Międzynarodowa Grupa Robocza
ds. Ochrony Danych w Telekomunikacji

24 kwietnia 2012 r.

Dokument roboczy
w sprawie

przetwarzania danych w chmurze obliczeniowej – kwestii ochrony danych i prywatności

- "Memorandum z Sopotu" -

51 Spotkanie,23-24 kwietnia 2012 r., Sopot (Polska)

Zakres

Niniejszy dokument roboczy poświęcony jest analizie przetwarzania danych osobowych w chmurze obliczeniowej (tzw. cloud computing – CC).

W niniejszym dokumencie nie analizuje się sytuacji, w której wszyscy użytkownicy końcowi, administrator danych, przetwarzający oraz wszyscy podprzetwarzający, którym powierzył przetwarzanie, podlegają takim samym przepisom o ochronie danych, posiadają siedziby w tej samej jurysdykcji oraz wszystkie operacje przetwarzania danych i przechowywanie danych odbywają się w ramach tej jurysdykcji. Dokument ten nie jest również najważniejszym punktem odniesienia w sytuacji, gdy usługa w chmurze znajdują się pod całkowitą kontrolą użytkownika usługi w chmurze.

I wreszcie, dokument roboczy dotyczy tylko wykorzystania usług w chmurze przez przedsiębiorstwa i organy publiczne, które przenoszą obecne procedury do "środowiska w chmurze", a nie wykorzystywania takich usług przez osoby fizyczne.

Ogólne podstawy

"Przetwarzanie w chmurze jest ewoluującym paradygmatem.." [1]

Przetwarzanie w chmurze (CC) wzbudza coraz większe zainteresowanie ze względu na obietnice większej wydajności gospodarczej, mniejszy wpływ na środowisko, łatwiejszą obsługę, większą przyjazność dla użytkownika oraz szereg innych korzyści.

We wrześniu 2011 r. Narodowy Instytut Standaryzacji i Technologii (NIST) wydał Specjalną Publikację SP 800-145, w której następująco zdefiniował przetwarzanie w chmurze:

"Cloud computing to model umożliwiający wszechstronny, wygodny, sieciowy dostęp na żądanie do wspólnej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci, aplikacji i usług), które można szybko zapewniać i udostępniać przy minimalnym wysiłku w zakresie zarządzania czy też interakcją z dostawcą usługi. Na model ten składa się pięć niezbędnych cech charakterystycznych, trzech modeli usług oraz czterech modeli zastosowania."[2]

Definicja ma m.in.:

„... na celu ... zapewnić podstawę do dyskusji, począwszy od tego, czym jest przetwarzanie w chmurze, aż po to, w jaki sposób najlepiej wykorzystać cloud computing."[3]

Definicja jest ważnym wkładem w trwający proces zrozumienia, czym rzeczywiście jest CC. Pojmowanie tego pojęcia szybko się rozwija. Definicja NIST jest doskonałym punktem wyjścia dla dalszego badania kwestii przetwarzania w chmurze i sposobu jego wykorzystywania.

Jednakże nadal istnieje niepewność co do CC, zwłaszcza gdy chodzi o prywatność, ochronę danych i inne kwestie prawne. Zalecenia zawarte w tym dokumencie mają na celu pomóc zmniejszyć tę niepewność.

Dokument sformułowano tak, aby najpierw przedstawić zalecenia. Druga część dokumentu zawiera dodatkowe informacje na temat CC oraz racjonalne podstawy zaleceń. Aby uzyskać dogłębniejszy wgląd w te kwestie, czytelnicy mogą najpierw przeczytać tę część.

Na potrzeby tego dokumentu klient usługi w chmurze uważany jest za administratora danych, zaś dostawca usługi w chmurze uważany jest za przetwarzającego dane. [4]

