Hosting a dane osobowe

Powierzać, albo nie powierzać?

Jarosław Żabówka
proinfosec@odoradca.pl

proInfoSec

Plan

- Powierzenie danych – krótkie przypomnienie
- Hosting – próba definicji
- Co oferują nam dostawcy
- Kiedy powinniśmy powierzać – próba odpowiedzi
- Zgłoszenia zbioru – jakie zabezpieczenia wpisać?
- Umowa niepowierznia?

Powierzanie

- Art. 31 ust. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
  - Powierzamy dane, a nie zbiór danych!
  - Umowa na piśmie?
  - Jeżeli nie podpiszemy umowy – udostępniamy dane.

Umowa powierzenia

- Art. 31 ust. 2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.
  - Umowa musi zawierać:
    - Cel przetwarzania
    - Zakres powierzanych danych
  - Umowa powinna zawierać:
    - Co się stanie z danymi, po zakończeniu umowy (pamiętajmy o kopiach bezpieczeństwa)
    - Zabezpieczmy swoje prawa, bo:

Umowa powierzenia - odpowiedzialność

- Art. 31 ust. 4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

  – ADO v Procesor – kto odpowiada w jakim zakresie?

Obowiązek procesora – zabezpieczenie danych

- Art. 31 ust. 3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

Przetwarzający musi

- Zastosować zabezpieczenia techniczne i organizacyjne
- Do przetwarzania dopuścić jedynie osoby upoważnione
- Wydać upoważnienia i prowadzić ewidencję
- Zapewnić kontrolę jakie dane i przez kogo zostały wprowadzone do zbioru
  - A jeżeli dane nie są w zbiorze?
  - Czy również w zakresie przetwarzania przez ADO?
- Spełniać wymagania wynikające z rozporządzenia

Ustawa o świadczeniu usług drogą elektroniczną

- Wyłączenie z odpowiedzialności
  - Art. 14. ust. 1. Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, (…)
  - Art. 15. Podmiot, który świadczy usługi określone w art. 12-14, nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych, o których mowa w art. 12-14.

Hosting – z punktu widzenia usude

- Brak definicji legalnej
- Czy hosting oznacza zawsze udostępnianie danych podmiotom trzecim?
- Usługodawcą bywają osoby korzystające z serwisu

Hosting z punktu widzenia dostawcy

- Hosting współdzielony
  - Najczęściej – web hosting
  - Współdzielone zasoby
  - Problemy z wydajnością i stosunkowo niskie bezpieczeństwo
- Serwer wirtualny (VPS)
  - Otrzymujemy do dyspozycji maszynę wirtualną
- Managed VPS
  - Otrzymujemy system na maszynie wirtualnej
- Serwer fizyczny
  - Otrzymujemy do własnej dyspozycji serwer fizyczny
- Kolokacja (hoteling)
  - Korzystamy z własnego serwera zainstalowanego w serwerowni dostawcy
- ...

Kiedy powinniśmy podpisać umowę powierzenia?

- Gdy dostawca przetwarza dane?
- Gdy umożliwiamy dostawcy dostęp do danych?
  - Art. 51. 1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je **lub umożliwia dostęp** do nich osobom nieupoważnionym, podlega karze (…)

Dostawcy

- *„Oczywiście, mamy przygotowaną umowę powierzenia”*
- *„Mamy certyfikat GIODO i możemy dać takie oświadczenie. Nie – umowy nie podpiszemy”*
- *„Klient ma prawo wystąpić do GIODO o przeprowadzenie procesu certyfikacji na własny koszt”*
- *„My nie mamy dostępu do Państwa danych”*
- *„Kiedyś pisałem do GIODO i mi nie odpowiedzieli, to ja ich też olewam”*
- *„Jeżeli Państwo chcecie, to możemy podpisać taką umowę, przecież tego i tak nikt nie sprawdzi”*
- *„Hosting zgodny z GIODO”*

Praktyka

- Czy GIODO wymaga serwera dedykowanego?
  - *„Zgodnie z wymaganiami GIODO kupiłem serwer dedykowany”*(?)
- Kupujemy moduł, szafę, pół szafy, 1U…
  - Inni klienci nie mają dostępu do moich zasobów. Czy na pewno?
- Remote hand
  - Czy serwisant wymieniający zasilacz powinien być upoważniony do przetwarzania danych?
  - A jeżeli administruje systemem?

