Cyberlaw.pl

CSA PL cloud security POLAND alliance SM

prezentują

Jak polscy dostawcy podchodzą do umowy powierzenia?

Raport z badania 2014

wzbogacony o rozmowę z Generalnym Inspektorem Ochrony Danych Osobowych

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Spis treści

Warszawa, 09.10.2014

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Wstęp

Outsourcing infrastruktury IT przybiera różne formy. Wiąże się z optymalizacją i jest chętnie wybierany przez przedsiębiorców. Jedną z najpopularniejszych odmian jest hosting oraz usługi chmurowe polegające na udostępnianiu miejsca na serwerze/serwerach.

Przedsiębiorcy, którzy decydują się na rozwiązania dostawców korzystają z zasobów m.in. w celu postawienia swoich własnych systemów pozwalających na obsługę ich klientów - osób fizycznych - taką jak przyjmowanie zamówień czy ich realizację w trybie online.

Postanowiliśmy bazować na powyższym przykładzie i sprawdzić jak dostawcy zareagują na potrzeby odbiorców swoich usług, dla których ważne jest bezpieczeństwo przetwarzanych danych oraz spełnienie wymagań przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zależało nam także na tym aby sprawdzić jak usługodawcy komunikują się ze swoimi potencjalnymi klientami oraz jakie i czy odpowiednie informacje im przekazują.

Badanie zostało przeprowadzone w dniach 13 - 22 sierpnia 2014r.
Jest to pierwsze tego typu badanie w Polsce. Wynikom przyglądamy się od strony dostawców, ich klientów oraz Generalnego Inspektora Ochrony Danych Osobowych.

Raport jak i samo badanie mają charakter wyłącznie edykacyjny.
Nie publikujemy nazw firm i ich wyników, aczkolwiek pełna lista dostępna jest na cele edukacyjne dla członków CSA Polska.

Zapraszamy

Beata Marek, Cyberlaw

Marcin Fronczak, CSA Polska

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Wstęp

Badanie zostało przeprowadzone przez Cyberlaw oraz Cloud Security Alliance Polska.

Cyberlaw.pl

Cyberlaw jest firmą prawniczą, która specjalizuje się w prawie nowych technologii.

Klientami są spółki z sektora TMT (Technologie, Media, Telekomunikacja), a także jednoosobowe działalności prowadzone przez programistów.

Najczęściej wprowadzamy na rynek polski i zagraniczny innowacyjne startupy z branży IT, aplikacje webowe i mobilne oraz e-sklepy. Zajmujemy się także bieżącą obsługą już istniejących projektów internetowych.

Skład zespołu jest interdyscyplinarny.

Dowiedz się więcej

CSA PL cloud security POLAND alliance SM

CSA Polska jest częścią globalnego Stowarzyszenia Cloud Security Alliance, które jest platformą komunikacji pomiędzy różnymi podmiotami takimi jak: eksperci w zakresie zarządzania ryzykiem i bezpieczeństwem informacji, prawnicy, przedstawiciele instytucji naukowych, dostawcy i odbiorcy usług.

Ta różnorodność sprawia, że CSA Polska jest doskonałym miejscem do wymiany wiedzy oraz doświadczeń w zakresie bezpieczeństwa cloud.

Dołącz do nas

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Metodyka

Badanie zostało przeprowadzone metodą ankietową i metodą wywiadu na grupie 50 losowo wybranych dostawców, którzy pozytywnie zakwalifikowali się jako podmioty, u których można zrealizować założony przez nas stan faktyczny. Dostawcy nie wiedzieli, że są badani.

Stan faktyczny: Przedsiębiorca zamierza skorzystać z podstawowej oferty na okres trwania 1 roku, która pozwoli mu na wydzielonych zasobach postawić własny system pozwalający na przyjmowanie zamówień od jego klientów - osób fizycznych. Wszystkie procesy związane z obsługą zamówień będą przeprowadzone online i przetwarzane na zasobach dostawcy.