Rozwój CC przyczynił się do zwrócenia uwagi na szereg ważnych kwestii, w tym na następujące kwestie:

a. nie istnieje jeszcze międzynarodowe porozumienie co do wspólnej terminologii;
b. rozwój technologii nadal postępuje;
c. ogromne ilości danych są gromadzone i kumulowane;
d. technologia jest nieograniczona i transgraniczna; [5]
e. przetwarzanie danych stało się globalne;
f. brakuje przejrzystości w odniesieniu do procesów, procedur i praktyk dostawcy usługi w chmurze, w tym w odniesieniu do tego, czy dostawcy usług w chmurze podpowierzają jakiekolwiek przetwarzanie oraz jeżeli tak, jakie są ich odnośne procesy, procedury i praktyki;
g. ten brak przejrzystości utrudnia przeprowadzenie właściwej oceny ryzyka;
h. ten brak przejrzystości utrudnia egzekwowanie przepisów dotyczących ochrony danych;
i. wywierany jest ogromny nacisk na dostawców usług w chmurze, aby szybko skapitalizowali znaczące koszty inwestycyjne;
j. wywierany jest coraz większy nacisk na dostawców usług w chmurze, aby zmniejszyli koszty, w tym koszty ich przetwarzania danych, po części przyspieszone ze względu na globalny kryzys finansowy; oraz
k. jest bardziej prawdopodobne, że w celu utrzymania niskich cen dostawcy usług w chmurze to będą oferowali standardowe warunki.

Okoliczności te mogą prowadzić do **zwiększonego ryzyka, że**:

A. administrator danych nie zauważy naruszeń bezpieczeństwa informacji, takich jak naruszenia poufności, integralności czy tez dostępności danych (osobowych);

B. dane będą przekazywane do jurysdykcji, które nie zapewniają odpowiedniego poziomu ochrony;
C. popełnione zostaną czyny naruszające przepisy i zasady ochrony danych i prywatności;
D. administrator danych zaakceptuje standardowe warunki, które dają dostawcy usługi w chmurze zbyt wiele swobody działania, w tym możliwość, aby dostawca usługi w chmurze mógł przetwarzać dane w sposób sprzeczny z instrukcjami administratora danych;
E. dostawcy usług w chmurze lub ich podprzetwarzający wykorzystujący dane administratorów danych do własnych celów bez wiedzy czy też zgody administratorów danych;
F. rozliczalność i odpowiedzialność najprawdopodobniej znikną w łańcuchu podprzetwarzających;
G. administrator danych straci kontrolę nad danymi i przetwarzaniem danych;
H. administrator danych lub jego zaufana strona trzecia (np. audytor) nie będzie w stanie odpowiednio monitorować dostawcy usługi w chmurze;
I. uniemożliwi się organom ochrony danych właściwe nadzorowanie przetwarzania danych osobowych przez administratora danych i dostawcę usług w chmurze; oraz
J. administrator danych będzie polegał na bezpodstawnej wierze w brak wglądu i monitorowania, w ten sposób potencjalnie naruszając ustawodawstwo w zakresie ochrony danych obowiązujące w kraju, w którym posiada siedzibę.

Poniższe zalecenia mają na celu przyczynienie się do **zmniejszenia zagrożeń związanych z wykorzystywanie usług przetwarzania w chmurze oraz propagowania rozliczalności i właściwego zarządzania**[6], tak aby można było osiągnąć z wykorzystywania CC, ale nie kosztem praw osoby fizycznej.

Zalecenia[7]

Ogólne zalecenia

Grupa Robocza zaleca, co następuje:

- Przetwarzanie w chmurze nie musi prowadzić do obniżenia standardów ochrony danych w porównaniu z konwencjonalnym przetwarzaniem danych;
- Administratorzy danych będą przeprowadzać konieczne oceny skutków w zakresie ochrony prywatności oraz oceny zagrożenia (gdy to konieczne, korzystając z pomocy zaufanych stron trzecich) przed podjęciem się projektów CC;
- Dostawcy usług w chmurze będą dalej rozwijać swoje praktyki w celu oferowania większej przejrzystości, bezpieczeństwa, rozliczalności i zaufania do rozwiązań CC, w szczególności jeżeli chodzi o informacje na temat potencjalnych naruszeń ochrony danych i bardziej zrównoważone klauzule umowne w celu propagowania możliwości przenoszenia danych (portability) i kontroli danych przez użytkowników usług w chmurze;
- Zostaną podjęte dalsze wysiłki na rzecz badań, certyfikacji stron trzecich, standaryzacji, technologii ochrony prywatności w fazie projektowania (privacy by design) i innych powiązanych programów w celu osiągnięcia pożądanego poziomu zaufania do CC;

- Ustawodawcy będą ponownie oceniać adekwatność istniejących ram prawnych pozwalających na transgraniczne przekazywanie danych i uwzględnią dodatkowe niezbędne gwarancje ochrony prywatności w erze CC[8], oraz
- Organy ochrony danych i prywatności nadal będą zapewniać informacje administratorom danych, dostawcom usług w chmurze oraz ustawodawcom w kwestiach dotyczących ochrony danych i prywatności.

