CHMURA OBLICZENIOWA

(CLOUD COMPUTING)

jako nowy model biznesu

Spojrzenie z perspektywy RODO

Tadeusz Wachowski

CHMURA OBLICZENIOWA vs. RODO

Chmura obliczeniowa w przepisach o ochronie danych osobowych

- Ustawa o ochronie danych osobowych
- Opinia 5/2012 Grupy Roboczej Art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej

Cloud Computing czyli chmura obliczeniowa

- Zgodnie z definicją opracowaną przez Grupę Roboczą Artykułu 29 ds. Ochrony Danych „**cloud computing** obejmuje zestaw technologii i modeli usług, które koncentrują się na wykorzystywaniu i dostarczaniu poprzez Internet aplikacji informatycznych, możliwości przetwarzania, zasobów pamięci";
- Przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922) nie określają zasad dotyczących przetwarzania danych osobowych w chmurze obliczeniowej, co powoduje utrudnienia w korzystaniu z tego typu usługi w jednostkach organizacyjnych;

Pojęcie „przetwarzania danych w chmurze obliczeniowej" nie jest obecnie uregulowane w przepisach prawa.

CHMURA OBLICZENIOWA

Pojęcie chmury nie jest jednoznaczne, w szerokim znaczeniu przetwarzanym w chmurze (outsorcing) jest wszystko to, co jest przetwarzane poza infrastrukturą informatyczną instytucji (ale dostępne przez sieć publiczną).

Jest kilka definicji chmury obliczeniowej (1/2):

- Chmura obliczeniowa to **usługa** polegającą na zdalnym udostępnieniu mocy obliczeniowej urządzeń IT lub aplikacji, oferowana przez zewnętrzne podmioty (outsourcing), **dostępną na żądanie** w dowolnej chwili, można ją skalować w miarę potrzeb.
- Chmura obliczeniowa to **model przetwarzania danych** oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzna organizacja). Chmura to usługa, **dająca wartość dodaną** użytkownikowi, oferowana przez infrastrukturę i oprogramowanie.

CHMURA OBLICZENIOWA

Jest kilka definicji (2/2):

- Chmura obliczeniowa jest **alternatywą** dla własnego centrum danych, nie wymagającą poniesienia nakładów inwestycyjnych na budowę własnej infrastruktury data center.
- Termin „chmura obliczeniowa” wiąże się z pojęciem "**wirtualizacji**".
- Zasada działania polega na **przeniesieniu odpowiedzialności** za świadczenie usług IT (przetwarzania danych, licencji oprogramowania, mocy obliczeniowej) na zewnętrzną infrastrukturę i umożliwienie stałego dostępu poprzez komputery klienckie.

CHMURA OBLICZENIOWA

Chmura obliczeniowa może być udostępniana jako:

- **prywatna** (ang. private cloud), będąca częścią organizacji, aczkolwiek jednocześnie jest autonomicznym dostawcą usługi,
- **publiczna** (ang. public cloud), będąca zewnętrznym, ogólnodostępnym dostawcą (np. Google Cloud, Microsoft Azure, Apple iCloud, itp.),
- **hybrydowa** (ang. hybrid cloud), będąca połączeniem zasad funkcjonowania chmury prywatnej i publicznej.

CHMURA OBLICZENIOWA

Ogólna klasyfikacja usług chmury obliczeniowej (1/2):

- **Platform as a Service** – PaaS (z ang. „platforma jako usługa") – zazwyczaj to sprzedaż dostosowanego do potrzeb użytkownika **kompletu aplikacji**. Korzystanie z PaaS nie wiąże się z koniecznością zakupu sprzętu ani instalacją oprogramowania. **Wszystkie potrzebne** programy **znajdują się na serwerach dostawcy.** Klient po swojej stronie ma dostęp do interfejsu poprzez program – klienta, np. przeglądarkę internetową.

  W tym modelu usługi najczęściej dostępne są dla użytkownika z dowolnego komputera połączonego z siecią publiczną (Internetem).