Ankieta składała się z 4 pytań:
1. Czy dostawca uważa się za przetwarzającego / processora?
2. Czy podpisuje umowę powierzenia przetwarzania danych osobowych?
3. Czy umowa jest płatna?
4. Czy można zapoznać się z wzorem umowy przed rozpoczęciem świadczenia usług?

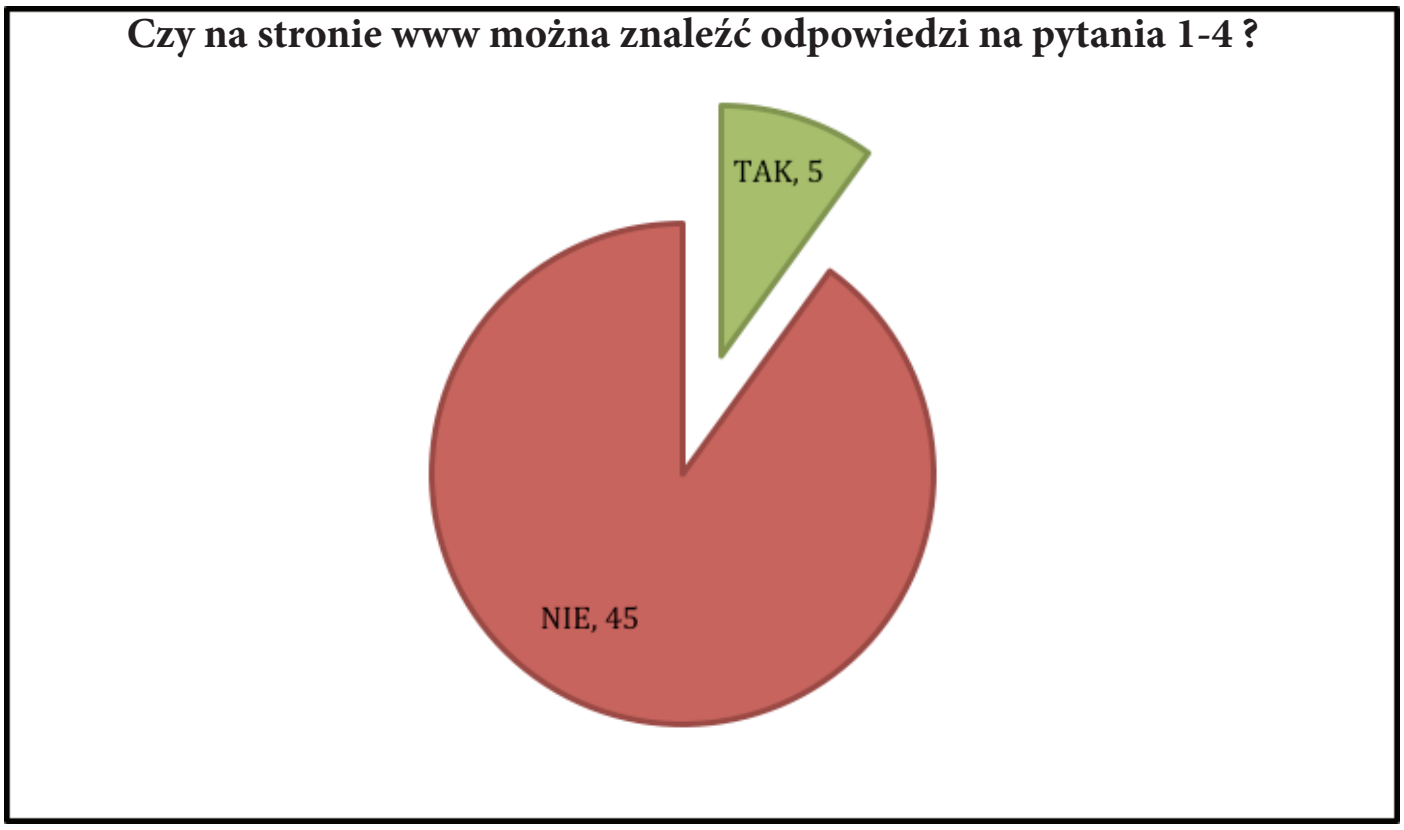
Metoda ankietowa (I faza badania) polegała na zbiorczym zebraniu odpowiedzi przez badacza na podstawie informacji dostępnych na stronie www każdego usługodawcy.