Dodatkowe wytyczne w sprawie dobrych praktyk

1. Wdrożenie CC powinno odbyć się w formie ostrożnych, wyważonych kroków, począwszy od informacji nie będących danymi szczególnie chronionymi ani poufnymi.
2. Przetwarzanie danych szczególnie chronionych[9] z wykorzystaniem CC budzi dodatkowe obawy. W związku z tym bez uszczerbku dla krajowych przepisów takie przetwarzanie wymaga dodatkowych zabezpieczeń.
3. **Dzienniki kontroli lokalizacji** powinny być udostępniane administratorom danych i organom ochrony danych. Dziennik kontroli powinien być rejestrowany automatycznie i pokazywać fizyczne lokalizacji, w których przechowuje się lub przetwarza dane osobowe oraz kiedy[10].
4. Należy ustanowić **automatycznie rejestrowany dziennik kontroli kopiowania i usuwania**, pokazując wyraźnie, które kopie danych osobowych utworzyli i usunęli przetwarzający lub jego podprzetwarzajacy.
5. Dziennik kontroli lokalizacji a także dziennik kontroli kopiowania oraz usuwania, również powinien zawierać kopię zapasową.
6. Powinny zostać rozwinięte efektywne **środki techniczne** przeciwko nielegalnemu przekazywaniu danych do jurysdykcji, bez wystarczającego poziomu ochrony danych.
7. Powinno się zapewnić, że **usunięcie** danych osobowych z dysków oraz z innych nośników może być przeprowadzone w skuteczny sposób, to jest poprzez **natychmiastowe nadpisanie losowych danych.** [11]
8. Powinno się zapewnić, że dane osobowe w spoczynku oraz w tranzycie[12] są **szyfrowane** przy użyciu uznanych, standardowych algorytmów z równoczesnym użyciem kluczy odpowiedniej długości. Klucze szyfrowania, nie powinny być stosowane przez nikogo, poza administratorem danych oraz dostarczycielem usług w chmurze. Nikt inny nie powinien mieć także do nich dostępu. Klucze szyfrowania nie powinny być używane ani dostępne dla innych klientów dostarczycieli usług w chmurze. Dane nie powinny być dostępne w niezaszyfrowanej formie dłużej oraz szerzej niż to absolutnie konieczne dla odbywającego się procesu przetwarzania danych. Metody wyświetlające niemożliwe do przeczytania dla dostarczycieli CC dane powinny być dalej rozwijane[13]. Użyteczne mogłoby być rozwinięcie opcji w których administrator danych może skutecznie oraz szybko odciąć dostarczyciela usług w chmurze lub jego podprzetwarzających od deszyfrowania danych (hamulec bezpieczeństwa).
9. Powinna istnieć automatyczna **rejestracja danych** każdego przetworzenia danych osobowych przez dostarczyciela usług w chmurze oraz jego podprzetwarzających. Rejestr powinien być łatwo dostępny dla administratora danych oraz być zaprojektowany w prosty, przejrzysty i zrozumiały sposób. Dostarczyciel usług w chmurze oraz jego podprzetwarzający powinni zapewnić integralność rejestrów.

