rozwiązań „chmurowych" z perspektywy biznesu jaki prowadzą kancelarie prawne napotykamy szereg mitów. Przytoczę kilka, starając się jednocześnie odnieść do faktów:

Mit 1: Wszystko powinno być w chmurze u jednego jej dostawcy

FAKT: Transfer danych kancelarii do chmury oraz jej wykorzystanie zawsze musi być poprzedzone oceną ryzyka, w zestawieniu z ofertą składaną przez dostawcę chmury przy zachowaniu zdrowego rozsądku! To z usług jakich i ilu dostawców chmury skorzystamy powinien decydować charakter usługi jakiej szukamy.

Mit 2: Korzystanie z chmury wiąże się z większymi ryzykami niż korzystanie z własnej infrastruktury IT

FAKT: Jest dokładnie odwrotnie – zakres stosowanych zabezpieczeń, wiodących rozwiązań chmurowych, gwarancje prawne, jak również efekt skali świadczonych usług jest niewspółmiernie większy niż lokalnych infrastruktur IT.

Mit 3: Organizacja, która korzysta z chmury nie może z niej nigdy zrezygnować

FAKT: Migracja pomiędzy rozwiązaniami „chmurowymi", łączenie rozwiązań od różnych dostawców oraz powrót do infrastruktury własnej jest możliwy i powszechnie stosowany, a żaden wiodący dostawca usług „chmurowych" nie powinien utrudniać lub wręcz uniemożliwiać tego procesu.

Mit 4: Klienci nie zaufają kancelarii, która korzysta z chmury

FAKT: Kluczową kwestią jest pokazanie klientowi, że jego dane są bezpieczne, ryzyko jest zarządzane przez nas, a wiodące współczesne rozwiązania chmurowe dostarczają ku temu wielu argumentów i są nieporównywalnie bezpieczniejsze niż lokalne infrastruktury IT.

Rozumiejąc czym jest cyberbezpieczeństwo oraz mając świadomość mitów dotyczących chmury, spróbujmy znaleźć odpowiedzi na pytania dotyczące jej bezpieczeństwa w kontekście działalności biznesowej kancelarii prawnych.

5.2 Odpowiedzi na pytania zadane podczas konferencji

Jakie są podstawowe ryzyka dla bezpieczeństwa danych związane z wdrożeniem rozwiązania chmurowego?

Podstawowych ryzyk, o których warto wspomnieć w tym kontekście jest wiele, wspomnę jedynie o kilku:

- Ryzyko niewłaściwego wyboru dostawcy „chmury". Skutków może być wiele, począwszy od braku możliwości zapewnienia odpowiednich zabezpieczeń, poprzez utratę dostępu do danych lokowanych w „chmurze", aż do poważnego wycieku informacji o charakterze incydentu bezpieczeństwa mogącego skutkować kompromitacją kancelarii korzystającej z danego dostawcy „chmury".

- Ryzyko prawne dotyczące braku możliwości zapewnienia zgodności prawnej przechowywania i przetwarzania danych w takich aspektach jak np. ochrona danych osobowych, ochrona informacji, regulacji branżowych itp.

- Ryzyko niedotrzymywania ustalonego SLA (poziomu świadczenia usługi) przez dostawcę „chmury" które może skutkować m.in. utratą dostępu do danych, brakiem możliwości ich odtworzenia, a w konsekwencji brakiem możliwości realizowania podstawowych procesów biznesowych.

- Ryzyko dostępu osób trzecich do danych – utrata poufności. Dostawca „chmury" powinien w sposób wiarygodny wykazać jakie procedury i technologie stosuje do zapewnienia kontroli dostępu do danych zgromadzonych w jego infrastrukturze „chmurowej". Ważną kwestią w tym kontekście jest zarządzanie tzw. kontami uprzywilejowanymi, którymi posługują się m.in. administratorzy dostawcy „usług chmurowych". Takie konta powinny podlegać szczególnej ochronie i okresowym audytom. Nie wolno nam zapominać, iż do zachowania poufności zobowiązują prawników również regulacje prawne dotyczące zachowania tajemnicy zawodowej.

- Ryzyko fizycznego zabezpieczenia centrów danych, w których świadczone są usługi „chmurowe". Dostawca „chmury" musi wykazać, jawnie jakie stosuje zabezpieczenia swoich centrów danych, łącznie ze wskazaniem czy, a jeśli tak to gdzie, zlokalizowany jest ośrodek

zapasowy oraz jaki jest czas przełączenia usług. Dostawca „chmury" powinien wykazać się stosownymi certyfikacjami potwierdzającymi bezpieczeństwo jego centrów przetwarzania danych.

- Ryzyko wycieku danych podczas komunikacji z usługą „chmurową". Dostawca „chmury" powinien wskazać w jaki sposób zabezpiecza, technicznie komunikację klienta z usługą „chmurową", czy stosuje przede wszystkim szyfrowanie połączeń w oparciu o wiarygodny protokół szyfrowania lub/i inne mechanizmy zabezpieczeń.

- Ryzyko dostępu do danych klienta przez dostawcę usługi „chmurowej". Dostawca powinien wskazać jakie mechanizmy szyfrowania danych są możliwe do zastosowania w zakresie danych lokowanych w usłudze „chmurowej". W jaki sposób przechowywane i udostępniane są klucze kryptograficzne, czy dostawca ma do nich dostęp.

- Ryzyko wycieku danych. Jakie mechanizmy data loss prevention (DLP) są możliwe do zastosowania w ramach usługi „chmurowej".

Powyższe aspekty wraz z wyjaśnieniem ich znaczenia to jedynie kilka wybranych ważnych tematów na które powinniśmy zwrócić uwagę myśląc o bezpieczeństwie usług, które chcemy pozyskać z „chmury".