Metoda wywiadu (II faza badania) polegała na udzieleniu odpowiedzi przez każdego z dostawców w trakcie rozmowy z badaczem - potencjalnym odbiorcą usługi. Odpowiedzi były uzyskiwane za pomocą rozmowy telefonicznej z Biurem Obsługi Klienta lub/i korespondencji mailowej z BOK.

Pełna lista badanych firm i szczegółowe omówienie ich wyników jest dostępne wyłącznie na potrzeby edukacyjne dla członków CSA Polska. Jeżeli nie jesteś członkiem Stowarzyszenia, a tematyka cloud jest Ci bliska dołącz do nas.

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Metoda ankietowa



45 podmiotów (90%) nie podaje jakichkolwiek informacji na badany temat.
Tylko na 5 stronach www (10%) znaleźliśmy odpowiedzi.

Uwaga: Spośród 5 dostawców, na których stronach www potencjalny klient może znaleźć odpowiedzi na interesujące go pytania następująca liczba ma dedykowany do tego celu dokument:

- baza wiedzy (2)
- white paper (1)

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Metoda wywiadu

31 dostawców (62%) przyznaje, że będzie przetwarzającym, 16 (32%) jest zdania, że w przypadku świadczenia usługi (w nawiązaniu do przedstawionego stanu faktycznego) nie będzie processorem, 3 (6%) nie potrafi odpowiedzieć na zadane pytanie.

Uwaga 1: Każdy z badanych podmiotów oferował usługę polegającą na udostępnieniu zasobów przy jednoczesnej możliwości przetwarzania przez niego danych osobowych.
Żaden z podmiotów, który nie określał się jako przetwarzający nie wskazywał na siebie jako na Administratora Danych.

Uwaga 2: Spośród 3 dostawców, którzy wskazali, że nie wiedzą jak się kwalifikować następująca liczba podała poniższe argumenty:

- „nie wiemy bo nie jest to jasne” (2)
- „jesteśmy w trakcie konsultacji z GIODO” (1)

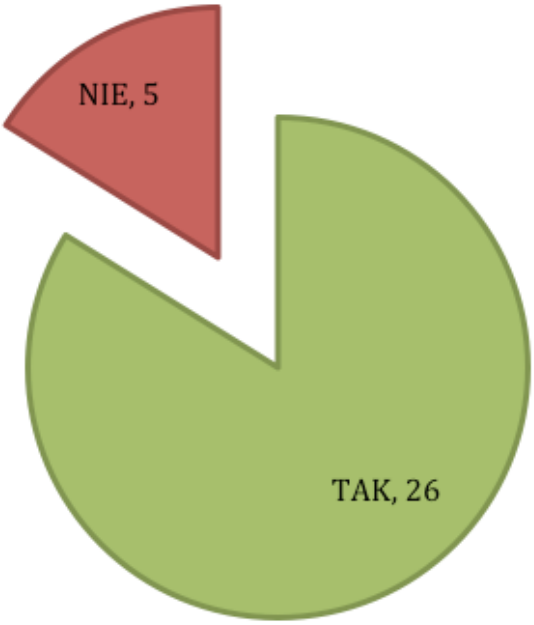
Uwaga 3: Spośród 16 podmiotów, którzy wskazali, że nie będą przetwarzającym następująca liczba podała poniższe argumenty:

- „nie jesteśmy przetwarzającym, o którym mowa w ustawie” (7)
  z czego 1 podał argument
    - „działamy wyłącznie w oparciu o regulamin, nie o umowę”

- „nie przetwarzamy danych” (3)
- „nie mamy dostępu do danych” (3)
- „nie adminitrujemy danymi” (1)
- „nie mamy wiedzy o przeznaczeniu przetwarzania [...] że będą przetwarzane dane osobowe” (1)
- „wykonujemy wyłącznie kopie zapasowe” (1)