Administrator danych

10. W umowie z dostarczycielem usług w chmurze, administrator danych powinien uprzednio zabezpieczyć informacje na temat wszystkich fizycznych lokalizacji w których, podczas trwania umowy, dane mogą być przechowywane lub przetwarzane, włączając w to kopie zapasowe, przez dostarczyciela usług w chmurze oraz/lub jego podprzetwarzających **(zasada przejrzystości lokalizacji)**.
11. W umowie, administrator danych powinien zapewnić, że ani dostarczyciel usług w chmurze ani jego podprzetwarzający nie przekazują danych do lokalizacji innych niż fizyczne lokalizacje wymienione w umowie, niezależnie od powodów oraz niezależnie od tego czy dane są zaszyfrowane. Powinno być to wspierane przez środki techniczne, których obecność oraz niezależność może być sprawdzona przez administratora danych.
12. Administrator danych powinien zapewnić, że umowa z dostarczycielem usług w chmurze nie zawiera dwuznaczności ani miejsca na interpretacje, które podważają zasadę stanowiącą, że dostarczyciel danych w chmurze przetwarza dane osobowe jedynie zgodzie z instrukcjami administratora danych. Jeśli dostarczyciele usług w chmurze byliby w stanie jednostronnie zmieniać umowę, administrator danych powinien mieć prawo do zakończenia kontraktu oraz przekazania danych do innego dostarczyciela usług w chmurze.
13. Umowa powinna wyraźnie stanowić o tym, że dostarczyciel usług w chmurze nie morze wykorzystywać danych administratora danych dla swoich własnych celów.
14. Administrator danych powinien mieć możliwość sprawdzenia lub sprawdzić wszystkie lokalizacje w których w całości lub w części przetwarza się dane osobowe, przetwarzało się w je przeszłości lub zgodnie z umową istnieje możliwość przetwarzania w przyszłości. Umowa powinna stanowić, że administrator danych ma prawo otrzymać pełen wgląd we wszystkie aspekty działalności dostarczyciela usług w chmurze oraz jego podprzetwarzających, które uważa za istotne dla zapewnienia wykonania umowy włączając zapewnienie, że przetwarzanie danych osobowych odbywa się zgodnie z instrukcją, legalnie oraz w odpowiednio bezpieczny sposób.
15. W umowie administrator danych powinien zabezpieczyć prawo do udzielania pozwolenia zaufanej stronie trzeciej (na przykład uznanej firmie audytowej)[14] na całkowite lub częściowe monitorowanie przetwarzania danych osobowych przez dostarczyciela usługi CC oraz jego pod-przetwarzających, o ile tacy istnieją.
16. Przed zastosowaniem CC, administrator danych powinien przeprowadzić ocenę ryzyka opartą o wgląd w specyficzne uwarunkowania oraz okoliczności, w których dane będą przetwarzane przez dostarczyciela usługi oraz jego pod-przetwarzających, o ile tacy istnieją. Ocena ryzyka powinna zawierać spis wszystkich miejsc w których dane osobowe są przetwarzane lub przechowywane. Jeśli dostawca usług CC wykorzystuje pod-przetwarzających dla częściowego przetwarzania, ocena ryzyka powinna zawierać także spis wszystkich miejsc wykorzystywanych przez pod-przetwarzających.
17. Administrator danych powinien dokonywać systematycznego przeglądu oraz ewaluacji oceny ryzyka tak długo jako dane osobowe są przetwarzane przez dostarczyciela usług w chmurze.
18. Przed zastosowaniem CC, administrator danych powinien rozważyć czy istnieje realna możliwość zakończenia współpracy z dostarczycielem usług w chmurze, włączając w to aktywną rolę dostarczyciela usług w chmurze w przekazaniu danych, tak aby uniknąć uzależnienia od dostawcy usług w chmurze (lock-in).

19. Administrator danych powinien rozważyć czy nie byłoby konieczne zabezpieczenie dostępu to przynajmniej jednej używalnej kopii danych poza kontrolą, zasięgiem wpływu dostarczyciela usług w chmurze (oraz jego pod-przetwarzających). Jeśli uzna się to za konieczne, kopia powinna być dostępna i używalna dla administratora danych, niezależnie od udziału dostarczyciela usług w chmurze oraz jego pod-przetwarzających.
20. Administrator danych powinien być w stanie w pełni wykonać swoje zobowiązania w stosunku do osoby, której dane dotyczą oraz organów ochrony danych w przypadku **naruszenia ochrony danych** i podjąć odpowiednie działania. Jako taki, administrator danych powinien zawrzeć jasne umowy z dostarczycielem usług w chmurze odnośnie szybkiej oraz kompletnej notyfikacji administratorowi danych lub organowi ochrony danych przypadków takiego naruszenia danych.
21. Administrator danych powinien zobligować umownie dostarczyciela usług w chmurze do wdrożenia efektywnej oraz szybkiej procedury, tak aby osoby, których dane dotyczą mogły wyegzekwować swoje prawa dostępu, poprawienia, usunięcia oraz zablokowania danych.

