Jak się upewnić, że usunięcie pliku z chmury jest skuteczne

Podpisując umowę na usługi przechowywania danych, warto poprosić o **gwarancje prawne i technologiczne.** Często stosuje się rozwiązania proceduralne, np. komisyjne niszczenie nośników informacji

Bartosz Marcinkowski
radca prawny, partner w kancelarii Domański Zakrzewski Palinka

Problem usuwania informacji, w tym danych osobowych, dotyczy nie tylko usług chmurowych (ang. cloud computing), lecz także wszelkich innych sytuacji, w których informacje zostają powierzone w celu ich przetwarzania, zwykle profesjonalnej firmie zajmującej się obróbką danych. Mówiąc o obróbce, mamy na myśli takie operacje, jak przechowywanie danych, ich aktualizacja, opracowywanie czy inne sposoby wykorzystywania dla celów i w sposób wskazany w umowie przez ich dysponenta, czyli administratora danych.

Jednak w przypadku usług chmurowych, świadczonych na dużą skalę i na rzecz dużej liczby podmiotów, problematyka zakończenia relacji prawnej i skutecznego, całkowitego usunięcia danych przez podmiot przetwarzający (tak zwanego procesora danych) stanowi przedmiot szczególnych obaw zleceniodawców. Chodzi wszak nie tylko o znaczne ilości informacji, lecz także o ich poufny charakter i odpowiedzialność przedsiębiorcy–zleceniodawcy jako administratora danych za brak należytej dbałości o dane osobowe znajdujące się w jego gestii. [ramka 1]

Wielu przedsiębiorców stawia pytanie: w jaki sposób zagwarantować, że informacje, które były powierzone procesorowi, zostaną całkowicie usunięte w sposób uniemożliwiający ich odtworzenie. Nie chodzi przy tym o deficyt zaufania, ale o ostrożność i pewność, że dane nie trafią w niepowołane ręce, a ich administrator pozostanie jedynym podmiotem, który nad danymi panuje i może nimi zgodnie z prawem dysponować.

Omawiając zagadnienie, trzeba wyraźnie wskazać dwie płaszczyzny. Po pierwsze – płaszczyznę prawną – tzn. w jaki sposób i w jakim zakresie można zapewnić metodami prawnymi (kontraktowymi) określone postępowanie stron umowy. Drugą jest płaszczyzna technologiczna, która sprowadza się do pytania, jakie środki technologiczne mogą i powinny być zastosowane w celu usunięcia informacji z nośników.

Unicestwienie czy anonimizacja

Mówiąc o regulacjach prawnych, należy rozróżnić dwie kategorie pojęć. Pierwszą z nich jest całkowite usuwanie (unicestwianie) informacji (art. 7 pkt 3 u.o.d.o.), w tym fizyczne unicestwienie nośników informacji, na których przechowywane są na przykład dane osobowe. Drugą kategorią jest anonimizacja danych osobowych – tak określa się pozbawienie ich cech umożliwiających powiązanie z konkretnymi osobami.

Teoretycznie ta druga możliwość jest zabiegiem prostym, gdyż poprzez usunięcie określonych jednostkowych informacji można osiągnąć zamierzony skutek oderwania danych od poszczególnych jednostek.

Można przy tym wyróżniać wiele metod dokonania takiej anonimizacji. Przede wszystkim można mówić o stosunkowo oczywistym zabiegu, jakim jest wyeliminowanie określonych informacji dotyczących konkretnych osób. Chodzi o podstawowe dane identyfikacyjne, takie jak imię, nazwisko czy adres zamieszkania. Taki zabieg może – acz nie musi – zapewnić skuteczną anonimizację danych. Dane stają się danymi statystycznymi bądź też w swym charakterze do nich zbliżonymi.

Obszerny dokument poświęcony metodom anonimizacji danych opracowała tzw. Grupa Robocza Art. 29 – unijne gremium, w skład którego wchodzi między innymi polski generalny inspektor ochrony danych osobowych. W opinii nr 05/2014 w sprawie technik anonimizacji z 10 kwietnia 2014 r. wyróżniono m.in. takie zabiegi, jak: pseudonimizacja, randomizacja, uogólnienie, agregacja czy dywersyfikacja danych.

Ale uwaga: ostatecznie sama Grupa Robocza stwierdza jednak, że żadna z opisanych metod nie daje stuprocentowej pewności i nieodwracalności przeprowadzonego procesu. [ramka 2]

Przepisy prawa nie wystarczą

Jednak zarówno w przypadku anonimizacji, jak i usuwania informacji wciąż aktualne pozostaje pytanie, jak uzyskać pewność, że zamierzony proces został dokonany w sposób prawidłowy, definitywny, a dane nie zostały skopiowane lub przekazane kolejnym podmiotom.