Jak można zabezpieczyć kancelarię i dane jej klientów w umowie z dostawcą chmury? Co to jest SLA?

W umowie takiej powinny zostać wskazane w sposób jawny m.in.: stosowane mechanizmy techniczne i organizacyjne dotyczące bezpieczeństwa w odniesieniu do każdej z usług z których zamierzamy korzystać.

W umowie również powinny znaleźć się zapisy lub wyraźne odniesienie do dokumentów takich jak polityka prywatności określająca m.in.: zasady dostępu do danych zgromadzonych w infrastrukturze chmurowej, prawa i obowiązki stron z nim związanych ale również polityki przetwarzania danych osobowych, polityki zapewniania ciągłości działania, polityk i procedur dotyczących zabezpieczeń, odtworzenia środowiska po awarii itp.

SLA (Services Level Agreement) to nic innego jak wskaźnik gwarantowanego poziomu świadczenia usługi, mówiąc wprost jest to zakładany przez dostawcę usługi (np. MS Office 365) maksymalny możliwy czas, w którym usługa ta może

być niedostępna, czyli nie będziemy mogli z niej korzystać. W jaki sposób poziom SLA przekłada się na czasy niedostępności usługi obrazuje poniższa tabela:

Dostępność	Czas niedostępności w ciągu miesiąca 30 dniowego
95%	36 godzin (2160 minut)
99%	7 godzin (432 minuty)
99,5%	3,5 godziny (216 minut)
99,9%	43 minuty i 12 sekund
99,99%	4 minuty i 19 sekund
99,999%	25 sekund

Jak widać w powyższej tabeli, poziom SLA wpływa bezpośrednio na cenę usługi. Wraz ze wzrostem poziomu SLA wzrasta jej cena. Oczekiwania dotyczące poziomu SLA należy zawsze rozważać w kontekście poziomu ryzyka jakie niesie dla nas chwilowa niedostępność usługi. Czym większe SLA tym większy koszt dla nas, tylko czy my zawsze potrzebujemy SLA na poziomie 99,9999.

Czy rozwiązania chmurowe są zgodne z RODO

Ponieważ na rynku mamy ogromną ilość rozwiązań i dostawców chmurowych, nie da się wprost odpowiedzieć na tak postawione pytanie. Co do zasady zawsze wybór dostawcy chmurowego powinien obejmować analizę aspektu zgodności z RODO. Również w większości przypadków duże podmioty dostarczające usługi chmurowe zapewniają zgodność przetwarzania danych osobowych w zakresie świadczonej usługi z regulacjami RODO oraz wielu innymi również międzynarodowymi.

Czy wdrażając rozwiązania chmurowe kancelaria zwiększa ryzyko utraty danych?

Również na tak zadane pytanie nie można odpowiedzieć jednoznacznie.

Ryzyko utraty danych przetwarzanych w chmurze zależy m.in. od poziomu bezpieczeństwa jaki zapewnia dostawca chmury i to nie chmury jako całości, a konkretnej usługi „chmurowej" z której klient korzysta.

Zależy ono również (zgodnie z powyższą definicją bezpieczeństwa) od świadomości aspektów bezpieczeństwa osób/użytkowników, którzy z usług „chmurowych" korzystają.

Z perspektywy technologicznej rozwiązania „chmurowe" dostarczane przez liczących się dużych dostawców „chmury", są co do zasady bezpieczniejszą formą przetwarzania, składowania i lokowania danych, szczególnie w kontekście możliwości i dostępności zaawansowanych zabezpieczeń IT dostarczanych przez dostawców chmurowych vs ich dostępności w lokalnych środowiskach IT tzw. on premises.

Czy wszystkie dane można umieścić w chmurze?

Większość współcześnie wytwarzanych danych w praktycznie każdej ich elektronicznej formie można umieścić w „chmurze". Pojawia się jedynie pytanie o sens takiego działania. Aby rozważać sens lokowania danych w chmurze, należy przede wszystkim określić po co chcemy skorzystać z takiego mechanizmu i co on nam daje.

Również musimy uwzględnić w jakim kontekście (procesie) powstają dane, które zamierzamy przenieść do „chmury", jaki mają charakter, klasyfikację i rodzaj (np. sensytywne, wrażliwe ale również medyczne, prywatne itp.). Zawsze powinniśmy szukać uzasadnienia biznesowego i ocenić ryzyko lokowania danych w chmurze, a sam ten proces nigdy nie powinien być realizowany w oderwaniu od procesu biznesowego w jakim dane powstają.

Czy wdrożenie rozwiązania chmurowego wiąże się zawsze z koniecznością przekazania danych dostawcy rozwiązania?

Nie. Wdrożenie rozwiązań chmurowych nie zawsze wiąże się z koniecznością przekazywania danych dostawcy chmury. Jakie dane są przekazywane, lokowane, przetwarzane w chmurze decyduje kilka czynników m.in.: typ usługi z jakiej użytkownik korzysta, rodzaj modelu świadczenia usług chmurowych (SaaS, PaaS, Iaas itd.), rodzaj architektury chmurowej, (chmura hybrydowa, chmura publiczna itp).

Użytkownik decydując się na korzystanie z usług chmurowych powinien być poinformowany w sposób jednoznaczny, jakie konkretnie dane są przekazywane dostawcy rozwiązania. Co do zasady w większości powszechnie świadczonych usług chmurowych to użytkownik sam decyduje, które dane i na którym etapie korzystania z usługi przekazuje dostawcy „chmury". Najczęściej takie mechanizmy definiowane są na poziomie ustawień parametrów usługi, czyli jej personalizacji, wdrożenia.

Na co zwrócić uwagę wybierając dostawcę?

