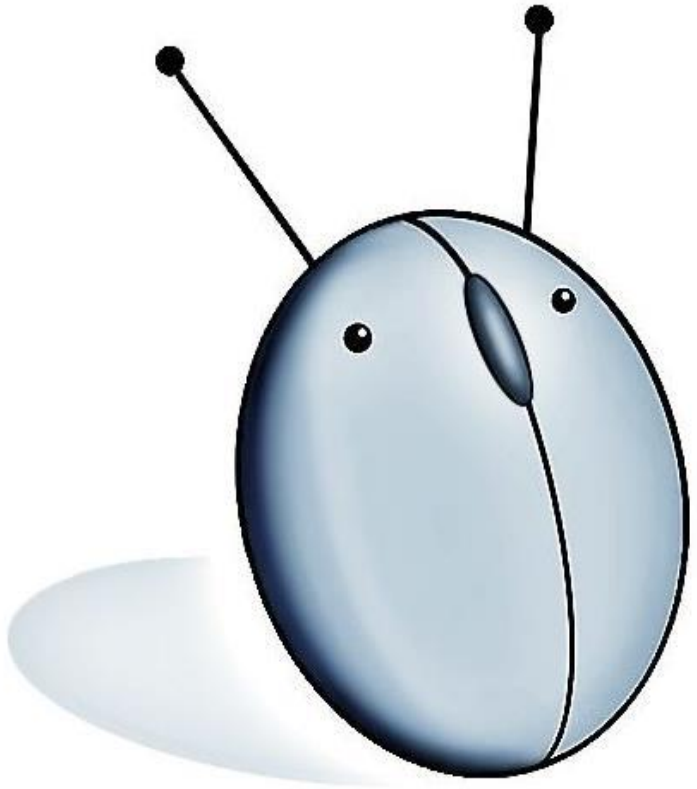
LegalTech Polska
TECH FOR LAW • LAW FOR TECH