Dostarczyciel usług w chmurze

22. Dostarczyciel usług w chmurze powinien zapewnić administratorowi danych pełną przejrzystość odnośnie miejsca przetwarzania oraz przechowywania danych osobowych przez dostarczyciela usług w chmurze oraz jego pod-przetwarzających, o ile tacy istnieją.
23. Dostarczyciel usług w chmurze powinien zapewnić administratorowi danych pełną przejrzystość odnośnie pod-przetwarzających z których usług korzysta oraz odnośnie przetwarzania, którego dokonują oni na rzecz dostarczyciela usług w chmurze.
24. Dostarczyciel usług w chmurze powinien zapewnić przejrzystość w sprawach umowy oraz powstrzymać się od oferowania CC na standardowych warunkach, pozwalających na jednostronne zmiany w kontrakcie.
25. Zachęcamy dostarczyciela usług w chmurze oraz jego pod-przetwarzających, o ile tacy istnieją, do działania zgodnie z dobrymi praktykami oraz do pozwolenia bezstronnej stronie trzeciej na przeprowadzenie porównania oraz oceny tych działań (benchmarking).
26. Standardowe warunki oferowane niektórym segmentom rynku, np. małym i średnim przedsiębiorstwom powinny być zaprojektowane w taki sposób, który szanuje prywatność oraz bierze pod uwagę odpowiednie środki ochronne.

Audyt

27. Biorąc pod uwagę możliwość kumulacji dużej ilości danych osobowych przez dostarczyciela usług w chmurze, powinien on być poddany audytowi strony trzeciej, dodatkowo do audytu przeprowadzanego przez administratora danych w jego własnym interesie. Audytor powinien być w pełni niezależny od dostarczyciela usług w chmurze oraz powinien poświęcić szczególną uwagę aspektom bezpieczeństwa związanym z przetwarzaniem danych osobowych. W szczególności, audytor powinien sprawdzić czy środki dotyczące następujących kwestii: dziennik kontroli pomieszczeń (zobacz część 3); dziennik kontroli kopiowania i usuwania (zobacz część 4), usuwanie (zobacz część 7), rejestracja danych (zobacz część 6) są stosowane oraz czy odbywa się to odpowiednio. Ponadto, audytor powinien sprawdzić czy środki dotyczące następujących kwestii: zapobieganie bezprawnemu przekazywaniu danych na obszary

będące w jurysdykcji nie zapewniającej odpowiedniej ochrony danych (część 6) oraz zapobieganie przekazywaniu danych do innych miejsc, niż te wyraźnie określone w umowie z klientem (zobacz części 10 i 11) są stosowane oraz czy odbywa się to odpowiednio. Audytorzy powinni także zapewnić, że nie jest możliwe aby dostarczyciel usług w chmurze lub jego pod-przetwarzający, o ile tacy istnieją, mogli niezauważeni obejść te środki.

