GIODO: Przetwarzanie danych osobowych w chmurach jest dopuszczalne, ale...

Opracowanie: Marcin Maj (Dziennik Internautów - di.com.pl), 24.05.2011

Firmy sięgają po cloud computing, zatem nasze dane osobowe też będą trafiać do chmur. Czy można przetwarzać dane osobowe w chmurze? Czy potrzebne są zmiany w prawie danych osobowych? Dziennikowi Internautów odpowiedzi na te pytania udzielił dr Wojciech Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych.

DI: Chmury często kojarzą się z usługami dla konsumentów, ale chyba większy problem z punktu widzenia ochrony danych osobowych przedstawiają te usługi chmurowe, które będą adresowane do firm i będą im pozwalały na redukcję swojej infrastruktury.

dr Wojciech Wiewiórowski (GIODO): Tak to prawda, choć uważam, że to jest kwestia dotycząca zarówno przedsiębiorców, jak i administracji publicznej, bo i ta rozważa, czy nie mogłaby części informacji, które posiada, przechowywać w przy zastosowaniu technologii chmurowych.

DI: Zatem jakaś firma świadcząca dla mnie usługę może przekazywać moje dane dalej, innej firmie świadczącej usługę chmurową. Automatycznie nasuwa się pytanie o to, kto odpowiada za dane i jak można to wszystko kontrolować.

GIODO: Musimy zacząć od stwierdzenia, że samo przetwarzanie w chmurach jest obecnie dopuszczalne prawnie, również z punktu widzenia przepisów dotyczących ochrony danych osobowych. Zatem możliwe jest przygotowanie tego typu oferty dla klientów indywidualnych, przedsiębiorców czy administracji publicznej. Bardziej istotne jest to, w jakiego rodzaju chmurze dane mają być przetwarzane - czy jest to klasyczna chmura publiczna, która obejmuje centra przetwarzania danych znajdujące się w dowolnym miejscu na świecie, wybranym przez jej dostarczyciela, czy też mamy do czynienia z różnego rodzaju chmurami dedykowanymi (np. prywatnymi lub hybrydowymi), na których kształt i sposób działania ma wpływ również ten, kto jest użytkownikiem chmury, a nie tylko ten, kto jest jej dostawcą.

Teoretycznie już dziś możliwe jest stosowanie obu tych rozwiązań, choć w jednym miejscu napotykamy problem, który jest bardzo trudny do przezwyciężenia. Z punktu widzenia obowiązujących przepisów przetwarzanie danych, zwłaszcza danych osobowych w chmurze obliczeniowej, może nastąpić tylko wtedy, jeżeli ten, kto przekazuje dane (użytkownik chmury), będzie w stanie ustalić, w których centrach przetwarzania (tzn. gdzie umieszczonych) dane te będą przetwarzane.

Ponadto już dziś część dostarczycieli chmur zapewnia użytkowników, że dane osobowe będą przetwarzane tylko w centrach znajdujących się na terenie Unii Europejskiej, co ma oznaczać, że dane osobowe nie będą przekazywane do tzw. krajów trzecich, o których mowa w ustawie o ochronie danych osobowych. Wydawać by się zatem mogło, że zapewniony będzie wystarczający poziom ochrony tych danych. Lecz niestety, tylko może się tak wydawać. Bowiem problemem niezmiernie trudnym do rozwiązania, jest to, że umowa o przetwarzanie danych w chmurze, która musiałaby się stać umową o przekazanie danych do przetwarzania w rozumieniu art. 31 ustawy o ochronie danych osobowych, powinna zapewniać administratorowi danych osobowych (czyli użytkownikowi chmury) uprawnienia kontrolne wobec dostarczyciela chmury. To jest, moim zdaniem, najsłabszy punkt stosowania istniejących przepisów na potrzeby przetwarzania danych osobowych chmurze, bo jeżeli którykolwiek z dostarczycieli chmur będzie mnie próbował przekonać, że administrator danych osobowych będzie miał możliwość kontroli jego centrów przetwarzania danych, to pozwolę sobie nie do końca w to uwierzyć. Wydaje mi się, że zorganizowanie tego typu rozwiązania, zarówno od strony technicznej, jak i od strony czysto biznesowej, byłoby co najmniej bardzo trudne. Dodatkowym problemem – przekraczającym ramy tego wywiadu – jest przetwarzanie w chmurach informacji objętych tajemnicami prawnie chronionymi (np. informacji niejawnej), gdzie jej „eksport" do centrów obliczeniowych poza terenem Polski może być prawnie zabroniony.

DI: Czy w związku z tym istnieje potrzeba zmiany prawa?

GIODO: Myślę, że w jakimś stopniu tak, choć ta potrzeba zmiany prawa niekoniecznie musi polegać na tworzeniu aktu prawnego dotyczącego cloud computingu. Nawet powiedziałbym, że bardzo niechętnie widziałbym osobny akt prawny, który dotyczy tylko tego zagadnienia. Raczej wydaje mi się, że istnienie cloud computingu powinno zostać uwzględnione w przygotowywanych obecnie nowelizacjach ustaw dotyczących ochrony prywatności i bezpieczeństwa zasobów. Dla mnie możliwym do przyjęcia rozwiązaniem, którego nie ma w prawie polskim, a zaczyna być już wykorzystywane w innych krajach Unii Europejskiej, jest rozwinięcie idei, która nazywa się Binding Corporate Rules (BCR), czyli „wiążące reguły korporacyjne". Umożliwiałoby ono potraktowanie przedsiębiorcy - dostarczyciela chmury jako „zaufanego obszaru przetwarzania danych".

