ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 797 STUDIA INFORMATICA NR 33 2013

Grzegorz Wojarnik*
Uniwersytet Szczeciński

BEZPIECZEŃSTWO PRZETWARZANIA DANYCH W MODELU *CLOUD COMPUTING* – UWARUNKOWANIA W KONTEKŚCIE OCHRONY DANYCH OSOBOWYCH W WARUNKACH PRAWA POLSKIEGO

Streszczenie

Model *cloud computing* jest coraz bardziej popularną technologią przetwarzania danych. Jednocześnie istotne jest, aby zdawać sobie sprawę z jego zalet, ale także pewnych ograniczeń. W artykule zostały przedstawione aspekty wykorzystania technologii *cloud computing* w kontekście prawnych aspektów ochrony danych osobowych.

Słowa kluczowe: technologie informatyczne, *cloud computing*, ochrona danych osobowych

1. Technologia *cloud computing*

Sformułowanie *cloud computing* jest określeniem kategorii zaawansowanych usług obliczeniowych na żądanie, początkowo oferowanych przez komercyjnych dostawców, takich jak Amazon, Google i Microsoft. Termin ten oznacza model, w ramach którego infrastruktura obliczeniowa jest postrzegana jako „chmura", z której korzystają zarówno przedsiębiorstwa, jak i pojedyncze osoby chcące mieć dostęp na żądanie do danych lub konkretnych usług sieciowych z dowolnego miejsca na świecie. Bardzo ważne jest, że w tym modelu przetwarzanie, przechowywanie danych i oprogramowanie są traktowane jako usługa (Buyya i in. red., 2011, s. 3).

Koncepcja *cloud computing* wykroczyła daleko poza dostarczanie oprogramowania na żądanie klientów. Obecnie powszechnie przyjmuje się, że *cloud*

* grzegorz.wojarnik.us@gmail.com

computing jest dostępny w trzech głównych postaciach (Hugos i Hulitzky, 2011, s. 44):

1. *Software-as-a-Service* (SaaS), zgodnie z którym dostawca oprogramowania dostarcza i udostępnia klientowi aplikację do wykorzystania bez potrzeby jej instalacji i utrzymania we własnej siedzibie czy też w ramach centrum danych. Taka forma technologii *cloud computing* będzie mogła być wykorzystana podczas tworzenia elektronicznego repertorium dostępnego jako rozwiązanie internetowe.
2. *Platform-as-a-service* (PaaS) rozumiane jako środowisko programistyczne, gdzie klient może tworzyć i rozwijać aplikacje na bazie zasobów usługodawców, eliminując potrzebę utrzymywania infrastruktury potrzebnej do procesu tworzenia oprogramowania.
3. *Infrastructure-as-a-Service* (IaaS) pozwalające firmom wynajmować centrum danych, bez konieczności tworzenia i utrzymywania takiego centrum we własnej firmie.

Do zasadniczych różnic pomiędzy technologią *cloud computing* a hostingiem tradycyjnym (Shrof, 2010, s. 34) należą:

1. Poziom automatyzacji jaki jest udostępniony dla użytkowników końcowych w zakresie usług internetowych, służący kontroli liczby wirtualnych instancji uruchomionych w dowolnym momencie.
2. Możliwość zapisywania i konfigurowania stanu wirtualnych komputerów przez użytkowników.
3. Obciążanie użytkownika opłatami za godzinę rzeczywistego wykorzystania infrastruktury w chmurze, w przeciwieństwie do miesięcznych lub rocznych opłat za tradycyjny hosting.
4. Udostępnianie również własnych systemów narzędzi programistycznych, takich jak obsługa kolejek (ang. *queue*), nierelacyjnych i relacyjnych baz danych, wirtualnych dysków itd.
5. Umożliwienie wielu użytkownikom na budowę w chmurze złożonych aplikacji bez konieczności wdrażania i konfigurowania tradycyjnej warstwy *middleware* (oprogramowanie wspierające tworzenie rozwiązań internetowych po stronie serwera) i produktów bazodanowych we własnych centrach obliczeniowych.

Przetwarzanie w chmurze pozwala na wykorzystywanie serwisów dostępnych w sieci Internet zamiast serwisów lokalnych, na przechowywanie plików w bezpiecznych i skalowalnych środowiskach internetowych zamiast na komputerze lub w sieci lokalnej, a także na tworzenie aplikacji w przestrzeni nieograniczonej pod względem przechowywanych danych mierzonych w gigabajtach.