Podstawy rekomendacji

28. CC jest stosunkowo **nowym paradygmatem** w przetwarzaniu danych, który wyewoluował z tego co, z powodu braku lepszego terminu, jest obecnie określane jako **tradycyjne przetwarzanie danych**. Przez wiele lat udało się zgromadzić gruntowne doświadczenie odnośnie tradycyjnego przetwarzania danych, jednak brakuje go w odniesieniu do CC.
29. Konsekwencją **zmiany paradygmatu** jest to, że podstawowe założenia, doświadczenia, pomysły, teorie oraz modele dotyczące przetwarzania danych nie przystają dłużej do praktyki i dlatego muszą być przedmiotem krytycznej refleksji, ponownej oceny i możliwej zmiany. Ma to zastosowanie także do prywatności oraz ochrony danych osobowych oraz tego jak **ryzyko** może być analizowane, szacowane oraz oceniane. To co było dobrą praktyką wczoraj niekoniecznie jest nią dzisiaj.
30. **Nowa sytuacja** musi być przeanalizowana a zastosowane **środki muszą być ostrożne**, szczególnie w odniesieniu do prywatności oraz ochrony danych a także ochrony praw osoby, której dane dotyczą w szerszym kontekście.
31. **Fundamentem technicznym** CC jest dobrze rozwinięta technologia sieciowa oraz wirtualizacja serwerów. Pozwala to na szybkie, dynamiczne przemieszczenie danych oraz przetwarzanie danych pomiędzy lokalnymi serwerami w indywidualnych centrach przetwarzania danych w chmurze oraz globalnie pomiędzy centrami przetwarzania danych w chmurze w państwach na całym świecie. Technologia posiada dużą skalowalność, bez ograniczeń dla przepustowości. Internet pozwala użytkownikowi końcowemu na dostęp do danych niezależnie od tego gdzie centra przetwarzania danych w chmurze są umieszczone.
32. **Ekonomiczną przyczyną** CC jest **ekonomia skali**. Konsolidacja przetwarzanych danych w dużych centrach poprawia efektywność wykorzystania kosztownych zasobów takich jak: ludzka wiedza, majątek (sprzęt, oprogramowanie, budynki), szyna komunikacyjna oraz energia. Dodatkowo, w następstwie ich rozmiaru dostarczyciele usług w chmurze posiadają znaczącą moc, gdy dochodzi do zakupu zasobów. Dostarczyciele usług w chmurze mogą dzięki temu zredukować koszty jednostkowe oraz zaoferować atrakcyjne ceny dla klientów. Warunkiem koniecznym dla osiągnięcia ekonomi skali jest posiadanie dużej ich liczby. Aby osiągnąć wystarczający obrót, usługi są oferowane globalnie przez Internet.
33. CC uważane jest za technologię, która zapewni szansę dostępu małym i średnim przedsiębiorstwom do skalowalnych zasobów komputerowych w przystępnej cenie. W związku z istnieniem dużej liczby relatywnie małych przedsiębiorstw, oczekuje się że dostarczyciele usług w chmurze opracują standardowy wzór umowy dla tego segmentu rynku.
34. CC jest znacznie bardziej dynamiczne niż tradycyjne przetwarzanie danych. Miejsce przetwarzanych danych może zmieniać się szybko. Obecna lokalizacja danych oraz miejsce ich przetwarzania może zależeć od różnych czynników, którym użytkownicy końcowi oraz administratorzy danych tradycyjnie poświęcili mało uwagi, i do których niekoniecznie mają wgląd oraz możliwość kontroli. Na przykład dostarczyciele usług

w chmurze często umiejscawiają centra przetwarzania danych w wielu państwach na kilku kontynentach, opierając się, między innymi, na dostępności oraz cenie elektryczności, łagodnym lokalnym klimacie oraz różnicach czasowych. Nieprzewidywalne okoliczności, takie jak zakłócenia w jednym z centrów danych czy niewystarczająca przepustowość w godzinach szczytu (overflow), mogą również wpłynąć na lokalizację danych w danym momencie. Kopie danych mogą być przekazane do innego centrum danych tak aby zapewnić dostępność w sieci w przypadku zakłóceń w jednym z centrów danych lub dla celów utworzenia kopii zapasowej (redundancy).

35. CC jest oparty na wielu klientach usług w chmurze dynamicznie dzielących wspólną pule zasobów dostarczyli usług w chmurze. Sytuacja taka może istnieć tylko jeśli możliwe jest utrzymanie **wyraźnej odrębności** pomiędzy danymi należącymi do różnych klientów oraz ich przetwarzaniem. Dzielenie się zasobami powoduje podwyższone ryzyko strat dużej skali lub nieuprawnionego ujawnienia danych.[15] Ryzyko jest tym większe, że CC jest oparty na optymalizacji kosztów w związku z wysokim obrotem (ekonomia skali). Klienci usług w chmurze powodują ryzyko dla siebie nawzajem. Im więcej klientów dzieli te same zasoby, tym większe jest ryzyko dla każdego indywidualnego klienta, i w ten sposób dla przetwarzania w chmurze jako całości.
36. Wiedza o CC oraz przegląd możliwego ryzyka koncentruje się obecnie na stosunkowo niewielkiej liczbie dużych dostarczycieli usług w chmurze, którzy z powodów komercyjnych oraz w celu zachowania konkurencyjności wydają się niechętni zgodzie na wgląd do swoich szczegółowych warunków oraz okoliczności. Nierówna dystrybucja wiedzy oraz możliwości wglądu pomiędzy dostarczycielami usług w chmurze a klientami, umieszcza tych ostatnich w niekorzystnej sytuacji, kiedy zawierają oni umowę oraz powoduje, że właściwe ocenienie przez nich ryzyka związanego z zamierzonym użyciem CC jest trudne.
37. **Kompleksowa ocena** musi być oparta na **wglądzie** do konkretnych ustawień oraz okoliczności dostarczycieli usług w chmurze we wszystkich miejscach gdzie przetwarzanie danych będzie się odbywać.
38. Technologia CC jest **nieograniczona** i **trans-graniczna**. Globalna baza klientów, w parze z globalnym rozmieszczeniem centrów przetwarzania danych w chmurze oraz dynamicznym ruchem danych (i ich przetwarzaniem), może powodować, że dane przekraczają granice państw oraz zmieniają jurysdykcję wraz z towarzyszącym temu brakiem przejrzystości. Dane osobowe mogą znaleźć się w centrum przetwarzania danych podlegającym jurysdykcji w której nie ma odpowiedniej ochrony danych, mogą być wykorzystane w sposób niezgodny z przeznaczeniem dla celów komercyjnych a dostęp do nich może uzyskać siły zewnętrze, które nie są uprawnione.[16]
39. Należy rozróżnić dwie wzajemnie wykluczające się role administratora danych oraz przetwarzających w ramach ochrony danych. **Administrator danych** to ten podmiot, który decyduje o celach i środkach zastosowanych w przypadku konkretnej czynności przetwarzania.
40. Uznaje się także, że administrator danych może powierzyć przetwarzanie danych **przetwarzającemu**, jednak tylko w zgodzie z wyraźną **instrukcją** administratora danych.
41. Wspólnie uznaną zasadą ochrony danych jest to, że przetwarzający nie może przetwarzać danych osobowych w większym stopniu niż wynika to z wyraźnych instrukcji administratora danych[17]. W przypadku CC oznacza to, że dostarczyciel usług przetwarzania w chmurze nie może jednostronnie podejmować decyzji lub