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

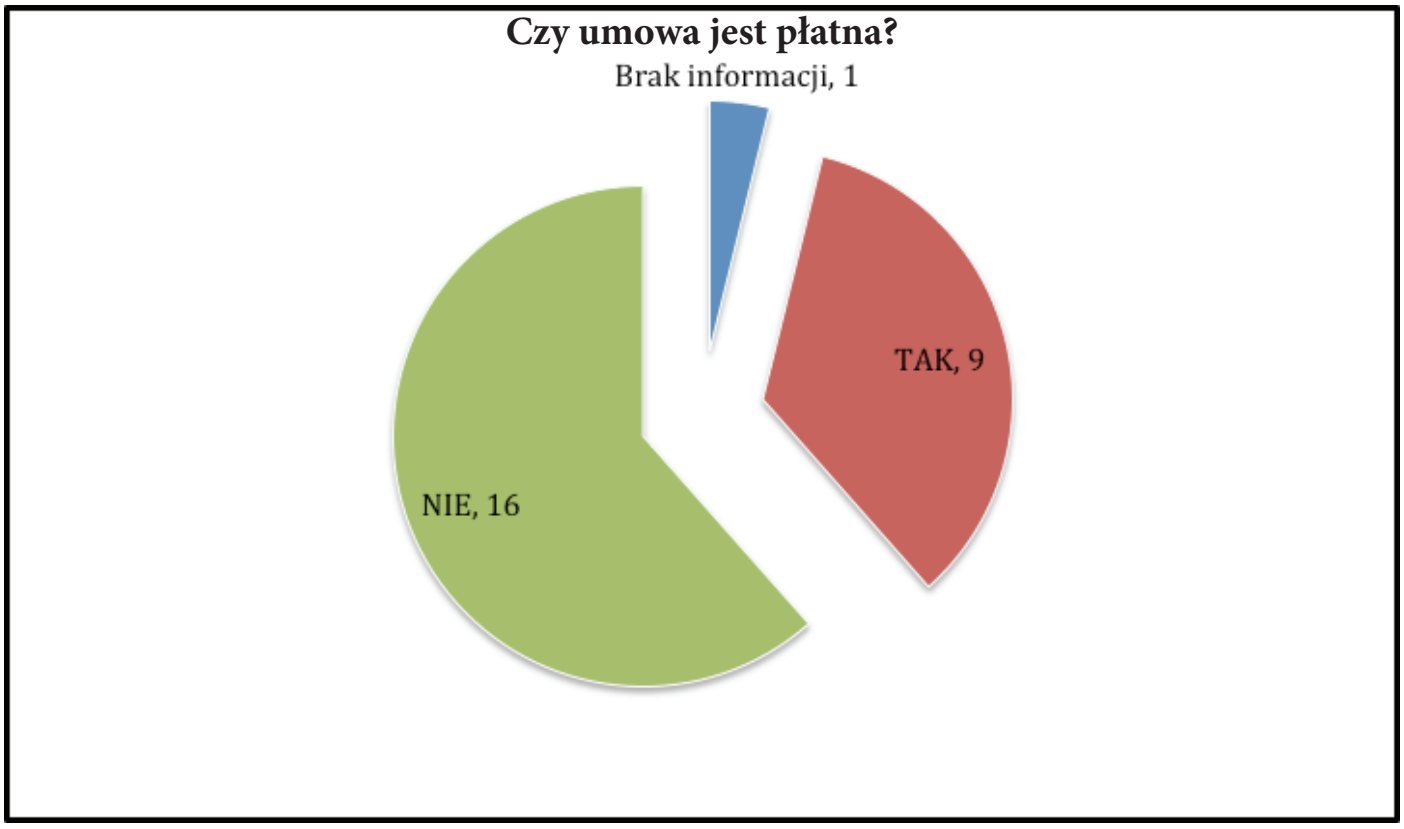
Czy dostawca podpisuje umowę powierzenia przetwarzania danych osobowych?