Dekalog chmuroluba 2018 – wprowadzenie

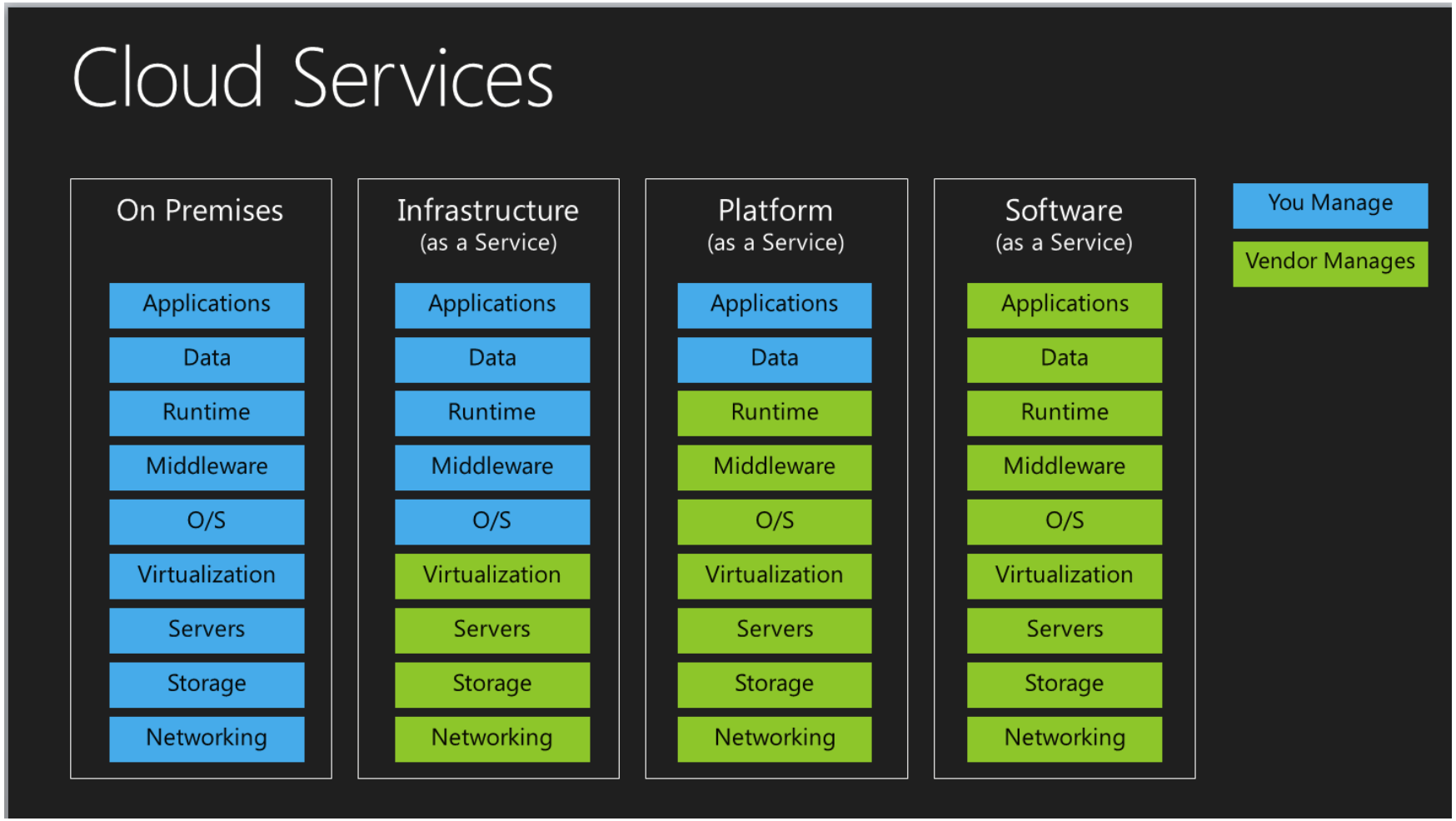
LegalTech Polska Meetup #8

26 kwietnia 2018 r.

Tomasz Zalewski
radca prawny



Saas, Paas i IaaS



Co to jest chmura?

Chmura to cudzy komputer

Co to jest chmura?

Chmura jest jak bank.
Przesyłasz swoje pieniądze, a następnie
pobierasz tyle, ile chcesz,
gdziekolwiek jesteś na świecie,
z bankomatu.

Co to jest chmura?

Chmura a własny komputer to
jak samochód autonomiczny a zwykły samochód.
I jedno i drugie służy do tego samego,
ale ryzyka z nimi związane są całkowicie różne.

Trzy akty prawne

- Ustawa o prawie autorskim i prawa pokrewnych
- Ustawa o usługach świadczonych drogą elektroniczną
- Rozporządzenie ogólne o ochronie danych osobowych (RODO)

Kłopoty prawników z chmurą

Art. 3 ustawy o radcach prawnych

*2. Radca prawny wykonuje zawód **ze starannością** wynikającą z wiedzy prawniczej oraz zasad etyki radcy prawnego.*

*3. Radca prawny jest **obowiązany zachować w tajemnicy** wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej.*

4. Obowiązek zachowania tajemnicy zawodowej nie może być ograniczony w czasie.

Kłopoty prawników z chmurą

Art. 23 kodeksu etyki radcy prawnego

Radca prawny obowiązany jest ***zabezpieczyć przed niepowołanym ujawnieniem*** *wszelkie informacje objęte 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.*

Kłopoty prawników z chmurą

Art. 35 kodeksu etyki radcy prawnego

Radca prawny może (…) wykonywać czynności zawodowe drogą elektroniczną, jeśli:

7) chroni tajemnicę zawodową, informując w treści korespondencji elektronicznej o jej poufnym charakterze; ***zabezpieczenie uznaje się za należyte, jeżeli 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****.*

Nisko zawieszona poprzeczka… ale…

- Dane muszą być zabezpieczone
- Standardy zabezpieczeń nie są dookreślone
- Zgoda klienta (poinformowanego o ryzykach) zwalnia z odpowiedzialności dyscyplinarnej
- Jednak nawet zgoda klienta nie zwalnia z odpowiedzialności np. za naruszenie RODO

Podejście oparte na ryzyku

- Analiza ryzyk
- Ustalenie ich wagi
- Ustalenie możliwych sposobów na zabezpieczenie przed tymi ryzykami
- Podjęcie decyzji
- Poinformowanie klienta

- Decyzja może być różna w zależności od zidentyfikowanych ryzyk oraz ustalenia ich wagi w konkretnej sytuacji

Podejście oparte na ryzyku

Ryzyka ogólne wynikające z specyfiki chmury:

1. Ryzyko poufności i integralności danych w czasie transferu przez Internet
2. Ryzyko braku dostępności do Internetu
3. Ryzyko dostępu osób trzecich (w tym służb specjalnych)
4. Ryzyko luk w procedurach i środkach bezpieczeństwa stosowanych przez usługodawców
5. Ryzyko braku możliwości audytu lub jego weryfikacji
6. Vendor lock-in
7. Ryzyka wynikające z użycia oprogramowania klienckiego (przeglądarki)

Umowa

- Usługa chmurowa to przede wszystkim **umowa**
- Umowa, w której trzeba uregulować:
  - Zasady korzystania z usługi
  - Oferowane usługi i ich zakres
  - Zasady dostępu do usługi
  - Zasady płatności
  - Zasady przedłużania/rozwiązania
  - Zasady usuwania błędów i awarii
  - Zasady przetwarzania danych osobowych
  - Zasady zmiany zakresu funkcjonalności
  - Zasady wzajemnej kontroli przez strony jej przestrzegania
  - Etc.