Wybierając dostawcę „chmury" trzeba w pierwszej kolejności mieć świadomość jak ważne dla nas usługi z perspektywy ciągłości funkcjonowania naszego biznesu będą realizowane za pośrednictwem rozwiązań chmurowych.

Mając świadomość istotności dla naszego biznesu usług z których zamierzamy korzystać powinniśmy zwrócić uwagę również na:

- pozycję rynkową dostawcy w zakresie interesujących nas usług,
- jak postrzegane są jego rozwiązania przez osoby już z nich korzystające (np. specjalistyczne fora internetowe i publikacje),
- czy, a jeśli tak to jakiego charakteru zdarzały się incydenty niedotrzymania poziomów SLA,
- czy, a jeśli tak to jakiego rodzaju zanotowano incydenty bezpieczeństwa w odniesieniu do konkretnych usług,
- sposoby od strony technicznej, organizacyjnej i prawnej umożliwiające wycofanie się klienta z korzystania z usług. Chodzi mi.in. o takie aspekty jak np. trwałe skasowanie danych, zwrot danych, migracja do innych rozwiązań po zaprzestaniu korzystania z usługi.
- określenie lokalizacji danych. Czy stosowany jest transfer danych do innego ośrodka szczególnie zlokalizowanego poza UE np. w ramach mechanizmów clastra geograficznego. Jeśli tak to jakie dane i gdzie trafiają.
- czy dostawca określa jakieś specjalne wymagania techniczne, które musi spełnić użytkownik korzystający z usługi lub sprzęt z którego następuje dostęp do niej.
- posiadane certyfikaty bezpieczeństwa w odniesieniu do usług i infrastruktury, na której są realizowane usługi „chmurowe". Są to m.in.: certyfikaty bezpieczeństwa centrów danych, certyfikaty na zgodność z normami bezpieczeństwa itp.
- czy, a jeśli tak to w jaki sposób możliwe jest audytowanie świadczonych usług bezpośrednio przez klienta.

Jak kształtuje się odpowiedzialność za bezpieczeństwo danych w chmurze?

Odpowiedzialność za bezpieczeństwo danych w chmurze jest szczegółowo regulowana w umowach i regulaminach odnoszących się do konkretnej usługi chmurowej dostarczanej klientowi. Uregulowania te są specyficzne zarówno z perspektywy dostawcy jak i konkretnej usługi, z której korzysta klient.

Najczęściej odpowiedzialność dostawcy usługi chmurowej ograniczona jest do zapewnienia ochrony podstawowych aspektów bezpieczeństwa informacji takich jak: poufność, integralność, niezaprzeczalności, dostępność zarówno wszelkich informacji jak i danych trafiających do chmury w związku z realizacją konkretnej usługi.

Najczęściej wyłączeniu odpowiedzialności podlegają takie aspekty jak, działania osób trzecich, utrata informacji (wyciek) spowodowana z winy użytkownika (np. udostępnienia danych do logowania) lub utraty informacji w wyniku działania oprogramowania szkodliwego (na sprzęcie i w infrastrukturze lokalnej użytkownika) lub też aktywności wynikającej z „niefrasobliwości" użytkownika zainicjowanej, np. działaniami socjotechnicznymi skierowanymi wobec niego.

Rozwiązanie chmurowe: największa korzyść i największe ryzyko?

Bez wątpienia we współczesnych, dostarczanych przez podmioty o wiarygodnej pozycji rynkowej, rozwiązaniach chmurowych przeważają korzyści.

Wiele z nich zostało już wymienionych w tekście oraz całej publikacji, a do najważniejszych można zaliczyć oczywiście, wysoką dostępność, niezawodność, nieporównywalnie wyższy poziom bezpieczeństwa niż dla porównywalnych usług realizowanych w oparciu o infrastruktury lokalne.

Również w przypadku chmury mamy praktycznie nieograniczoną skalowalność usług, rozliczalność i oczywiście koszty, niewspółmiernie niskie w stosunku do tych samych usług realizowanych lokalnie.

Oczywiście w odniesieniu do usług chmurowych występują również ryzyka m.in. wyboru niewiarygodnego dostawcy rozwiązań, skutkiem czego może wystąpić brak zapewnienia przez niego mechanizmów bezpieczeństwa naszych danych.

Dostawca usług „chmurowych” musi wyeliminować, a przynajmniej ograniczyć ryzyko dostępu do danych osób nieuprawnionych, co z kolei dla klienta może skutkować utratą poufności, a docelowo utratą reputacji biznesowej kancelarii.

5.3 Prelegent i autor rozdziału

Marek Laskowski

Marek Laskowski jest doświadczonym managerem IT z wieloletnią praktyką zawodową związaną z zarządzaniem dużymi działami IT w firmach polskich i zagranicznych.

Marek prowadził praktykę doradztwa strategicznego, dotyczącego doskonalenia obszarów IT w polskich i międzynarodowych firmach z wielu branż. Z wykształcenia jest psychologiem (UW), dodatkowo ukończył studia podyplomowe z zakresu zarządzania IT w dużych przedsiębiorstwach (SGH). Ukończył szereg szkoleń z zakresu zarządzania projektami, zespołami i technologią IT.

Wcześniej zajmował stanowisko Dyrektora Biura Informatyki w Polskiej Wytwórni Papierów Wartościowych S.A., gdzie kierował zespołem IT i nadzorował współpracę z kilkudziesięcioma dostawcami rozwiązań IT, dotyczących wielu obszarów technologicznych. Zajmował również stanowisko Dyrektora Biura Informatyki w Instytucie Pamięci Narodowej - realizując szereg dużych inicjatyw z zakresu organizacji zarządzania i bezpieczeństwa IT, posiada również uprawnienia do zasiadania w Radach Nadzorczych Spółek Skarbu Państwa.