Spośród 31 podmiotów, którzy uważają się za przetwarzających, 26 (84%) podpisuje umowę powierzenia, 5 (16%) nie przewiduje takiej możliwości.

Uwaga: W przypadku dostawców, którzy nie podpisują umowy powierzenia, potencjalny klient otrzymuje jedną z następujących informacji:

- „nie przetwarzamy danych osobowych na serwerze [...] wykonujemy kopie”
- „w ramach hostingu nie będą i nie są przetwarzane dane osobowe”
- „nie mamy wiedzy o tym, że będą przetwarzane dane osobowe [...] mamy wgląd”
- „z przyczyn technicznych nie jest możliwe zawarcie umowy”
- „nie możemy dać gwarancji, że środowisko spełnia wymagania GIODO”



16 dostawców (~61%) nie pobiera opłaty, 9 (~35%) pobiera, 1 usługodawca (~4%) nie jest w stanie udzielić odpowiedzi.

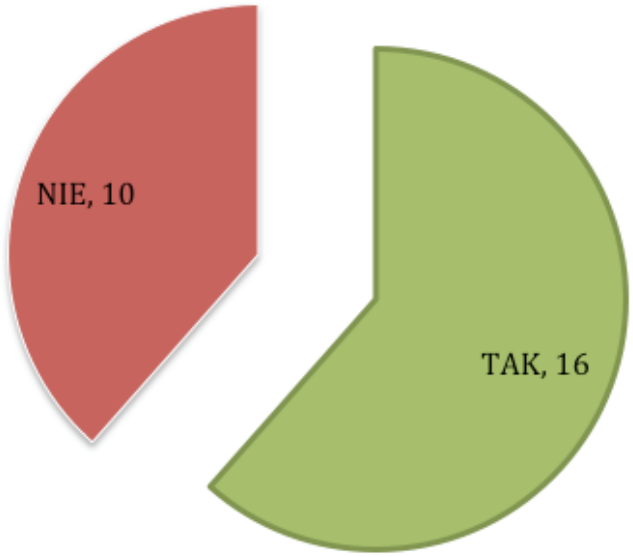
Uwaga: Spośród 9 dostawców, u których należy wnieść opłatę z tytułu powierzenia danych osobowych u 2 (~22%) należy wnosić opłatę co roku, w pozostałych 7 przypadkach (~78%) opłata jest jednorazowa (do cen należy doliczyć VAT):

Jednorazowo:
- 200 zł (2)
- 150 zł (1)
- 100 zł (2)
- 99 zł (1)
- 50 zł (1)

Co roku:
- 120 zł (1)
- 99 zł (1)

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Czy można zapoznać się z wzorem umowy powierzenia przed rozpoczęciem świadczenia usługi?



16 podmiotów (62%) oferuje możliwość wglądu do wzornika umowy przed rozpoczęciem świadczenia usługi, 10 (38%) uzależnia okazanie wzornika od zakupu usługi udostępniania zasobów i rozpoczęcia świadczenia.

Wnioski

Omówienie wyników metody ankietowej:

90% dostawców nie dostarcza jakiejkolwiek informacji na tematy poruszone w badaniu za pomocą strony www czyli głównego kanału sprzedaży swoich usług. Podmioty te są mniej konkurencyjne względem tych, którzy informują potencjalnych klientów na temat dla nich niezwykle istotny czyli powierzania przetwarzania danych osobowych.

Zgodnie z art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych Administrator danych (czyli potencjalny klient dostawcy) może powierzyć innemu podmiotowi (udostępniającemu infrastrukturę IT), w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych.

W przypadku gdy Administrator danych nie zawrze odpowiedniej umowy powierzenia naraża się na uchybienia w trakcie kontroli GIODO i sankcje z tym związane. W jego interesie leży zatem jej zawarcie.

Z punktu widzenia dostawcy umowa powierzenia jest dodatkowym zobowiązaniem jednakże w przypadku świadczenia usług klientom biznesowym jest ona niezbędnym elementem do tego by w ogóle świadczenie tych usług rozpocząć w momencie gdy obie strony wiedzą, że będą przetwarzane dane osobowe.