- **Software as a Service** – SaaS (z ang. „oprogramowanie jako usługa") – klient otrzymuje **konkretne, wybrane funkcje** oprogramowania. Korzysta z takiego **oprogramowania, jakiego aktualnie potrzebuje**. Klient ma jedynie zapewniony dostęp do konkretnych, funkcjonalnych narzędzi (niekoniecznie połączonych ze sobą jednolitym interfejsem), nie interesuje go ani infrastruktura, ani środowisko pracy.

  Programy działają na serwerze dostawcy, a klient nie jest zmuszony nabywać z tytułu ich użycia licencji. **Płaci** jedynie **za każdorazowe ich użycie**, a dostęp do nich uzyskuje na żądanie.

CHMURA OBLICZENIOWA

Ogólna klasyfikacja usług chmury obliczeniowej (2/2):

- **Infrastructure as a Service** - IaaS (z ang. „infrastruktura jako usługa") – model polegający na dostarczaniu klientowi **infrastruktury informatycznej**, czyli sprzętu, oprogramowania oraz usług serwisu. Przykładowo, klient wykupuje konkretną liczbę serwerów (wirtualnych serwerów), przestrzeni dyskowej lub określony zasób pamięci i mocy obliczeniowej. Nie oznacza to jednak, że sprzęt fizycznie zostanie zainstalowany w siedzibie klienta. W tym modelu zdarza się, że klient dostarcza usługodawcy własne oprogramowanie do zainstalowania na wynajmowanym sprzęcie.

Uwaga, nie zapominajmy o najstarszej znanej formie usług świadczonych w chmurze – **kolokacji**.

Kolokacja polega na **wynajęciu pomieszczenia** serwerowni, dostępu do energii elektrycznej, klimatyzacji i dostępu do Internetu. Pozostałe składniki – sprzęt, zabezpieczenia (zapory), zarządzanie obciążeniem, system operacyjny, oprogramowanie i aplikacje opłaca firma korzystająca.

OCHRONA DANYCH W CHMURZE

Przetwarzanie danych osobowych w chmurze obliczeniowej, pomimo korzyści ekonomicznych związanych z korzystaniem z takiej usługi, może powodować wiele zagrożeń.

W szczególności będą to:

- możliwość braku kontroli nad danymi osobowymi;
- niewystarczające informacje na temat tego, w jaki sposób, gdzie i przez kogo dane osobowe są przetwarzane;
- brak wpływu na prawidłowe działania udostępnionej infrastruktury.

Administrator danych osobowych, zanim zdecyduje się skorzystać z rozwiązania typu „chmura”, powinien przede wszystkim określić swoje potrzeby oraz **szczegółowo przeanalizować umowę**, którą proponuje dostawca usługi, tak aby zostały zapewnione ujęte w przepisach (i normach) standardy przetwarzania danych osobowych.

OCHRONA DANYCH W CHMURZE

Kilka słów przypomnienia:

Dane osobowe – to wszelkie informacje dotyczące zidentyfikowanej osoby lub dane umożliwiające jednoznaczne zidentyfikowanie osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na specyficzne czynniki określające jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

Administrator danych osobowych - to podmiot decydujący zarazem o celach i środkach przetwarzania danych;

Przetwarzanie danych - to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

Zbiór danych – to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

Podmiot przetwarzający - to podmiot, który przetwarza dane osobowe w imieniu administratora.

O administratorze i podmiocie przetwarzającym mówi Rozdział IV RODO – art. 24-43

RODO/GDPR

Istotne fakty

- data wejścia w życie RODO – 24 maja 2016 r.;
- data rozpoczęcia obowiązywania RODO – 25 maja 2018 r.;
- okres dostosowawczy (okres pomiędzy datą wejścia w życie i datą obowiązywania RODO).

Najważniejsze konsekwencje prawne dla usługobiorców „chmury obliczeniowej”

- nowe wymogi odnośnie wyboru procesora;
- nowe obowiązki dla procesorów;
- procesorzy będą mogli być adresatami decyzji nakładających kary pieniężne;
- nowe mechanizmy wykazywania zgodności z przepisami o ochronie danych osobowych.