W DZP pełni funkcję Dyrektora Działu IT odpowiadając za wszelkie aspekty cyfrowe Kancelarii. W toku pracy zawodowej wraz z zespołem IT kancelarii Marek zrealizował kilka dużych projektów w obszarze infrastruktury, bezpieczeństwa m.in. implementację dużego systemu klasy anty APT, rozwiązań ERP oraz rozwiązań dotyczących bezpośrednio dziedziny określanej jako lega-tech, opartych m.in. o mechanizmy AI, Cognitive services, Machine Learning itp. Jest pasjonatem nowych technologii IT i ich wykorzystania w procesach transformacji cyfrowej.

ROZDZIAŁ SZÓSTY

CHMURA - ZALECENIA DLA RADCÓW PRAWNYCH

6.1 – Wstęp

Usługi chmurowe są bardzo różnorodne, są świadczone w kilku modelach i wariantach wdrożenia. Dodatkowo, w przypadku usług świadczonych w modelu oprogramowanie jako usługa (SaaS), użytkownicy często nawet mogą sobie nie zadawać sprawy z tego, że aplikacja z której korzystają jest zainstalowana na platformie usług chmurowych.

Wreszcie, samo środowisko radców prawnych jest zróżnicowane i obejmuje zarówno kancelarie jednoosobowe, kilkuosobowe, jak również duże firmy prawnicze zrzeszające kilkudziesięciu prawników. W przeciwieństwie do największych firm prawniczych, które często mają swoje własne działy IT, mniejsze kancelarie korzystają z usług specjalistów IT raczej wyjątkowo. Sytuacji nie poprawia też fakt, że usługi chmurowe są ciągle postrzegane jako nowość w stosunku do tradycyjnych modeli korzystania z oprogramowania (instalacja na własnym sprzęcie) i w związku z tym, wiedza na temat zasad świadczenia tych usług i kwestii wymagających analizy prawnej nie jest jeszcze powszechna. Dodatkowo, nie wszyscy radcy prawni specjalizują się lub interesują się kwestiami IT.

Usługi chmurowe niewątpliwie mogą przynieść radcom prawnym szereg korzyści, od dostępu do najnowszych aplikacji pozwalających im na poprawę obsługi klienta po podwyższenie bezpieczeństwa IT. Te pozytywne skutki wystąpią jednak tylko wtedy, gdy radca prawny wybierze odpowiedniego dostawcę usługi.

Poniżej wskazujemy zatem kilka podstawowych kwestii, na które należy zwrócić uwagę przy wyborze dostawcy usług chmurowych.

Na co należy zwrócić uwagę wybierając dostawcę usługi chmurowej?

6.2 Odpowiedzi na pytania zadane podczas konferencji

Umowa z dostawcą usługi chmurowej powinna odnosić się do kwestii poruszonych w odpowiedziach na zadane poniżej pytania. Warto przy tym jednak pamiętać, że takie umowy są często dosyć obszerne i złożone z kilku dokumentów. Dodatkowe wyjaśnienia mogą być zawarte na specjalnych portalach dostawców usług chmurowych lub mogą być udostępniane podmiotom korzystającym z usługi (w ramach tzw. paneli administracyjnych).

Do jakich celów będą wykorzystywane usługi chmurowe?

Radca prawny powinien określić w jakich celach chce wykorzystywać usługi chmurowe oraz jakie rozwiązania informatyczne będą służyły realizacji tych celów. Jeżeli radca prawny chciałby korzystać z aplikacji biurowych i poczty elektronicznej w chmurze, czy z oprogramowania księgowego będzie to najczęściej model usługi określany SaaS (oprogramowanie jako usługa). Jeżeli chciałby przechowywać dane archiwalne w chmurze to często będzie to skutkowało wyborem innego modelu usługi – IaaS (infrastruktura jako usługa). Model usługi chmurowej ma istotne znaczenie dla sposobu i wyników przeprowadzanych analiz zgodności z przepisami czy analiz wrażliwości korzystania z usług chmurowych przez radców prawnych.

Po ustaleniu, jakim celom mają służyć usługi chmurowe, radca prawny powinien zebrać informacje na temat dostępnych rozwiązań i ich dostawców. Takie rozpoznanie rynku pozwoli uniknąć nieporozumień na późniejszym etapie, gdyby okazało się np. że dane rozwiązanie nie oferuje w standardowej konfiguracji funkcjonalności, na których radcy prawnemu zależało i konieczne jest uiszczenie dodatkowej opłaty lub w ogóle nie ma możliwości rozszerzenia o taką funkcjonalność.

Oczywiście kancelaria może mieć już preferowanego dostawcę lub usługę (np. jeżeli wcześniej testowała takie oprogramowanie lub otrzymała rekomendacje ze strony klienta lub innych prawników). W takim przypadku mimo wszystko warto ustalić, czemu ma służyć takie oprogramowanie i czy dane rozwiązanie spełnia te wymogi. Warto w szczególności rozważyć możliwość testowego korzystania

z usługi chmurowej przed podjęciem ostatecznej decyzji o przejściu na to rozwiązanie. Pozwoli to nie tylko ocenić czy dane rozwiązanie spełnia oczekiwania radcy prawnego, ale zwykle umożliwia pozyskanie dodatkowych informacji o usłudze, które są dostępne tylko dla użytkowników (np. szczegółowe historyczne informacje o dostępności usługi, szczegółowe raporty z audytów bezpieczeństwa itp.).

Jakie kategorie danych mogą być przekazywane do dostawcy usług chmurowych?