Dekalog chmuroluba – propozycja checklisty dla użytkownika i dostawcy

- Chmura to zawieranie umów zazwyczaj poprzez akceptację regulaminu
- Chmura to konieczność ujednolicenia nie tylko usługi ale i zasad korzystania z niej
- Jednak jeśli regulamin jest jednostronny, to wielu klientów zrezygnuje z usługi
- Jak zatem uregulować zagadnienia istotne dla obu stron i tak, aby obie uznały je za satysfakcjonujące?
- Dekalog chmuroluba – próba stworzenia listy kontrolnej
- W każdej umowie muszą być uregulowane zagadnienia z Dekalogu

Przykazanie pierwsze – oferowana usługa i jej zakres musi być opisany

- Regulamin to umowa
- Klienta interesuje jednak w pierwszej kolejności, co konkretnie kupuje:
  - jakie funkcjonalności
  - jakie są ograniczenia tych funkcjonalności
  - czy planowane są nowe
  - czy planowane są zmiany
  - do czego zobowiązuje się dostawca (czy do należytej staranności czy do konkretnego rezultatu?)
- Dostawca też lepiej będzie zabezpieczony, jeśli:
  - wskaże dokładnie co oferuje, a co nie
  - określi planowane zmiany w tym zakresie
- Opis niekoniecznie w regulaminie, raczej w odrębnym dokumencie
- Czy dostawca gwarantuje zgodność usługi np. z obowiązującym prawem?

Przykazanie drugie – jakość usług powinna być konkretna

- Service Level Agreement (SLA)
- Standardy świadczenia usług (dostępność, zasady kalkulacji wskaźników etc.)
- Zasady raportowania o jakości usług
- Zasady postępowania w razie problemów (usuwanie błędów i awarii, czas reakcji, czas usunięcia problemu)
- Zasady postępowania, gdy jakość jest poniżej gwarantowanego (np. tzw. kredyty)
- Zasady przeprowadzania prac konserwacyjnych

Przykazanie trzecie – sposób świadczenia usługi powinien być określony

- W przypadku chmury nie obowiązuje zasada, że klienta nie powinno interesować, jak dostawca zapewnia świadczenie usługi

- Dostawca powinien wskazać klientowi:
  - Gdzie znajdują się fizycznie serwery i inna infrastruktura, z których korzysta do świadczenia usługi (i powiadomić o zmianach)
  - Czy korzysta z podwykonawców, a jeśli tak, to z których konkretnie i co oni robią (i powiadomić klienta o zmianach)

- Dane te są potrzebne:
  - w celu oceny ryzyk prawnych
  - W celu oceny ryzyk faktycznych
  - W celu oceny kwestii dotyczących przetwarzania danych osobowych

Przykazanie czwarte – sposoby zapewnienie bezpieczeństwa świadczonych usług muszą być opisane

- Zobowiązania umowne dotyczące poufności są zobowiązaniami formalnymi
- Klient powinien wiedzieć konkretnie, jak poufność i bezpieczeństwo jego danych będzie zapewnione
- Jeśli oferowane jest szyfrowanie, stosowany mechanizm powinien być dokładnie opisany
- Klient powinien być powiadamiany o wszystkich incydentach bezpieczeństwa!
- Dostawca powinien wskazać klientowi:
  - Jakie stosuje środki bezpieczeństwa w odniesieniu do swojej infrastruktury?
  - Jak klient może uzyskać dostęp do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych dot. bezpieczeństwa?
  - Jak robi kopie bezpieczeństwa? Jak często?
- Zapewnienia dotyczące bezpieczeństwa danych powinny być weryfikowalne
  - Zgodność z normami ISO (innymi standardami) potwierdzona
  - Regularny audyt plus audyty w razie incydentów bezpieczeństwa
  - Dostęp klienta do wyników audytów

Przykazanie piąte – zasady odpowiedzialności powinny być dookreślone

- Chmura może być funkcjonalnym odpowiednikiem umowy licencyjnej na program komputerowy, ale ryzyko dla użytkownika jest znacznie wyższe!
- Awaria u dostawcy może oznaczać paraliż działalności klienta!
- Dostawcy bardzo ograniczają swą odpowiedzialność, w zamian często powołując się na swoją „wiarygodność biznesową”
- Cyberbezpieczeństwo to klasyczny „ruchomy cel” – można starać się je zapewnić, ale nie zagwarantować
- Umowa powinna:
  - wskazywać wyraźnie na wyłączenia odpowiedzialności
  - wskazywać, czy dostawca jest ubezpieczony