Taki rodzaj przetwarzania polega na korzystaniu z pakietu biurowego zainstalowanego na komputerze, z serwisu realizującego funkcje biurowe w środowisku przeglądarki internetowej, co całkowicie eliminuje konieczność konfiguracji oraz instalacji takiej aplikacji. Mniej więcej w latach 2005–2008 składowanie danych *on-line* stało się tańsze i bardziej bezpieczne niż przechowywanie danych w sieci lokalnej lub na komputerze osobistym (Cafaro i Aloisio red., s. 7).

Dzięki rozwiązaniom *cloud computing* istnieje możliwość przeniesienia całej struktury technologicznej firmy, opierającej się na infrastrukturze technicznej, do przetwarzania w chmurze, co sprzyja optymalizacji kosztów. Przeniesienie to powoduje, że bezpieczeństwo zasobów jest outsourcingowane do specjalistycznych centrów obliczeniowych, dzięki czemu w przedsiębiorstwie używa się tylko tych zasobów, które są w danym momencie potrzebne, a każda rozbudowa nie wiąże się z koniecznością restrukturyzacji środowiska serwerowego.

2. Zalety *cloud computing* jako narzędzia wspierającego gromadzenie i przetwarzanie danych

Z punktu widzenia organizacji lub przedsiębiorstwa, w których jednym z działań jest utrzymywanie własnych systemów oraz danych, rozwiązanie polegające na stworzeniu usługi realizującej różne funkcje przetwarzania danych w technologii *cloud computing* można rozpatrywać na kilku poziomach: funkcjonalnym, bezpieczeństwa oraz dostępności.

Poziom funkcjonalny zapewnia możliwość wykorzystania technologii informatycznych do przyspieszenia pracy użytkowników wewnętrznych systemów zajmujących się przetwarzaniem danych organizacji lub przedsiębiorstwa. W ramach każdego systemu informatycznego można zaimplementować takie ułatwienia, jak sprawdzanie poprawności danych, dostępność słowników danych w celu wyboru danych już wcześniej wprowadzonych, wyszukiwanie danych, sporządzanie zestawień według różnych kryteriów i wiele innych. Ten poziom jest realizowany przez różne oprogramowanie dostępne na rynku, realizujące funkcje istotne z punktu widzenia danego podmiotu.

Jeśli chodzi o bezpieczeństwo danych, to można je rozpatrywać jako bezpieczeństwo ogólne, rozumiane jako możliwość dostępu do tych danych przez osoby nieuprawnione oraz zgodność danego rozwiązania informatycznego z zasadami określanymi przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO). I w tym przypadku wszelkie rozwiązania internetowe, wykorzystujące

dostawców dysponujących odpowiednimi certyfikatami, pozwalają niejako na delegowanie przez dane przedsiębiorstwo tych obowiązków na inne podmioty tak, aby sama organizacja lub przedsiębiorstwo nie musiało tworzyć na własne potrzeby tej całej infrastruktury, która zapewniałaby zgodność ze standardami bezpieczeństwa wymaganymi przez GIODO. Ten poziom może być realizowany za pośrednictwem firm hostingowych, które spełniły wymagania GIODO z zakresu bezpieczeństwa danych w kontekście ochrony danych osobowych.

Ostatni poziom dostępności jest ściśle związany z poziomem bezpieczeństwa. Dostępność jest tu rozumiana jako możliwość korzystania z danego rozwiązania niezależnie od posiadanego sprzętu oraz niezależnie od innych użytkowników korzystających z danego serwisu. O ile każdy dostawca internetowy pozwala na korzystanie z jego rozwiązań na całym świecie przez dowolnego użytkownika, o tyle już nie jest w stanie zapewnić w prosty sposób odpowiedniej skalowalności dla dowolnej liczby użytkowników serwisu. Jedną z naczelnych zalet usług *cloud computing* jest skalowalność, które daje użytkownikom serwisu nadzieję, że np. znaczne i skokowe zwiększenie liczby jego użytkowników nie odbije się na wydajności świadczonych usług. Kolejną zaletą jest wykorzystanie mechanizmów redundancji zapisanych danych, polegające na tym, że dane w chmurze są powielane pomiędzy różnymi serwerami po to, aby w przypadku problemów z działaniem jednego serwera jego funkcje mógł przejąć inny.