Radca prawny powinien określić, jakie kategorie danych mogą być przetwarzane w ramach usług chmurowych i przekazywane do dostawcy tych usług, biorąc pod uwagę ich wrażliwość (począwszy od danych publicznie dostępnych do danych bardzo poufnych). W szczególności, radca prawny powinien określić, czy mogą to być dane osobowe (w tym dane wrażliwe) oraz dane objęte tajemnicą zawodową (dane klientów). W oparciu o zastosowaną klasyfikację danych, radca prawny może ocenić, czy będzie konieczne zastosowanie dodatkowych środków zabezpieczenia danych szczególnie poufnych w ramach danych objętych tajemnicą zawodową (np. poprzez ich dodatkowe szyfrowanie własnym kluczem).

Kim jest dostawca usług chmurowych?

Radca prawny powinien sprawdzić, kto jest dostawcą usługi. W praktyce często występują rozwiązania w których dostawcy posługują się odsprzedawcami, którzy odpowiadają za obsługę klienta wobec dostawcy usługi, w tym za składanie zamówień czy rozliczanie płatności. Radca prawny powinien ustalić kto jest dostawcą usługi, czy ma z nim bezpośrednią umowę i ewentualnie jaka jest rola innych podmiotów uczestniczących w oferowaniu usług chmurowych. Niewątpliwie preferowanym rozwiązaniem jest zawarcie umowy z dostawcą usług chmurowych (niezależnie od ewentualnych umów z innymi podmiotami, takimi jak odsprzedawcy). Takie rozwiązanie pozwala na występowanie z ewentualnymi roszczeniami bezpośrednio do dostawcy usługi oraz ma wpływ na ocenę wiarygodności podmiotu świadczącego usługę (zob. poniżej).

Czy dostawca usług chmurowych jest wiarygodny?

Radca prawny powinien zweryfikować wiarygodność dostawcy usług chmurowych biorąc pod uwagę m. in.:

- doświadczenie i reputację dostawcy;
- siedzibę dostawcy – strony umowy (UE/nie-UE);
- rzetelność, w tym opinie z wcześniejszej współpracy z dostawcą;
- wypłacalność i wiarygodność finansową;
- potencjalne konflikty interesów (tj. ewentualne ryzyka związane z przechowywaniem danych klienta radcy prawnego, który toczy spór lub negocjacje z dostawcą usługi na zasobach tego dostawcy bez dodatkowego zabezpieczenia);
- w miarę możliwości – strukturę właścicielską;
- lokalizacje centrów danych (UE/nie-UE).

Kto jest właścicielem danych przekazywanych do usług chmurowych?

W pierwszej kolejności należy ustalić, czy dostawca usług chmurowych może wykorzystywać dane przekazywane przez radcę prawnego tylko do świadczenia wybranych przez radcę prawnego usług chmurowych i ewentualnie usług pomocniczych (np. usług wsparcia), czy też dostawca wymaga od klienta zgody na korzystanie z jego danych również w innych celach (np. licencji na korzystanie przez dostawcę z przekazywanych mu danych do celów innych niż związane ze świadczeniem usługi, takich jak cele reklamowe, lub nawet przekazania praw do takich danych). Rozwiązania, w których dostawca usług chmurowych mógłby nabyć prawo do korzystania z danych objętych tajemnicą zawodową do innych potrzeb niż świadczenie usługi, nie powinny być akceptowane.

Czy dostawca usług chmurowych jest przetwarzającym czy administratorem danych osobowych przekazywanych przez radcę prawnego do chmury?

Ważne jest także ustalenie w jakim charakterze występuje dostawca usług chmurowych z perspektywy przetwarzania danych osobowych przekazywanych przez radcę prawnego tj. czy jest tylko przetwarzającym dane osobowe w imieniu radcy prawnego, czy też może występować w roli administratora (tj. wykorzystywać dane przekazywane przez radcę prawnego do własnych celów np. do oferowania radcy prawnemu lub jego pracownikom reklam).

Jak wskazuje GIODO w Zestawieniu wyników kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzonych w kancelariach prawnych[1] „decydując się na wykorzystanie usług poczty elektronicznej oferowanych przez podmioty zewnętrzne zazwyczaj będzie dochodzić do przetwarzania danych osobowych w tzw. chmurze obliczeniowej". W takim przypadku, radca prawny i dostawca takich usług powinni zawrzeć umowę o powierzeniu przetwarzania danych osobowych[2]. Umowa o powierzenie przetwarzania powinna spełniać wymogi wskazane w art. 28 RODO, a w szczególności określać przedmiot, czas trwania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą a także prawa i obowiązki administratora.

Dostawca usługi powinien pełnić rolę administratora jedynie w ograniczonym zakresie tj. w odniesieniu do danych radcy prawnego, które są zawarte w umowie zawieranej z dostawcą lub które są przetwarzane w związku z zawarciem takiej umowy (np. dane do rozliczeń, dane osób kontaktowych, dane dotyczące korzystania z usługi). Dostawca usług chmurowych nie powinien stawać się administratorem danych objętych tajemnicą zawodową radcy prawnego.

1 Zestawienie wyników kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzonych w kancelariach prawnych, Warszawa, 2017, http://www.giodo.gov.pl/pl/1520291/9847

2 jw. S. 7 i 9.

Czy dostawca usług chmurowych oferuje odpowiednie środki bezpieczeństwa (zgodne ze standardami i normami)?