Przykazanie szóste – dane osobowe chronione zgodnie z RODO

- Na podstawie RODO odpowiedzialność za naruszenie przepisów o ochronie danych osobowych ponosi zarówno klient jak i dostawca
- Powierzenie danych osobowych do przetwarzania zgodne z RODO
- Dostawca musi zapewnić usunięcie lub zwrot danych osobowych po zakończeniu świadczenia usług
- Dostawca musi spełnić szczególne warunki w sytuacji transferu danych osobowych za granicę, do kraju innego niż należący do EOG

Przykazanie siódme – klient musi mieć prawo do odzyskania swoich danych

- Na podstawie RODO dostawca musi zapewnić przenoszalność danych osobowych
- To wymaganie to wierzchołek góry lodowej
- W chmurze przetwarza się także dane nieosobowe np. dotyczących sprzedaży, stanów magazynowych, dane eksploatacyjne
- Dostawca musi zapewnić klientowi przenoszalność danych
- Umowa musi być szczegółowa w zakresie przenoszalności danych:
  - format danych
  - odpowiednie terminów na dokonanie eksportu
  - udostępnienie narzędzi do eksportu
  - koszt eksportu w razie, gdy dostawca nie zapewnia stosownych narzędzi
- Przenoszalność danych staje się krytyczna w razie rozwiązania umowy!

Przykazanie ósme – zakończenie korzystania z usługi to nieuchronne zdarzenie

- Zakończenie korzystania z usługi chmurowej to spory kłopot dla klienta
- Jeśli nie ma oprogramowania alternatywnego, musi znaleźć innego dostawcę i przenieść dane
- Zasady rozwiązywania umowy powinny być klarowne i jasne
- Co do zasady rozwiązanie przed terminem tylko w razie naruszenia umowy, w tym zaległości płatniczych
- Mechanizm przedłużania umowy na kolejne okresy
- Dostawcy chętnie ulegają pokusie stworzenia mechanizmu vendor lock-in, ale czy to się opłaca na dłuższą metę?
- A co w przypadku upadłości dostawcy? Czy klienci powinni oczekiwać rozwiązania od dostawcy (np. escrow?)

Przykazanie dziewiąte – ureguluj kwestie specyficzne dla usługi świadczonej drogą elektroniczną

- Dostawca usługi chmurowej nie ponosi odpowiedzialności za dane klienta, jednak jeśli zostanie powiadomiony, może zacząć za nie odpowiadać
- Dostawca nie ma obowiązku monitorowania danych klienta pod kątem nielegalnych treści
- Plany Komisji Europejskiej wprowadzenia zmian w odniesieniu do większych podmiotów
- Umowa musi przewidywać mechanizmy pozwalające na szybkie reagowanie w razie otrzymania zawiadomienia przez dostawcę, że dane klienta mogą naruszać prawo

Przykazanie dziesiąte – zasady dostępu osób trzecich muszą być ścisłe

- Media donoszą o przypadkach, gdy dostawca usługi chmurowej bez wiedzy klientów uzyskiwał dostęp do ich danych lub udostępnił taki dostęp policji, służbom specjalnym, prokuraturze etc.
- Problem backdoorów – świadomie wbudowanych lub ukrytych tam przez hackerów
- Problem ustawodawstw innych państw, gdzie mogą być serwery
  - Dostęp służb USA do danych innych podmiotów niż obywatele amerykańscy (The Patriot Act)
- Umowa powinna regulować wyraźnie kwestie związane z żądaniami osób trzecich dot. dostępu do danych klienta
- Najważniejsza jest transparentna informacja na linii dostawca - klient

Dekalog SaaS

I. **Pierwsze** – oferowana usługa i jej zakres musi być opisany
II. **Drugie** – jakość usług powinna być konkretna
III. **Trzecie** – sposób świadczenia usługi powinien być określony
IV. **Czwarte** – sposoby zapewnienie bezpieczeństwa świadczonych usług muszą być opisane
V. **Piąte** – zasady odpowiedzialności powinny być dookreślone
VI. **Szóste** – dane osobowe chronione zgodnie z RODO
VII. **Siódme** – klient musi mieć prawo do odzyskania swoich danych
VIII. **Ósme** – zakończenie korzystania z usługi to nieuchronne zdarzenie
IX. **Dziewiąte** – ureguluj kwestie specyficzne dla usługi świadczonej drogą elektroniczną
X. **Dziesiąte** – zasady dostępu osób trzecich muszą być ścisłe

LegalTechPolska
TECH FOR LAW • LAW FOR TECH

Kontakt:

Fundacja LegalTech Polska
Tomasz Zalewski
+48 502 18 45 96

tomasz.zalewski@legaltechpolska.pl
Twitter: @tomasz_zalewski
https://legaltechpolska.pl/