Dalsza część raportu zawiera rozmowę z Generalnym Inspektorem Ochrony Danych Osobowych, w której m.in. wskazane zostało kiedy dostawca nie może zasłaniać się art. 12 - 15 ustawy o świadczeniu usług drogą elektroniczną.

Tylko 5 dostawców (10%) dostarcza informacje za pomocą swojej strony firmowej dzięki temu ich oferta jest lepiej widoczna i może być lepiej odbierana przez potencjalnych klientów

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Wnioski

Omówienie wyników wywiadu:

6% dostawców nie wie czy określić się jako przetwarzający w sytuacji gdy przedstawiony jest im stan faktyczny. Liczba ta nie jest drastycznie duża, ale w przypadku podmiotów profesjonalnie świadczących usługi outsourcingu IT nie jest to liczba zadowalająca. Odpowiedź sugeruje bowiem potencjalnemu klientowi, że usługodawca nie zna zagadnienia.

Jednocześnie niepokojące jest to, że aż **32%** dostawców nie postrzega siebie jako przetwarzających pomimo tego, że argumenty, którymi się posługują pozostawiają wiele wątpliwości w tym zakresie. Udzielanie zdawkowych odpowiedzi „nie przetwarzamy danych osobowych” bądź „nie mamy wglądu do danych” przy jednoczesnym braku takich informacji w regulaminie usług jak i braku możliwości złożenia takiego oświadczenia na piśmie jest nieprzekonujące. Zauważa się ponadto w tej grupie, że dostawcy nie rozumieją od kiedy można uznać, że wiedzą jakiego rodzaju dane będą przez nich gromadzone i tym samym nie stosuje się wyłączeń, o których mowa w art. 12 - 15 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

62% dostawców wskazuje na siebie jako przetwarzających, ale z tej grupy 3% nie podpisuje umowy powierzenia z klientem. Z punktu widzenia potencjalnego odbiorcy usług jest to sytuacja niedopuszczalna. Oznacza bowiem, że dostawca nie jest transparentny, gdyż określa się jako processor, ale jednocześnie nie podpisuje umowy powierzenia, która jest niezbędna do tego by powierzenie przetwarzania danych było zgodne od strony formalnej.

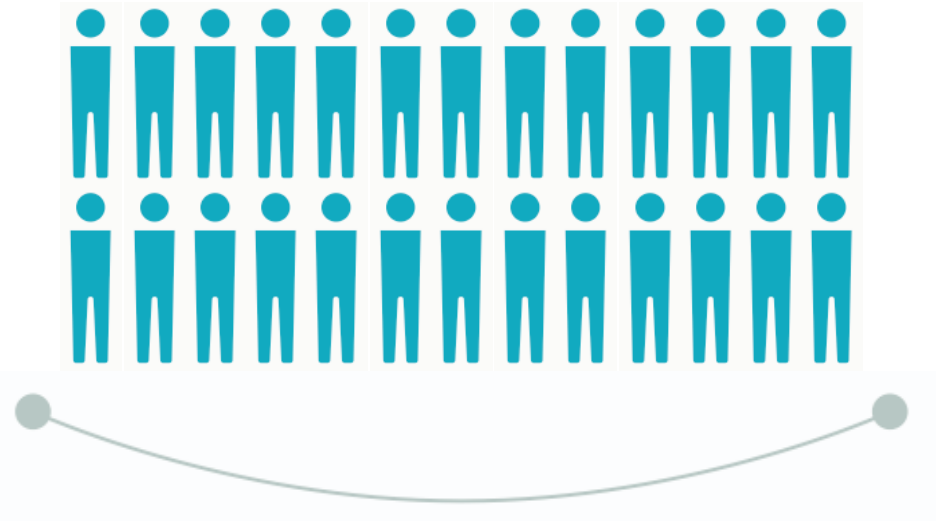
48% dostawców nie podpisuje umów powierzenia co ma bezpośredni wpływ na to, że potencjalny klient szuka innego usługodawcy, który udostępni mu zasoby i pozwoli mu zapewnić zgodność prawną. Dostawcy powinni pamiętać o tym, że zgodność z przepisami dotyczącymi ochrony danych osobowych jest jednym z pierwszych czynników, który ma realny wpływ na wybór ich oferty.