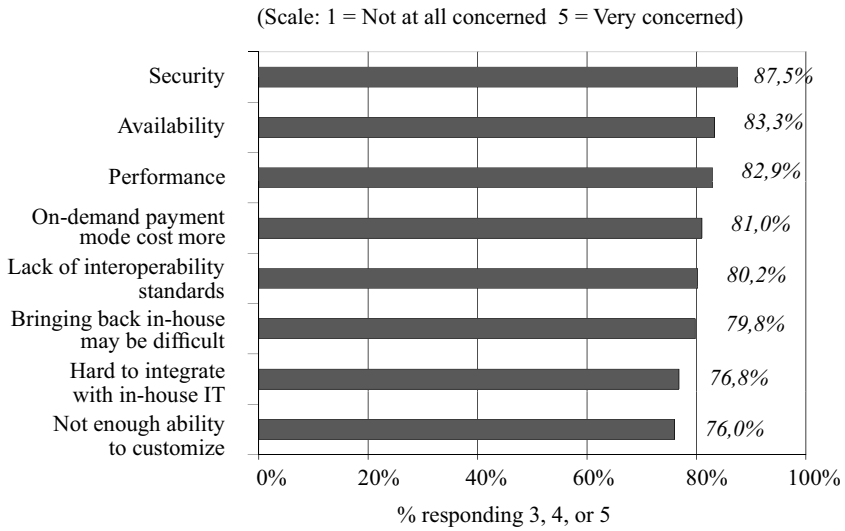
Oczywiście należy też mieć świadomość pewnych zagrożeń udostępniania danych w chmurze i wiedzieć, w jaki sposób są i mogą być niwelowane przez producentów rozwiązań opartych na *cloud computing*. Problemy zabezpieczania danych w chmurze dotyczą wysyłania danych do serwerów realizujących funkcje *cloud computing*, ale jednocześnie istnieją technologie (np. SSL), które na tyle sprawdziły się np. w przypadku usług bankowych, iż można uznać, że bez problemu sprawdzą się także w przypadku innych usług. Z drugiej strony do danych umieszczonych w chmurze mogą mieć dostęp chociażby pracownicy dostawcy usług *cloud computing*, ale w tym przypadku decyzja, w jaki sposób oraz czy w ogóle będą szyfrowane te dane, zależy od producenta konkretnego serwisu. Obecnie wszyscy najważniejsi dostawcy usług *cloud computing* pozwalają na wszechstronne zabezpieczanie aplikacji i danych tak, aby spełniały nawet najbardziej zaawansowane zasady bezpieczeństwa danych.

Podsumowując tę część rozważań, należy stwierdzić, że stopień bezpieczeństwa danych w chmurze zależy w większym zakresie od konkretnego rozwiązania niż od samej usługi *cloud computing*, która najczęściej wspiera wszelkie dostępne i uznane

za standardy mechanizmy bezpieczeństwa danych. Tylko od programistów i twórców serwisu zależy więc, na ile zostaną te mechanizmy wykorzystane, aby zapewnić poziom zabezpieczeń akceptowany przez użytkowników i dostosowany do ich potrzeb.

3. Bezpieczeństwo danych jako kluczowy czynnik rozwoju technologii przetwarzania w chmurze w kontekście uregulowań przetwarzania danych osobowych

Przetwarzanie danych w modelu *cloud computing* jest związane w pewnym sensie z utratą kontroli nad fizycznym bezpieczeństwem gromadzonych danych. Chmury publiczne charakteryzują się dzieleniem zasobów obliczeniowych z różnymi firmami poza danym przedsiębiorstwem – nie ma więc właściwie żadnej bezpośredniej kontroli nad tym, w jaki sposób zarządza się tymi zasobami. Dodatkowo „wyprowadzenie" danych do takiego współdzielonego środowiska, w którym znajdują się dane z wielu organizacji oraz firm, może dać instytucjom rządowym „uzasadnione powody", aby wykorzystać te dane bez wiedzy ich właścicieli. Oczywiście wszystko to można uzasadniać chęcią zapobiegania łamaniu prawa przez innych ludzi czy organizacje. Dlatego też właśnie bezpieczeństwo danych jest najczęściej wymieniane jako kwestia związana z wyzwaniami stojącymi przed technologią cloud computing (rysunek 1).



Rysunek 1. Wymagania stojące przez rozwiązaniami w modelu *cloud computing*
Źródło: Gens (2009).