Zasadne jest zatem pytanie, czy samymi rozwiązaniami prawnymi można osiągnąć stuprocentową gwarancję określonego zachowania partnera biznesowego. Otóż należy uznać, że metodami wyłącznie kontraktowymi gwarancji takiej nie osiągniemy. Rozwiązania prawne mogą wprawdzie stymulować, motywować i mobilizować stronę umowy do podjęcia określonych działań (rola prewencyjna), jednak same przez się nie chronią przed naruszeniem uzgodnień.

Precyzyjne zapisy

Dlatego standardowo w umowach o powierzenie przetwarzania danych (co reguluje art. 31 u.o.d.o.) konieczne jest zastosowanie dodatkowych zapisów, które precyzują zasady zwrotu danych zleceniodawcy, jak również kwestie usuwania informacji i zakazu ich nieautoryzowanego przekazywania osobom trzecim.

W umowach często przewidziane są rozwiązania proceduralne, takie jak wymóg komisyjnego usuwania nośników informacji czy rejestrowania procesu ich usuwania. Niemniej jednak znów pojawia się wątpliwość: wobec mobilności i łatwości powielania informacji fakt unicestwienia nośnika traci na znaczeniu, nawet w razie zabezpieczenia danych środkami kryptograficznymi.

Gwarancje i kary umowne

Dlatego też opisanym zobowiązaniom usługodawcy towarzyszą zwykle prawnie wiążące zapewnienia gwarancyjne dotyczące jego postępowania. Co więcej: przestrzeganie wskazanych zobowiązań może być zabezpieczone np. karami umownymi wymagalnymi w razie naruszenia postanowień umowy.

Kary te pełnią przede wszystkim funkcję dyscyplinującą, aczkolwiek nie można wykluczyć ich realnego wymierzenia, choć – trzeba tutaj dodać – ich dochodzeniu na drodze sądowej mogą towarzyszyć poważne trudności natury dowodowej. Konkretnie: przekonujące wykazanie, że dane nie zostały skutecznie usunięte lub zanonimizowane, może w praktyce być bardzo utrudnione. Nie dotyczy to jednoznacznych przypadków, na przykład gdy źródło wycieku danych nie może budzić wątpliwości. [przykłady 1 i 2]

Staranny wybór przetwarzającego

Zatem siłą rzeczy opisane rozwiązania – przepisy prawa i zapisy kontraktowe – nie mogą zapewnić pełnego komfortu uczestnikom obrotu, pozostawiając pewną sferę ryzyka.

Dlatego gwarancje prawne (i pozaprawne okoliczności biznesowe) mogą i powinny być wsparte rozwiązaniami informatycznymi.

Zwłaszcza że kasowanie danych w chmurze jest – również w ujęciu informatycznym – dość złożonym zagadnieniem. Z jednej strony obejmuje techniczne metody usuwania bieżących danych w wyniku zwykłych operacji użytkownika chmury. Z drugiej strony dotyczy również trwałego usunięcia danych w przypadku ewentualnej rezygnacji z usług online. [rozmowa]

W tej sytuacji szczególnego znaczenia nabierają renoma procesora danych, historia jego dotychczasowych osiągnięć i reputacja.

Podsumowując, dopiero kompleksowe rozwiązania prawno-informatyczne i proceduralne mogą przynieść zamierzony skutek i dać pewność usunięcia danych.

Ramka 1. Administrator odpowiada

Zgodnie z ustawą o ochronie danych osobowych z 29 sierpnia 1997 r. (t.j. Dz.U. z 2015 r. poz. 2135 ze zm.; dalej: u.o.d.o.) administrator danych może ponieść odpowiedzialność karną za wiele naruszeń związanych z przetwarzaniem danych osobowych, w tym za naruszenie obowiązku ich odpowiedniego zabezpieczenia. Obecnie u.o.d.o. nie przewiduje odpowiedzialności finansowej administratora za brak należytej dbałości przy przetwarzaniu danych osobowych. Ma się to jednak zmienić wraz z wejściem w życie planowanego nowego unijnego rozporządzenia dotyczącego ochrony danych osobowych (II kwartał 2018 r.), które przewiduje kary finansowe w wysokości nawet do 20 mln euro za naruszenie przepisów ochrony danych osobowych.

Ramka 2. Dyrektywa daje alternatywę

Przepisy unijne uznają anonimizację przechowywanych danych osobowych jako alternatywę dla ich usunięcia. Przykładowo w dyrektywie 2002/58/WE z 12 lipca 2002 r. o prywatności i łączności elektronicznej (Dz.Urz. UE z 2012 r. L 201, s. 37) motyw 26 stanowi, że: „Dane dotyczące ruchu wykorzystywane w marketingu usług komunikacyjnych lub dostarczenia usług tworzących wartość dodaną powinny również zostać usunięte lub uczynione anonimowymi po dostarczeniu usług".
Podobnie art. 6 ust. 1 stanowi, że:
„Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu(...)". JP