Radca prawny powinien ocenić oferowane przez dostawcę usługi środki bezpieczeństwa fizycznego oraz organizacyjnego. Teza, że przechowywanie danych na własnym sprzęcie jest zawsze najbezpieczniejsze jest co najmniej dyskusyjna. Jeżeli bowiem radca prawny nie aktualizuje stosowanego przez siebie oprogramowania lub nie dba o bezpieczeństwo fizyczne używanego sprzętu, dane przechowane w ten sposób mogą być bardzo łatwo dostępne dla osób nieupoważnionych[3]. Warto podkreślić, że RODO wprowadza fundamentalną zmianę w podejściu do zapewniania bezpieczeństwa przetwarzania danych osobowych. W przeciwieństwie do obowiązujących wcześniej przepisów dotyczących przetwarzania danych osobowych, RODO nie ustanawia szczegółowych wymogów dla systemów, w których przetwarzane są dane osobowe (takich jak kazuistyczne regulacje dot. chociażby hasła i częstotliwości jego zmiany), ale przesuwa ciężar analizy i oceny ryzyka, a także zastosowania odpowiednich środków bezpieczeństwa na administratora i podmiot przetwarzający dane osobowe.

Należy zatem rzetelnie ocenić, jakie środki bezpieczeństwa oferują rozważani dostawcy usług chmurowych. Pomocne przy takiej ocenie mogą być wyniki audytów lub certyfikaty z audytów przeprowadzone przez niezależnych audytorów na zlecenie dostawcy usługi zgodnie z uznanymi krajowymi lub międzynarodowymi standardami zarządzania ryzykiem IT (np. ISO 27001, SSAE 16 SOC 1 lub SOC II).

Radca prawny powinien również sprawdzić, czy umowa z dostawcą zobowiązuje personel dostawcy (w tym jego podwykonawców) do zachowania poufności w zakresie objętym jego tajemnicą zawodową.

3 W Zestawieniu, GIODO wskazał na jeszcze bardziej drastyczny przypadek braku zabezpieczenia dysku sieciowego zawierającego dane osobowe klientów kancelarii przed dostępem osób nieupoważnionych oraz przed zabraniem przez osobę nieuprawnioną, gdy dysk sieciowy znajdował się w niezamykanej na klucz szafie ustawionej w korytarzu, w którym przebywają osoby postronne (s. 9).

Z uwagi na charakter usług chmurowych (w tym współdzielenie zasobów przez wielu klientów), kontrola zastosowanych środków bezpieczeństwa różni się w przypadku usług chmurowych i „standardowych" usług IT. Tytułem przykładu, powszechnie akceptowaną praktyką w odniesieniu do dużych dostawców usług chmurowych, jest to że ich centra danych nie są udostępniane klientom w celu kontroli ze względów bezpieczeństwa, a nawet w przypadku umożliwienia przeprowadzenia kontroli w takim centrum danych, może być to utrudnione z uwagi na jego lokalizację i konieczność zaangażowania specjalisty z zakresu IT. Radca prawny powinien brać pod uwagę specyfikę usług przy ocenie możliwości samodzielnej kontroli środków bezpieczeństwa.

Radca prawny powinien też ustalić, czy umowa zapewnia archiwizację lub sporządzanie kopii bezpieczeństwa przez dostawcę usługi chmurowej.

Należy jednocześnie podkreślić, że nawet najlepsze zabezpieczenia po stronie dostawcy usługi chmurowej nie zwalniają radcy prawnego z odpowiedniej ochrony danych objętych tajemnicą zawodową i innych chronionych danych (np. danych osobowych). Warto przypomnieć, że radca prawny powinien zapewnić, aby również jego personel był zobowiązany do zachowania poufności. W tym celu powinien wymagać, aby jego personel nie korzystał m.in. z darmowych rozwiązań chmurowych udostępnianych konsumentom. Takie darmowe rozwiązania często bowiem nie zapewniają adekwatnego poziomu bezpieczeństwa. Dodatkowo, często wiążą się one z przekazaniem dostawcy prawa do korzystania z danych zamieszczanych w chmurze do własnych celów dostawcy. Obowiązkiem radcy prawnego powinno być zapewnienie kontroli dostępu do danych, gdy radca prawny zamierza udostępniać klientom pliki danych w swojej chmurze. W takim przypadku żadna osoba, poza radcą prawnym (jego personelem) i wyznaczonym klientem, nie powinna mieć możliwości uzyskania dostępu do takiego pliku. Jeżeli usługi udostępniane przez radcę prawnego zostałyby bowiem wykorzystane do wymiany wrażliwych danych handlowych między klientami, mogłoby to mieć np. skutki antymonopolowe (zmowa kartelowa).

Usługa chmurowa jest usługą automatyczną, wymagającą w niektórych obszarach konfiguracji lub monitorowania (np. zapoznawania się z zawiadomieniami o incydentach bezpieczeństwa, zapoznania się z audytami usług chmurowych przygotowywanych przez audytorów działających na zlecenie dostawcy usług). Radca prawny musi mieć świadomość, że podobnie jak przy standardowych rozwiązaniach informatycznych, jego rola i konieczność zabezpieczania takich rozwiązań nie kończy się wraz z zakończeniem wdrożenia, ale że jest to proces ciągły.

Gdzie są przechowywane dane klienta przekazywane do usług chmurowych?

Radca prawny powinien ustalić, czy dostawca zobowiązuje się do przechowywania danych w centrach danych na terenie UE lub w innym kraju zapewniającym należyty poziom ochrony (np. Szwajcaria, Norwegia, w określonych sytuacjach – Kanada).

Jeżeli konieczne może być udostępnianie danych podmiotom spoza takich krajów (np. w celu świadczenia usług wsparcia przez podwykonawców), dostawca powinien zagwarantować odpowiednie mechanizmy w celu zapewnienia poufności takich danych oraz zgodności z przepisami o ochronie danych osobowych (np. zobowiązanie podwykonawcy do zachowania poufności, a w zakresie danych osobowych – standardowe klauzule umowne).

Informacja o miejscu przechowywania danych powinna być wyraźnie wskazana w umowie z uwagi na potencjalne konsekwencje z perspektywy przetwarzania danych osobowych.