Analitycy firmy konsultingowej Gartner wymieniają siedem grup bezpieczeństwa, które należy wziąć pod uwagę w kontekście wykorzystania technologii w organizacji cloud computing (Gartner, 2008):

1. Dostęp upoważnionych użytkowników – analiza kwestii specjalnego dostępu do danych, szczególnie z punktu widzenia zatrudniania administratorów zarządzających danymi.
2. Zgodność z przepisami – gotowość dostawcy usług *cloud computing* do poddania się kontrolom zewnętrznym i/lub obecność w centrach danych odpowiednich certyfikatów bezpieczeństwa.
3. Lokalizacja danych – możliwość kontroli nad fizyczną lokalizacją danych.
4. Segregacja danych – szyfrowanie jest dostępne na wszystkich etapach wykorzystania ich w chmurze, a systemy szyfrowania zostały zaprojektowane i przetestowane przez doświadczonych specjalistów.
5. Odtwarzanie – wiedza, co się stanie z danymi w przypadku awarii. Dostawca usług *cloud computing* musi zapewnić możliwość odzyskania danych w krótkim czasie po awarii usługi.
6. Reakcja na działania niezgodne z prawem – usługodawca powinien mieć możliwość badania wszelkich niewłaściwych lub niezgodnych z prawem działań, które dotyczą danych lub systemów działających w ramach usług *cloud computing*.
7. Długoterminowa rentowność – obecność scenariuszy przekazania danych w sytuacji pojawienia się takiego żądania ze strony usługobiorcy usług *cloud computing*.

Ramy architektury bezpieczeństwa powinny być ustalone z uwzględnieniem procesów zapewniających bezpieczeństwo wewnątrz- i zewnątrzorganizacyjne (uwierzytelnianie i autoryzacja, kontrola dostępu, poufności, integralności, zarządzanie bezpieczeństwem itp.), procedur operacyjnych, specyfiki wykorzystywanych technologii, zasobów ludzkich i zarządzania organizacją, bezpieczeństwa i programu bezpieczeństwa oraz raportowania bezpieczeństwa. Dokument zawierający plan polityki bezpieczeństwa w organizacji musi określać bezpieczeństwo i zasady prywatności dla spełnienia celów biznesowych. Technologia i metody projektowania systemów bezpieczeństwa powinny zostać uwzględnione jako niezbędne do świadczenia usług *cloud cumputing* we wszystkich warstwach technologicznych (Rittinghouse, Ransome, s. 172), takich jak:

– uwierzytelnianie użytkowników,
– autoryzacja,

– dostępność danych,
– poufność danych,
– integralność,
– odpowiedzialność,
– zachowanie prywatności.

W polskim prawie nie ma regulacji zabraniających prowadzenia oraz gromadzenia danych w postaci elektronicznej. W związku z powyższym w praktyce powszechnie są wykorzystywane rozwiązania, w ramach których oczywiste jest stosowanie różnorodnych funkcji oprogramowania komputerowego do procesu przetwarzania danych.

Odnosząc się do danych gromadzonych i przetwarzanych za pośrednictwem programów komputerowych, należy mieć na uwadze, że przechowywane dane oraz system, w ramach którego są przechowywane, powinny najczęściej spełniać wymogi ochrony danych osobowych, które wielokrotnie w ramach takiego systemu są przetwarzane.

Właściwie w każdej praktyce działalności gospodarczej dochodzi do przetwarzania danych osobowych. Dlatego też w związku z rejestracją tych danych dany podmiot podlega pod Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Ustawa, 1997) oraz Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Rozporządzenie, 2004).

Ustawa o ochronie danych osobowych nakłada na administratora tych danych obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinność zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Dodatkowo ustawa nakłada obowiązek zgłaszania zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Takie zgłoszenie powinno zawierać następujące elementy:
– wniosek o wpisanie zbioru danych do rejestru zbiorów danych osobowych,
– oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany oraz podstawę prawną upoważniającą do prowadzenia

zbioru, a w przypadku powierzenia przetwarzania danych podmiotowi odpowiedzialnemu za przetwarzanie danych osobowych lub wyznaczenia podmiotu mającego siedzibę w państwie trzecim – oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania,
– cel przetwarzania danych,
– opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,
– sposób zbierania oraz udostępniania danych,
– informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,
– opis środków technicznych i organizacyjnych zastosowanych w celu dopuszczenia dostępu do nich tylko przez osoby upoważnione,
– informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach regulujących podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych,
– informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Ustawodawca przewidział zwolnienie w obligacji do respektowania tych zasad, a są to administratorzy danych (*Zwolnienia z obowiązku rejestracji*):
– zawierających informacje niejawne,
– które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,
– przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym,
– przetwarzanych przez Generalnego Inspektora Informacji Finansowej,
– przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym,
– dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,
– przetwarzanych w związku z zatrudnieniem u nich lub świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,

– dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,
– tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego,
– dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,
– przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
– powszechnie dostępnych,
– przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
– przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

Z kolei rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych określa, jakie wymogi powinien spełniać system, w ramach którego przetwarzane są dane osobowe. Warto tutaj zaznaczyć, że te wymogi nakładają konieczność zapewnienia wysokiego poziomu bezpieczeństwa, który jest wymagany dla wszystkich systemów podłączonych do sieci publicznej. Jak widać, jest to obowiązek wspólny dla wszystkich systemów komputerów, które są podłączone do sieci Internetu.

Wymogi stawiane w zależności od poziomu bezpieczeństwa systemów informatycznych według Generalnego Inspektora Ochrony Danych Osobowych są następujące (Krasińska i Mizerek oprac., 2011):

1. Dla poziomu niskiego:
   a) obszar, w którym przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;
   b) przebywanie osób nieuprawnionych w obszarze, w którym przechowywane są dane osobowe, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych;

c) w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych;
d) jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas pilnuje się, aby:
   – w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
   – dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia;
e) system informatyczny służący do przetwarzania danych osobowych zabezpiecza się w szczególności przed:
   – działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
   – utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
f) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie;
g) w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się z co najmniej 6 znaków;
h) dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych;
i) kopie zapasowe:
   – przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
   – usuwa się niezwłocznie po ustaniu ich użyteczności;
j) osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym są przetwarzane, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych;
k) urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do:
   – likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

– przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
– naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

2. Dla poziomu podwyższonego:
   a) w przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono z co najmniej 8 znaków i zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
   b) urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych;
   c) instrukcję zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.
3. Dla poziomu wysokiego:
   a) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
   b) w przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
      – kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną,
      – kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

Jak widać, tych reguł jest na tyle dużo, że umieszczając dane oraz systemy w modelu *cloud computing* należy dokładnie sprawdzić, w jaki sposób ten model przetwarzania danych pozycjonowany będzie w kontekście zgodności z prawem przetwarzania danych osobowych.

Bibliografia

Krasińska M, Mizerek S. oprac. (2011), *ABC wybranych zagadnień z ustawy o ochronie danych osobowych*, www.giodo.gov.pl/487/id_art/4739/j/pl/ 2011 (dostęp 1.03.2013).

Buyya R., Broberg J., Goscinski A. red. (2011), *Cloud Computing: Principles and Paradigms*, John Wiley & Sons, Inc., New Jersey.

Cafaro M., Aloisio G. red. (2011), *Grid, Couds and Virtualization*, Springer-Verlag London Limited, London.

Gartner (2008), *Seven cloud-computing security risks*, www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 (dostęp 1.03.2013).

Gens F. (2009), *New IDC IT Cloud Services Survey: Top Benefits and Challenges*, http://blogs.idc.com/ie/?p=730 (dostęp 1.03.2013).

Hugos M., Hulitzky D. (2011), *Business in the Cloud*, John Wiley & Sons, Inc., Hoboken, New Jersey.

Rittinghouse J.W., Ransome J.F. (2010), *Cloud Computing Implementation*, *Management, and Security*, CRC Press, Boca Raton.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, DzU z. 2004 r., nr 100, poz. 1024, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20041001024 (dostęp 1.03.2013).

Shrof G. (2010), *Enerprise Cloud Computing*, Cambridge University Press, New York.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, DzU z 1997 r., nr 133, poz. 883, http://isap.sejm.gov.pl/DetailsServlet?id=WDU19971330883 (dostęp 1.03.2013).

Zwolnienia z obowiązku rejestracji, http://www.giodo.gov.pl/530/id_art/2659/ (dostęp 1.03.2013).

SECURITY OF DATA PROCESSING IN CLOUD COMPUTING MODEL – CONDITIONS IN THE CONTEXT OF DATA PROTECTION IN THE CONDITIONS OF THE POLISH LAW

Summary

Processing model of cloud computing is an increasingly popular data processing technology. At the same time important to be aware of its strengths, but also limitations.

This paper presents aspects of the use of cloud computing technology in the context of the legal aspects of the protection of personal data.

Translated by Grzegorz Wojarnik

Keywords: IT technologies, cloud computing, personal data protection