przygotowywać przesłanie danych osobowych (i tym samym ich przetwarzanie) do nieznanego centrum przetwarzania danych w chmurze. Zasada ta obowiązuje niezależnie od tego czy dostarczyciel usług internetowych uzasadnia taki transfer redukcją kosztów, zarządzaniem przepływem w godzinach szczytu (overflow), równoważeniem obciążenia, tworzeniem systemów wsparcia, etc. Dostarczyciel usług przetwarzania w chmurze nie może także przetwarzać danych dla własnych celów. [18]

42. Następna powszechnie uznawana zasada ochrony danych wymaga od administratora danych, aby implementował on **techniczne oraz organizacyjne środki bezpieczeństwa** w celu ochrony danych przed przypadkowym lub bezprawnym zniszczeniem, utratą lub pogorszeniem oraz przeciw bezprawnemu ujawnieniu, naruszeniu lub innemu przetwarzaniu naruszającemu przepisy prawa. To samo odnosi się do przetwarzających.
43. Wypełnienie obowiązków administratora danych wymaga, aby monitorował on przetwarzanie przez przetwarzającego tak aby zapewnić, że odbywa się ono zgodnie z instrukcjami administratora danych oraz przy zastosowaniu odpowiedniej ochrony.
44. Bez zdejmowania z siebie odpowiedzialności, administrator danych może wydać wyraźne instrukcje stanowiące, że monitorowanie przetwarzania przez przetwarzającego będzie częściowo przeprowadzane przez **zaufaną stronę trzecią** (np. audytora). Warunkiem jest to, że strona trzecia ma niezbędne kwalifikacje, jest niezależna od przetwarzającego, ma pełen dostęp oraz wgląd do faktycznych warunków oraz okoliczności w jakich odbywa się przetwarzanie przez przetwarzającego oraz może przedstawić wiarygodny raport na temat swoich obserwacji, ocen oraz konkluzji administratorowi danych. Grupa Robocza będzie nadal obserwować rozwój w obszarze przetwarzania danych w chmurze i aktualizować ten dokument, jeśli okaże się to konieczne.

Przypisy

[1] Narodowy Instytut Standaryzacji i Technologii (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, Wrzesień 2011, s. 2

[2] Narodowy Instytut Standaryzacji i Technologii (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, Wrzesień 2011, s. 3

[3] Narodowy Instytut Standaryzacji i Technologii (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, Wrzesień 2011, s. 2

[4] Zobacz punkty 39, 40 oraz niżej. Podprzetwarzający dostarczyciela usług w chmurze w kontekście przetwarzania danych osobowych są również uważani za przetwarzających.