Dodatkowo, w przypadku radców prawnych wykonujących zawód w ramach stosunku pracy szczególnie istotna może być kwestia zachowania w poufności danych objętych tajemnicą radcowską w relacjach wewnętrznych. Prawnicy wewnętrzni często przetwarzają dane o wysokim stopniu poufności. Konfiguracja usług informatycznych, czy to w tradycyjnym ujęciu, czy też usług online powinna zapewniać poufność tych danych i brak dostępu do nich osób nieuprawnionych wewnątrz organizacji.

Czy trudno zakończyć korzystanie z usługi chmurowej? Z jakim kosztami się to wiąże? Czy dostawca usługi ma obowiązek usunięcia danych?

Radca prawny powinien unikać wyboru dostawców usług chmurowych, którzy nie zapewniają możliwości skopiowania danych z usług chmurowych w edytowalnej postaci, zwłaszcza w przypadku zakończenia współpracy. Takie usługi mogą być dodatkowo płatne, więc radca prawny powinien przed zawarciem umowy z dostawcą ustalić jakie koszty będą wiązały się z takim „wyjściem" z usługi chmurowej.

Dostawca usług chmurowych powinien również zapewniać, że dane przekazane przez radcę prawnego będą usuwane po zakończeniu przez niego korzystania z usługi, jeśli radca prawny sam nie usunie tych danych. Warto podkreślić, że obowiązek zwrotu albo usunięcia danych osobowych jest również obowiązkiem podmiotu przetwarzającego zgodnie z RODO, o ile przepisy państwa członkowskiego nie zobowiązują go do zachowania kopii.

Możliwość wypowiedzenia umowy przez dostawcę usługi chmurowej w każdym czasie bez wskazywania powodu jest istotnym ryzykiem, które radca prawny powinien uwzględnić w swojej analizie. Powyższe nie oznacza, że dostawca usługi nie może zastrzec sobie możliwości wypowiedzenia ze skutkiem natychmiastowym w uzasadnionych przypadkach (np. jeżeli radca prawny nie płaci za usługę), czyli w standardowych przypadkach.

Czy oferowana jest umowa dotycząca poziomu świadczenia usług (Umowa SLA)?

Radca prawny powinien ustalić, czy dostawca usług chmurowych oferuje umowę SLA (ang. Service Level Agreement) właściwą dla danego modelu usług i jakie są jej warunki. Zalecane jest też zebranie historycznych danych o dostępności danej usługi w przeszłości (takie dane są często publikowane przez dużych dostawców usług chmurowych). Dla usług istotnych dla praktyki radcy

prawnego (np. poczta elektroniczna), radca prawny powinien sprawdzić, czy umowa SLA wlicza czas planowanych przerw w świadczeniu usługi przy ustalaniu czasu niedostępności usługi skutkującego odpowiedzialnością radcy prawnego. W przypadku dużych dostawców usług chmurowych, brak spełnienia wymogów określonych w umowie SLA skutkuje przede wszystkim obniżeniem wynagrodzenia za daną usługę. W praktyce takie rozwiązanie jest zbliżone do kar umownych, gdyż nie wymaga wykazywania odpowiedzialności dostawy, ani szkody po stronie korzystającego. Radca prawny powinien jednak ustalić, czy dostawca ponosi również odpowiedzialność za inne szkody związane z nienależytym wykonaniem umowy (tj. czy odpowiedzialność na podstawie umowy SLA nie jest jedyną odpowiedzialnością dostawcy).

Radca prawny powinien ocenić, jaki wpływ na świadczone przez niego usługi prawne może mieć brak dostępu do danych przechowywanych w usługach chmurowych i jeśli byłby to wpływ istotny – rozważyć jakie alternatywne rozwiązania mogą zostać przez niego zastosowane. Warto jednocześnie podkreślić, że brak dostępności do usługi może nie wynikać tylko z awarii po stronie dostawcy usług, ale również z awarii po stronie radcy prawnego albo dostawcy dostępu do Internetu.

Radca prawny powinien monitorować komunikaty dostawcy usług dotyczące dostępności czy planowanych przerw w funkcjonowaniu usługi i odpowiednio organizować pracę, aby takie okoliczności nie miały wpływu na jego usługi.

Czy radca prawny będzie informowany o incydentach bezpieczeństwa?

Dostawca powinien przekazywać radcy prawnemu informacje o incydentach bezpieczeństwa, w szczególności w celu umożliwienia mu spełnienia wymagań wynikających z regulacji dotyczących ochrony tajemnicy radcowskiej oraz wynikających z RODO. Zgodnie z RODO, w określonych poważnych przypadkach naruszenia ochrony danych osobowych, radca prawny jako administrator będzie miał obowiązek zawiadomienia o takim naruszeniu właściwego organu nadzorczego lub osób których dane dotyczą. Radca prawny powinien zadbać o to, aby umowa o powierzenie przetwarzania danych osobowych zawierana w ramach umowy na usługi przetwarzania w chmurze nakładała na usługodawcę takie obowiązki.

Na jakich zasadach organy państwa będą mogły mieć dostęp do danych przechowywanych w usługach chmurowych?

Policja lub inne organy wymiaru sprawiedliwości mogą w określonych w przepisach przypadkach uzyskiwać zgodnie z prawem dostęp do danych przechowywanych w usługach chmurowych, czy to poprzez radcę prawnego, czy też kierując żądanie bezpośrednio do dostawcy usługi chmurowej. Radca prawny powinien ustalić jakie obowiązki umowne ma dostawca usługi w takim przypadku. Zaleca się, aby dostawca usługi miał obowiązek, w granicach dopuszczalnych przepisami prawa, do powiadomienia o takim żądaniu radcy prawnego i umożliwienia mu podjęcia odpowiednich działań. W odniesieniu do danych szczególnie wrażliwych zamieszczanych w usługach chmurowych, radca prawny powinien rozważyć możliwość dodatkowego zabezpieczenia tych danych np. poprzez zaszyfrowanie przy wykorzystaniu własnych kluczy (zob. również Praktyczne wskazówki Rady Adwokatur i Stowarzyszeń Prawniczych Europy w zakresie poprawy bezpieczeństwa teleinformatycznego prawników przed bezprawnym nadzorem).