trzy pytania

Poufność jest utrzymywana od początku do końca umowy

MIROSŁAW SZYMCZAK
Microsoft, Cloud Solutions Sales Manager

Co się dzieje z danymi informatycznymi klienta przechowywanymi w chmurze, które mają zostać skasowane?
Po zakończeniu umowy subskrypcja przechodzi w tryb zwany „okresem prolongaty". W tym 30-dniowym okresie usługa świadczona jest w normalny sposób, pozwalający klientowi na dostęp i zrobienie kopii zapasowych lub migrację zgromadzonych danych. W tym czasie administrator otrzymuje powiadomienia na temat daty wygaśnięcia usługi i terminu zablokowania jej świadczenia. Następnie usługa przechodzi w tryb „wyłączenia" – 90-dniowy okres, w którym do danych ma dostęp tylko administrator subskrypcji i w którym może dokonać operacji związanych z tworzeniem kopii zapasowych i migracji danych. Okres ten na życzenie można skrócić. Po jego zakończeniu dane klienta są całkowicie usuwane z naszego centrum danych, ich odzyskanie nie jest możliwe.

Jaka jest gwarancja, że tak się stało rzeczywiście?
Zasady, procedury i mechanizmy wdrożone dla całkowitego i bezpiecznego usuwania danych ze wszystkich nośników zapewniają, że danych nie można odzyskać przy użyciu jakichkolwiek środków technicznych. Microsoft używa procedur i rozwiązań usuwania danych zgodnych ze standardem NIST 800–88 (Narodowy Instytut Standardów i Technologii, Publikacja Specjalna 800–88, wytyczne dla sanityzacji mediów). Dla dysków twardych, które nie mogą być skasowane, używany jest proces fizycznego zniszczenia, w trakcie którego dyski ulegają rozdrobnieniu, co sprawia, że odzyskiwanie danych jest niemożliwe. Odpowiednie środki usuwania zależą od rodzaju dysku czy urządzenia. Protokoły zniszczenia dysków są przechowywane i audytowane zgodnie z procesem ISO, a bezpieczne usuwanie danych i ponowne wykorzystania sprzętu wykonywane jest zgodnie z normami ISO 27001. Rygorystyczne inspekcje przeprowadzane są przez podmioty zewnętrzne, np. British Standards Institute. Ponadto w ramach dbałości o jawność działań dajemy możliwość sprawdzenia tego, jak wdrażamy wiele z tych środków bezpieczeństwa – klient może poprosić podmioty wystawiające certyfikaty o przekazanie wyników audytów lub uzyskać te wyniki od przedstawiciela firmy.

Jak wygląda bieżące kasowanie danych?
We wszystkich przypadkach poufność danych utrzymywana jest w całym cyklu życia danych. W szczególności system przechowywania danych sprawia, że dane klientów stają się niedostępne natychmiast po wykonaniu operacji usunięcia (delete). Wszystkie operacje na danych, w tym usuwanie, są spójne. Na przykład wykonanie operacji usuwania danych kasuje wszystkie odwołania do powiązanego elementu danych i nie można do nich uzyskać żadnego dostępu za pośrednictwem interfejsów bezpośrednich ani programistycznych. Również żadne interfejsy nie pozwalają na odczyt danych niezainicjowanych, tym samym uniemożliwiając czytanie usuniętych danych tego samego lub innego klienta, zanim miejsce na dysku będzie nadpisane. Bity fizycznych danych są nadpisywane, kiedy odpowiedni blok pamięci jest ponownie wykorzystany do przechowywania innych danych, tak jak jest to robione na standardowych dyskach twardych komputerów.

PRZYKŁAD 1

Nie zabezpieczyła się – ma kłopoty

Firma X powierzyła firmie Y przetwarzanie danych osobowych przy użyciu usługi chmurowej, nie zastrzegając przy tym w umowie procedury usuwania danych po rozwiązaniu umowy. Po rozwiązaniu umowy firma Y jedynie poinformowała firmę X o usunięciu danych, nie wykazując jednak, jak tego dokonała. W efekcie firma X musi teraz wzmocnić monitoring sieci pod kątem ustalenia, czy należące do niej dane nie wyciekły do wiadomości publicznej. Firma X jako administrator danych osobowych jest bowiem pierwotnie odpowiedzialna za ewentualne naruszenie bezpieczeństwa danych osobowych (z ewentualnym prawem regresu z tego tytułu wobec firmy Y).

PRZYKŁAD 2

Przezorny zawsze ubezpieczony

Firma X postanowiła powierzyć firmie Y przetwarzanie danych z użyciem usługi chmurowej. Firma X zastrzegła w umowie procedury na okoliczność usuwania danych po rozwiązaniu umowy oraz wpisała do umowy zapis wprowadzający karę umowną w wysokości do 200 tys. zł w wypadku wycieku danych, pomimo ich komisyjnego zniszczenia.
W tej sytuacji firma X ma prawo uczestniczyć w fizycznym niszczeniu nośnika zawierającego dane osobowe. Natomiast kara umowna ma funkcję prewencyjną wobec następczego wycieku danych z winy firmy Y.