[5] Zobacz punkt 38

[6] Na stronach 9-10 dokumentu ENISA: *Cloud Computing – Benefits, risks and recommendations for information security*, listopad 2009, wymieniono, w losowym porządku, najważniejsze ryzyka dla bezpieczeństwa, jak: utrata zdolności zarządzania, bycie zależnym od dostarczyciela usług w chmurze (lock-in), błąd oddzielenia (isolation failure), ochrona danych, niezabezpieczone lub niekompletne usunięcie danych, szkodliwy pracownik (malicious insider). Aby dowiedzieć się więcej zobacz publikację. Podkreślono tutaj problem utraty zdolności zarządzania.

[7] Lista zaleceń nie jest wyczerpująca.

[8] Więcej: Międzynarodowa Konferencja Rzeczników Ochrony Danych oraz Prywatności: Międzynarodowe standardy ochrony danych oraz prywatności (Rezolucja Madrycka), 5 listopada 2009. Dostępne na stronie internetowej:http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

[9] Koncepcja danych wrażliwych posiada odmienne znaczenia w różnych kulturach prawnych, zobacz art. 8 dyrektywy 95/46/WE, Art. 9 Ogólne Rozporządzenia o Ochronie Danych oraz Raport Federalnej Komisji Handlu: "Protecting Consumer Privacy in an Era of Rapid Change", 2012

[10] Np. dzienniki kontroli lokalizacji mogą zapewnić jasny przegląd tego, kiedy indywidualne dane osobowe są sprawdzane w konkretnych miejscach, jak również kiedy oraz do jakiej lokalizacji są przekazywane.

[11] Usunięcie poprzez nie odwoływanie się do danych a następnie nadpisanie poprzez ponowne wykorzystanie pamięci generalnie nie jest wystarczające, ponieważ otwiera możliwość tego, że dane staną się ponownie dostępne przez odnowienie odniesienia przed lub w trakcie ponownego wykorzystywania pamięci.

[12] W przypadku przekazywanych danych powinno się stosować szyfrowanie typu end-to-end. Należy zapewnić, że dane osobowe w procesie przekazywania są chronione przeciw aktywnym (na przykład: ataki polegające na podszywaniu się (typu replays), wstrzyknięcie obciążenia (traffic injections)) oraz pasywnym (np. podłuchiwanie) atakom. Ponadto, dostęp do danych w spoczynku przez nieuprawnione strony musi być ograniczony przez odpowiednie techniczne oraz organizacyjne mechanizmy (np. kontrola dostępu, szyfrowanie danych).

[13] Przykładem badań w tym obszarze jest inicjatywa Sealed Cloud, którą przedstawiono w projekcie dokumentu *Sealed Cloud - a novel approach to defend insider attacks* , przygotowanym przez Hubert A. Jäger i Arnold Monitzer. Dokument jest dostępny pod adresem: http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf

[14] Więcej na temat zaufanych stron trzecich w punkcie 44.

[15] Na stronach 9-10 dokumentu ENISA: *Cloud Computing – Benefits, risks and recommendations for information security*, listopad 2009, wymieniono, w losowym porządku, najważniejsze ryzyka dla bezpieczeństwa, jak: utrata zdolności zarządzania, bycie zależnym od dostarczyciela usług w chmurze (lock-in), błąd oddzielenia (isolation failure), ochrona danych, niezabezpieczone lub niekompletne usunięcie danych, szkodliwy pracownik (malicious insider). Aby dowiedzieć się więcej zobacz publikację. Należy podkreślić, że błąd oddzielenia (isolation failure) znalazł się na czele listy ryzyk.

[16] Choć dane osobowe mogą być przetwarzane w ramach jednej jurysdykcji, dostarczyciel usług w chmurze, lub spółka matka, może także mieć siedzibę w innej jurysdykcji, pozwalając w ten sposób zagranicznym instytucjom wdrażania prawa na dostęp do danych w usłudze przetwarzania danych w chmurze nawet jeśli fizycznie dane znajdują się poza granicami tego kraju. Może być wymagana umowa międzynarodowa aby rozwiązać tą kwestię.

[17] Lub z prawa.

[18] Jeśli dostarczyciele usług w chmurze przetwarzają dane bez wiedzy administratora, dostarczyciel usług w chmurze powinien być uważany za współ-administratora i jako taki być odpowiedzialny za nieuprawnione, niezależne przetwarzanie danych.