Czy umowa z dostawcą reguluje najważniejsze kwestie?

Umowa na usługi chmurowe, ze względu na szeroki i masowy zasięg takich usług, ma zazwyczaj charakter standardowy i adhezyjny. Umowy mogą składać się z wielu dokumentów. Ważne jest zatem ustalenie, czy radca prawny dysponuje kompletem dokumentów umownych. Radca prawny powinien zachować zawarte przez siebie umowy na usługi chmurowe.

Radca prawny powinien przeanalizować warunki umowy o usługi chmurowe oferowane przez dostawców usług chmurowych, w szczególności biorąc pod uwagę następujące kwestie:

- zakres usług;
- wykorzystywanie danych przez dostawcę usług online;
- zapisy dotyczące bezpieczeństwa, w tym uzyskiwania kopii audytów usług chmurowych;
- postanowienia dotyczące ochrony danych osobowych;

- postanowienia dotyczące przekazywania danych organom państw trzecich;
- zobowiązania dot. zachowania poufności;
- zasady odpowiedzialności;
- poziom dostępności zapisany w SLA i odpowiedzialność za niedotrzymanie SLA;
- podwykonawcy i prawo sprzeciwu wobec zmiany podwykonawcy;
- zakończenie usługi i usuwanie danych;
- zmiana warunków umowy i czas akceptacji zmiany;
- okres obowiązywania umowy, wypowiedzenie usługi.

Czy dostawca zapewniający transmisję danych (dostęp do Internetu) jest wiarygodny?

Dostawcy usług chmurowych nie odpowiadają za zapewnienie radcy prawnemu dostępu do Internetu, za pośrednictwem którego uzyskuje się dostęp do danych w usługach chmurowych. Radca prawny powinien upewnić się, czy dostawca Internetu zapewnia odpowiednie warunki techniczne takiej usługi, które będą umożliwiały ciągły, bezpieczny i komfortowy dostęp do tych danych. Dane w transmisji powinny być szyfrowane[4]. Dostawcy Internetu oferują też często specjalnie zabezpieczone połączenia na potrzeby usług chmurowych. Radca prawny powinien rozważyć, czy nie skorzystać z takiego rozwiązania.

W przypadku znacznego korzystania z usług chmurowych radca prawny powinien również zastanowić się nad posiadaniem dwóch dostawców dostępu do Internetu, aby zapewnić sobie ciągłość działania w przypadku awarii u jednego z nich.

4 Zob. również informacje dot. zapewnienia poufności komunikacji zawarte w Praktycznych Wskazówkach Rady Adwokatur i Stowarzyszeń Prawniczych Europy w zakresie poprawy bezpieczeństwa teleinformatycznego prawników przed bezprawnym nadzorem.

6.3 Prelegenci i autorzy rozdziału

Renata Zalewska

Renata Zalewska jako radca prawny Microsoft w swojej praktyce zawodowej zajmuje się kwestiami prawnymi dotyczącymi ochrony danych osobowych, prywatności, cyberbezpieczeństwa, usług IT w tym usług cloud computing z uwzględnieniem regulacji sektorowych.

Wcześniej Renata Zalewska była radcą prawnym takich firm z sektora IT jak: Dell Sp. z o.o. oraz Dell Products Poland Sp. z o.o., wspierając ich działalność sprzedażową w Warszawie i produkcyjną w rozwijającej się fabryce Della w Łodzi. Pełniła także regionalną funkcję Radcy Prawnego CA Technologies Sp. z o.o. („CA") koordynując wsparcie prawne spółek CA z obszaru Europy Środkowo-Wschodniej. Renata Zalewska rozpoczynała swoją karierę zawodową jako prawnik spółki Softbank S.A.

Renata Zalewska jest członkiem Okręgowej Izby Radców Prawnych w Warszawie, a także członkiem – założycielem Polskiego Stowarzyszenia Prawników Przedsiębiorstw.

Agata Szeliga

Agata Szeliga jest radcą prawnym, a od 2009 r. partnerem w kancelarii Sołtysiński Kawecki & Szlęzak.

Kieruje praktykami zajmującymi się prawem ochrony danych i prywatności oraz pomocy publicznej i zamówień publicznych. Reprezentuje klientów zarówno przed organami polskimi (sądami, organami administracji, w tym przed regulatorami – UODO i jego poprzednikiem GIODO oraz UKE), jak i przed Komisją Europejską.

W ramach praktyki prawa ochrony danych osobowych i prywatności zajmuje się w szczególności, przygotowywaniem umów i innych dokumentów w zakresie danych osobowych, analizą struktur biznesowych pod kątem zgodności z przepisami dotyczącymi ochrony danych osobowych, reprezentowaniem w postępowaniach dotyczących danych osobowych.

Realizowała również szereg projektów doradczych w zakresie licencjonowania i wdrażania oprogramowania oraz świadczenia usług związanych z oprogramowaniem, w tym dotyczących „cloud computing" oraz blockchain.

Publikacja pokonferencyjna została opracowana przez Treesk. sp. z o.o. na zlecenie Krajowej Izby Radców Prawnych. O ile nie zaznaczono inaczej, wszystkie fotografie wykorzystane w publikacji pochodzą z pixabay.com, Warszawa 2018

KRAJOWA IZBA RADCÓW PRAWNYCH
WARSZAWA 2018