RODO/GDPR

1. Nowe wymogi odnośnie wyboru procesora (art.28 ust.1)

Administrator ma obowiązek korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą (art.28 ust.1)

RODO/GDPR

2. Nowe zasady odpowiedzialności (m.in. art. 82 i nast.)

Administrator może ponosić:

- odpowiedzialność administracyjną za procesora na zasadach określonych w art.58 ust.2 (środki naprawcze), sporna jest możliwość nakładania kar pieniężnych (art. 83);
- odpowiedzialność cywilnoprawną (w pewnych przypadkach odpowiedzialność solidarna z procesorem) (art.82).

Procesor może ponosić:

- odpowiedzialność administracyjną i cywilnoprawną określoną w RODO (art. 82);
- dodatkowo - jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania (art.28 ust.10).

RODO/GDPR

3. Nowe zasady dotyczące bezpieczeństwa danych (art.32 i nast.)

- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów oraz usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- pseudonimizacja i szyfrowanie danych osobowych;
- regularne testowanie i ocena skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania;
- oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- wywiązywanie się z w/w obowiązków można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

RODO/GDPR

4. Nowe sposoby wykazywania zgodności z przepisami o ochronie danych osobowych – (art.40 i nast.)

- odpowiednia dokumentacja (np. na podstawie analiza ryzyka przetwarzania danych, stwierdzonych naruszeń ochrony danych osobowych);
- stosowanie innych zatwierdzonych mechanizmów certyfikacji;
- przystąpienie do zatwierdzonych kodeksów postępowania.

5. Nowe obowiązki administratorów danych, wymagające wsparcia ze strony procesorów

- powiadomień o naruszeniach bezpieczeństwa danych;
- oceny skutków przetwarzania, etc.

6. Nowe wymogi odnośnie treści umów powierzenia przetwarzania danych osobowych (art.28 ust.3)

- podstawą przetwarzania jest umowa, której treść została zmodyfikowana w stosunku do dotychczasowego stanu prawnego (art.28 ust.3) - uwzględniając charakter przetwarzania oraz dostępne mu informacje, procesor **musi zobowiązywać** się do pomagania administratorowi wywiązać się z obowiązków określonych w art. 32–36 (bezpieczeństwo danych, powiadamiania o naruszeniach, ocena skutków przetwarzania danych z uwagi na wysokie ryzyko dla podmiotów danych)

CHMURA OBLICZENIOWA a RODO

Podstawy zgodnego z rozporządzeniem RODO przetwarzania danych osobowych

- Zapewnienie podstaw prawnych przetwarzania;
- Wypełnienie obowiązków informacyjnych;
- Analiza ryzyka;
- Zabezpieczenie zbioru danych osobowych;
- Obowiązek prowadzenia **rejestru czynności** przetwarzania danych osobowych (art. 30 – Rejestrowanie czynności przetwarzania)

W przepisach unijnego Rozporządzenia (RODO) **zrezygnowano z obowiązku rejestracji zbiorów** danych osobowych, co oznacza, że po 25 maja 2018, zbiorów danych osobowych nie będzie trzeba rejestrować w GIODO. Rejestr prowadzony przez administratora danych powinien zawierać:

- Imię i nazwisko lub nazwę administratora, dane kontaktowe administratora oraz wszystkich współadministratorów;
- Cel przetwarzania danych;
- Jeśli administrator danych powoła inspektora ochrony danych – w rejestrze należy wskazać jego imię i nazwisko oraz dane kontaktowe;
- Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

CHMURA OBLICZENIOWA a RODO

Podstawy zgodnego z rozporządzeniem RODO przetwarzania danych osobowych – rejestr czynności

Przepisy RODO przewidziały wyjątek od **obowiązku prowadzenia rejestru** czynności przetwarzania (art. 30).

Obowiązek ten nie będzie miał zastosowania w sytuacji gdy administrator danych zatrudnia mniej niż 250 osób, lecz mimo tego obowiązek taki będzie zawsze istniał względem administratorów, gdy przetwarzanie, którego dokonują:

- Może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
- Nie ma charakteru sporadycznego;
- Obejmuje szczególne kategorie danych osobowych;
- Obejmuje dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO.

Biorąc pod uwagę powyższe, większość administratorów danych będzie musiała prowadzić przedmiotowy rejestr gdyż proces przetwarzania danych osobowych rzadko będzie odbywał się sporadycznie.