Problemy

- Dostawcy nie są zainteresowani podpisaniem umów powierzenia
- Brak możliwości weryfikacji zabezpieczeń
- Szyfrujemy dane na dyskach, szyfrujemy komunikację, a i tak dostawca ma dostęp np. w ramach usługi „rescue mode”
- Jaki poziom szyfrowania oznacza, że dostawca nie ma dostęu do danych?
- Nawet w wypadku kolokacji, gdy rzeczywiście tylko my mamy dostęp do serwera, pozostaje jeszcze infrastruktura sieciowa, taśmy z kopiami,…

Umowa o niepowierzaniu

- Czy gdy dzierżawię szafę w data center, to oznacza, że dostawca przechowuje (czyli przetwarza) moje dane – uważam, że nie.
- Jeżeli jednak serwisant ma dostęp do szafy, to może mieć do nich dostęp. Dlatego podpisujemy umowę powierzenia, mimo, że nie chcemy żeby dostawca przetwarzał nasze dane…
- Wprowadźmy umowę niepowierzania danych.

Dane osobowe w chmurze

Czy w ogóle jest o czym mówić?

Plan

- Chmura – czyli co?
- Klasyfikacja chmur
- Nowe wyzwania dla bezpieczeństwa
- Dane osobowe w chmurze?

Definicja

- Ciągle brak jednoznacznej definicji
- Definiujemy poprzez różne modele
- Dużo produktów nazywamy chmurami, ze względów marketingowych
- Chmura – świadczone z wykorzysaniem technik wirtualizacji usługi, często rozliczane poprzez rzeczywiście zużyte zasoby (czas procesora, energia elektryczna).

Nie mówimy tu o

- Chmurze telekomunikacyjnej (CaaS)
- „Pseudochmurze” oferowanej przez małych dostawców usług hostingowych. Oferują oni zwykłe usługi hostingowe, sprzedając zakupione po hurtowych usługi hostingowe.
  - Duży problem z podpisaniem umowy powierzenia
  - Nigdy nie wiemy, kiedy nasze zasoby zostaną przeniesione do innego podprocesora
  - Z natury będziemy mieli do czynienia z podpowierzeniem.

Rodzaje chmur (Deployment Models)