Dzisiaj nie tylko ustawa o ochronie danych osobowych, ale też dyrektywa, którą ona wdraża, jest skrajnie terytorialna, czyli mówi o przetwarzaniu na terenie Polski, przetwarzaniu na terenie Unii Europejskiej, przetwarzaniu w krajach trzecich, które zapewniają adekwatną ochronę - wszystko odnosi do poziomu państw. Natomiast rozsądnym rozwiązaniem byłoby potraktowanie korporacji, które wprowadziły takie Binding Corporate Rules dotyczące przetwarzania danych osobowych jako czegoś w rodzaju odpowiednika państw. Czyli potraktowanie firmy X, która jest dostarczycielem chmury, jako zaufanego obszaru przetwarzania danych. To jest rozwiązanie, które jest możliwe, ma już nawet pewnego rodzaju historię w opiniach Grupy Artykułu 29, w ramach której spotykają się rzecznicy ochrony danych osobowych z wszystkich krajów Unii Europejskiej, natomiast dla prawa polskiego byłaby nowa.

Temu zagadnieniu chcemy poświęcić dwa wydarzenia organizowane w naszym Biurze - 14 czerwca 2011 r. konferencję dotyczącą BCR w Polsce, zaś 15 czerwca 2011 r. warsztaty międzynarodowe z przedstawicielami innych organów ochrony danych osobowych na temat tego, jak radzić sobie z BCR.

DI: Właściwie od jak dawna ten temat istnieje wśród specjalistów od ochrony danych osobowych?

GIODO: Temat cloud computingu był poruszany na spotkaniach tzw. Grupy Berlińskiej, czyli grupy, która zajmuje się ochroną danych osobowych i ochroną prywatności w telekomunikacji i w internecie, mniej więcej półtora roku temu, czyli w tym momencie, kiedy serwisy cloud computingowe zaczęły być coraz bardziej powszechne. Myślę, że sporym przełomem było również to, co w 2009 r. zrobiła ENISA, czyli Agencja Unii Europejskiej zajmująca się bezpieczeństwem w sieci. Opublikowała ona dwa dokumenty dotyczące problemów prawnych związanych z cloud computingiem, które wywołały dyskusję na ten temat w kręgach międzynarodowych. Polska stara się być w tej kwestii bardzo aktywna od samego początku dyskusji. Od chwili objęcia przeze mnie funkcji Generalnego Inspektora Ochrony Danych Osobowych, czyli od sierpnia 2010 roku, starałem się wskazywać na tę tematykę, mając świadomość, że w najbliższym czasie będzie to jedno z istotniejszych zagadnień. W tej sprawie jesteśmy też dość aktywni na spotkaniach międzynarodowych. Można zatem powiedzieć, że od półtora roku cloud computing jest jednym z tematów dyskusji, natomiast podejścia do niego w różnych krajach UE bywają różne, choć wynika to raczej z charakteru obowiązujących tam przepisów prawnych niż z jakichś problemów filozoficznych rozumienia cloud computingu czy jego znaczenia.

Zdajemy sobie sprawę z tego, że cloud computing będzie coraz bardziej popularny. Może za trzy lata usługa ta rozwinie się i zyska nową nazwę, ale ten model biznesowy jest czymś, co musi być obszarem zainteresowań rzeczników ochrony danych osobowych.

DI: Komisja Europejska rozpoczęła niedawno konsultacje dotyczące cloud computingu. Czy Pan weźmie udział w tych konsultacjach? Co Pan będzie proponował?

GIODO: Indywidualnie jako GIODO z Polski prawdopodobnie nie. Raczej będę się starał uczestniczyć w przygotowywaniu stanowiska, które wyraziłaby Grupa Artykułu 29 reprezentująca wszystkich rzeczników ochrony danych osobowych z państw Unii Europejskiej, chyba że pojawi się jakiś problem, który będzie bardzo specyficzny dla Polski, co - szczerze mówiąc - nie wydaje mi się prawdopodobne. Raczej wolałbym, żeby głos w tej sprawie wspólnie zabrali wszyscy unijni rzecznicy ochrony danych osobowych, bo wówczas będzie to głos mocny, a przez to bardziej skuteczny. Przy czym zaznaczam, że koledzy z Europy wiedzą, że polski rzecznik jest zainteresowany stałym udziałem w odbywających się w tej sprawie konsultacjach zmierzających do wypracowania owego wspólnego stanowiska.

Przy okazji rozmowy na temat cloud computingu pragnę zwrócić uwagę, że na ten temat pojawia się coraz więcej dobrej literatury, dostępnej również w internecie. Wskazuję na nią podczas każdego swojego wystąpienia o cloud computingu. Warto się z nią zapoznać, ponieważ wiele rozwiązań, nie tylko z Europy czy z USA, ale np. australijskich, jest naprawdę wartych przestudiowania i rozważenia, na ile mogą one nam pomóc w rozwiązywaniu polskich problemów.