Uwaga! Na **procesorze** będzie spoczywał **obowiązek prowadzenia rejestru**, tzw. rejestru czynności przetwarzań dokonywanych w imieniu administratora. Procesor będzie musiał w każdym przypadku, w którym zostają mu powierzone dane osobowe, prowadzić taki rejestr.

CHMURA OBLICZENIOWA a RODO

Kilka słów podsumowania, czyli kto jest kim w „chmurze”?

Administrator danych osobowych (ADO), to **KLIENT** usług świadczonych w chmurze

Administrator to podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art.4 RODO).

Podmiot przetwarzający (procesor) to podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 RODO), to **DOSTAWCA** usługi w chmurze – bo przetwarza nasze dane.

Procesorem jest dostawca usługi, przetwarza on bowiem dane osobowe w imieniu i na rzecz administratora danych (ADO). Na mocy umowy realizuje cel ściśle określony przez administratora i nie ma uprawnień do podejmowania innych czynności, niezwiązanych z tym celem.

Podmioty świadczące usługi przetwarzania danych w chmurze zobowiązane są przetwarzać te dane w celu i zakresie określonym w umowie powierzenia, o której mowa w art. 29 RODO. Administrator danych powinien określić cel **jeszcze przed zebraniem** danych, na wypadek zaistnienia konieczności **wyrażenia zgody** przez osoby, których dane dotyczą.

CHMURA OBLICZENIOWA a RODO

Funkcje Administratora Danych (Klienta)

- Określenie ostatecznego celu przetwarzania;
- Decydowanie o powierzeniu przetwarzania;
- Oddelegowanie wszystkich/części działań w zakresie przetwarzania zewnętrznej organizacji;
- Odpowiedzialność za przestrzeganie przepisów w zakresie ochrony danych osobowych.

Obowiązki Administratora Danych (Klienta)

- Zapewnienie legalności (podstawa prawna przetwarzania);
- Wypełnienie obowiązku informacyjnego;
- Zgłoszenie zbioru do rejestracji (obecnie), a po 25.05.2018 - prowadzić rejestr czynności;
- Zapewnienie bezpieczeństwa danych (wdrożenie odpowiednich środków organizacyjnych i technicznych).

CHMURA OBLICZENIOWA a RODO

Funkcje dostawcy (Procesora)

- Dostarczenie środków oraz platformy klientowi;
- Zapewnienie poufności;
- Zapewnienie fizycznego bezpieczeństwa danych;
- Pozostałe funkcje zdefiniowane w umowie pomiędzy administratorem a przetwarzającym.

Obowiązki dostawcy (Procesora)

- Szereg obowiązków musi wynikać wprost z umowy pomiędzy administratorem i procesorem
- RODO wprowadziło nowe gwarancje dotyczące ochrony danych osobowych. Art. 32 RODO stanowi bowiem, że oceniając stopień bezpieczeństwa danych, należy uwzględnić w szczególności ryzyko wiążące się z ich przetwarzaniem. Oznacza to, że **dostawcy chmury** przed rozpoczęciem przetwarzania danych będą musieli dokonać **stosownej analizy ryzyka**.
- Powyższa konstrukcja prawna jest jednym z **elementów zabezpieczających** powierzone przez administratora dane.

CHMURA OBLICZENIOWA a RODO

Powierzenie przetwarzania danych – podstawy

- Umowa pomiędzy administratorem danych a podmiotem, któremu powierzono przetwarzanie danych w formie pisemnej;
- Zobowiązanie podmiotu, któremu powierzono przetwarzanie danych do przetwarzania danych wyłącznie w zakresie i celu przewidzianym w umowie;
- Zobowiązanie podmiotu, któremu powierzono przetwarzanie danych do zabezpieczenia danych osobowych (z zastosowaniem środków prawnych, technicznych i organizacyjnych);
- Odpowiedzialność podmiotu, któremu powierzono przetwarzanie danych za przestrzeganie przepisów ustawy.