- Chmura prywatna

- Community cloud

- Chmura publiczna

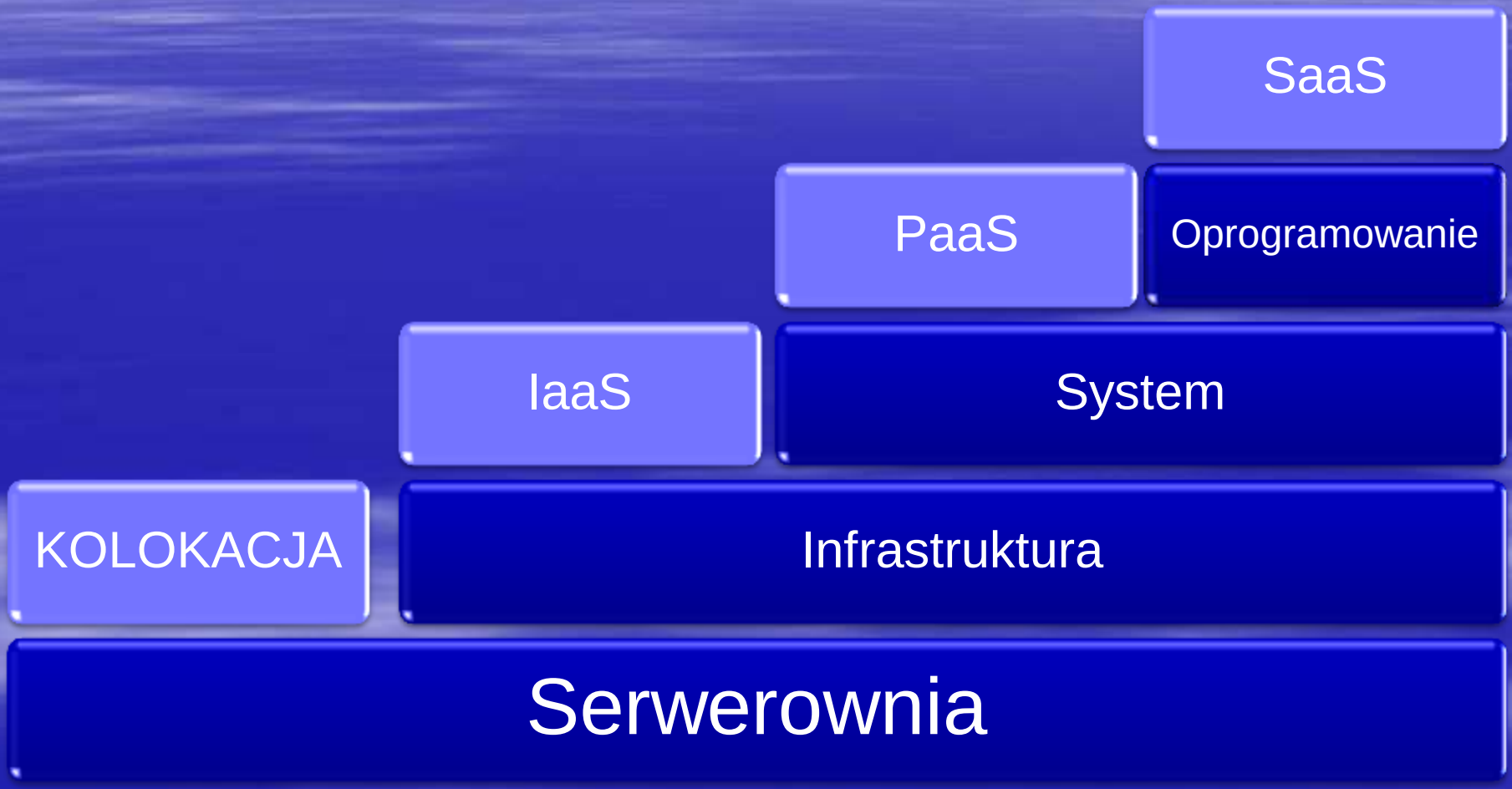
- Zewnętrzna chmura prywatna

- Chmura hybrydowa

Rodzaje chmur a ODO

- Chmura prywatna
  - Pozostaje pod kontrolą organizacji – nie różni się od własnej serwerowni
- Community cloud
  - Zależy od przyjętego modelu.
- Chmura publiczna
  - Nie różni się istotnie od hostingu.
  - Zależnie od udostępnianych zasobów, może stwarzać więcej dylematów co do zawartości umowy powierzenia.
  - U dużych dostawców, praktycznie tracimy kontrolę nad danymi.
- Dzierżawiona chmura prywatna
  - W praktyce nie różni się od kolokacji lub hostingu
- Chmura hybrydowa

Modele chmur (Service Models)



Modele chmur

- Kolokacja
  - Nie zawsze traktowana jako chmura
- IaaS
  - Czasami nazywane HaaS (Host as a Service)
  - Usługi typu VPS, serwer dedykowany – nie różni się od hostingu
- PaaS
  - Dostawca dostarcza nam platformę systemową (np. system na maszynie wirtualnej)
  - W praktyce konieczne będzie podpisanie umowy powierzenia
- SaaS
  - Dostawca dostarcza nam oprogramowanie dla końcowego użytkownika
  - Podpisanie umowy powierzenia zwykle będzie konieczne.

Inne modele

- Intercloud
- BpaaS
- Cloud storage
- Cloud database

Chmury a ODO

- Teza: Chmury generalnie nie stanowią nowej jakości z punktu widzenia ochrony danych osobowych.
- Problemem mogą być chmury publiczne. Wydaje się, że nie powinno się wykorzystywać tych rozwiązań dla przetwarzania danych osobowych i innych wrażliwych dla organizacji informacji (np. problemy z DropBox-em)

Bezpieczeństwo informacji

- Rozwiązania wprowadzają nowe podatności
- Właściwie dobrane, wdrożone i zarządzane chmury, mogą podnieść poziom bezpieczeństwa informacji.
- Chmury mogą zostać wykorzystane dla zapewnienia ciągłości działania.
- Chmura może podnieść poziom dostępności danych (ale złe rozwiązanie, może go drastycznie obniżyć)

Ryzyka CC wskazywane przez Garnera

- Personel dostawcy
- Zgodność z przepisami
- Lokalizacja danych
- Separacja danych różnych klientów
- Odzyskiwanie danych
- Wsparcie wyszukiwania nielegalnych operacji
- Długoterminowa dostępność

http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

Cloud Security Alliance

- https://cloudsecurityalliance.org/
  - „Top Threats to Cloud Computing”
  - „Security Guidance for Critical Areas in Cloud Computing”

Top Threats to Cloud Computing

- Abuse and Nefarious Use of Cloud Computing (IaaS, PaaS)
- Insecure Interfaces and APIs (IaaS, PaaS, SaaS)
- Malicious Insiders (IaaS, PaaS, SaaS)
- Shared Technology Issues (IaaS)
- Data Loss or Leakage (IaaS, PaaS, SaaS)
- Account or Service Hijacking (IaaS, PaaS, SaaS)
- Unknown Risk Profile (IaaS, PaaS, SaaS)

Bardzo dziękujemy za uwagę
i zapraszamy do dyskusji.