CHMURA OBLICZENIOWA a RODO

Powierzenie przetwarzania danych – na co zwrócić uwagę w umowie (1/2)

- Precyzyjne określenie środków bezpieczeństwa (zapis – „odpowiednie środki techniczne i organizacyjne” –to zbyt mało);
- Przedmiot i ramy czasowe usług w chmurze - dane osobowe powinny być przechowywane nie dłużej, niż jest to niezbędne dla osiągnięcia celu przetwarzania. Po tym okresie powinny być usunięte lub zanonimizowane tak, by nie można było ustalić tożsamości osoby, której dane dotyczą;
- Określenie warunków zwrotu danych osobowych lub ich zniszczenia po zakończeniu realizacji usługi;
- Klauzule poufności (obowiązujące zarówno dostawcę usługi w chmurze jak i jego pracowników);
- Obowiązek dostawcy usługi do wspierania klienta (ADO) w realizacji praw osoby, której dane są przetwarzane;
- Zakaz przekazywania danych osobom trzecim przez dostawcę usługi w chmurze (chyba, że umowa przewiduje realizacje usługi poprzez zaangażowanie podmiotów, którym zostanie podpowierzone przetwarzanie danych);
- Administrator powinien mieć możliwość decydowania, komu dane są podpowierzane oraz w jakim celu i zakresie. RODO uwzględnia możliwość podpowierzenia danych osobowych podwykonawcy, jednak nie może się to odbywać zgody administratora danych (28 ust. 2 RODO);
- Administrator powinien mieć zapewnione prawo przeprowadzania audytów i kontroli, potwierdzających prawidłowe przetwarzanie danych także przez podwykonawców.

CHMURA OBLICZENIOWA a RODO

Powierzenie przetwarzania danych – na co zwrócić uwagę w umowie (2/2)

- Zobowiązanie dostawcy usługi „chmury obliczeniowej" do powiadamiania klienta usługi w chmurze o wszelkich przypadkach naruszeń ochrony danych;
- Zawiadamianie administratora danych o każdym prawnie wiążącym wniosku o udostępnienie danych osobowych.
- Umowa o realizację usługi przetwarzania danych w chmurze powinna określać miejsce przetwarzania danych osobowych;
- Istotne jest poprawne określenie prawa właściwego, jakie będzie stosowane na terenie obowiązywania umowy – zwłaszcza w razie zaistnienia sporu między stronami;
- Klient ma prawo do monitorowania parametrów usług;
- Obowiązek współpracy dostawcy usług w chmurze (procesora) z Administratorem danych (ADO);
- Obowiązek dostawcy w chmurze informowania ADO o wszelkich zmianach dotyczących określonej usługi;
- Rejestrowanie i kontrolowanie istotnych operacji przetwarzania danych w chmurze;

….a na zakończenie

4 kroki do wdrożenia RODO w chmurze

- **Identyfikowanie i klasyfikacja danych** – celem tego kroku ma być zmapowanie danych i zidentyfikowanie, jakie dane osobowe posiada organizacja (własne lub powierzone) oraz gdzie dokładnie te dane się znajdują;
- **Zarządzanie** – zrozumienie, w jaki sposób przetwarzane są dane osobowe i jakie zasady określają ich udostępnianie. Na tym etapie identyfikujemy również ryzyka związane z przetwarzaniem;
- **Ochrona** – gdy już wiemy, jakie dane osobowe przetwarza organizacja, należy ustanowić odpowiednie środki monitorowania i kontroli ich bezpieczeństwa w celu umożliwienia wykrywania incydentów, jak również na bieżąco identyfikować obszary podwyższonego ryzyka podatności na incydenty bezpieczeństwa;
- **Raportowanie** – krok ten ma na celu wdrożenie procedur umożliwiających administratorom danych wykonywanie ich uprawnień, zgłaszanie incydentów bezpieczeństwa w zgodzie z RODO oraz opracowanie odpowiedniej dokumentacji przetwarzania danych.

Dziękuję za uwagę

Tadeusz Wachowski

k.wachowski@eidas.edu.pl

Interdyscyplinarne Centrum Modelowania Matematycznego Uniwersytetu Warszawskiego

Zakład Elektronicznej Techniki Obliczeniowej ZETO Koszalin

Koszalin, 8 grudnia 2017