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

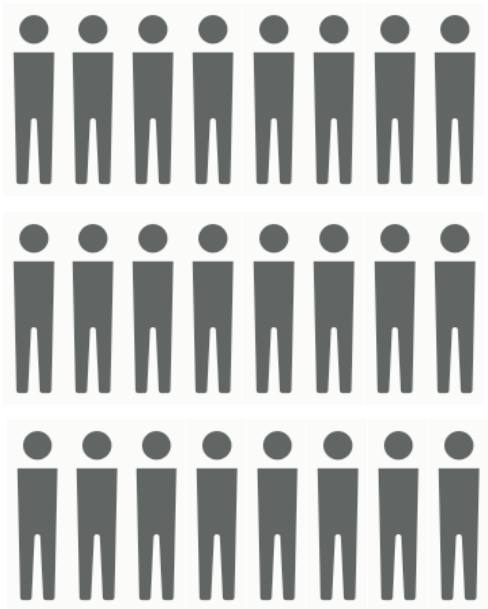
Wnioski

52% dostawców deklaruje podpisanie pisemnej umowy powierzenia przetwarzania danych osobowych, a tym samym odpowiada na potrzeby swoich klientów. Wynik ten nie jest dobry. Oznacza to bowiem, że niewiele ponad połowa badanych firm ma ofertę dostosowaną do potrzeb rynku.

Tylko 26 dostawców może konkurować warunkami oferty o względy klienta



Pozostali dostawcy są poza zasięgiem zainteresowań



biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Wnioski

Spośród dostawców, którzy podpisują umowę, ~**35%** pobiera z tego tytułu opłatę. Opłata ta jest relatywnie niska. Jeżeli jednak klient porównywałby usługi tej samej jakości to niższa opłata z tytułu podpisania umowy powierzenia byłaby konkurencyjna.

1 dostawca (~**4%**), nie potrafił określić wysokości opłaty. Poinformował natomiast, że wycena zostanie przedłożona później. Argumentował to brakiem dostępu do cennika. Z punktu widzenia klienta jest to sytuacja kuriozalna. Zachodzi jednak wysokie prawdopodbieństwo, że dostawca albo nie podpisywał jeszcze umowy powierzenia z klientem albo podpisuje je ze zróżnicowanym cennikiem.

Dla porównania ~**62%** dostawców deklaruje, że nie pobiera dodatkowej opłaty.

Warto wiedzieć, że w umowa powierzenia przetwarzania danych osobowych powinna regulować kwestie wynagrodzenia z tytułu świadczonej usługi. W przypadku braku informacji na ten temat domniemuje się, że z tytułu świadczonej usługi należy się wynagrodzenie. Brak zapisów w umowie jest zatem niekorzystny dla odbiorcy usługi. Przedmiotem badania nie była jednak analiza wzornika umów stąd w tym miejscu jedynie sygnalizujemy, że w umowie powinna pojawić się adnotacja na temat wysokości pobieranego wynagrodzenia bądź odpowiednio braku ponoszenia dodatkowych opłat przez klienta.

Spośród dostawców, którzy podpisują umowę, ~**38%** uzależnia wgląd do wzornika od rozpoczęcia świadczenia usługi głównej (udostępnianie zasobów) na rzecz klienta. Jest to sytuacja wyjątkowo niekorzystna dla odbiorcy usługi, gdyż nie ma on możliwości wglądu do warunków umowy powierzenia i negocjowania zmiany przed wyborem właściwego dostawcy, na którego zasobach „postawi” system. Jednocześnie nie ma pewności czy będzie mógł bezpiecznie i zgodnie z prawem przetwarzać dane, którymi administruje.

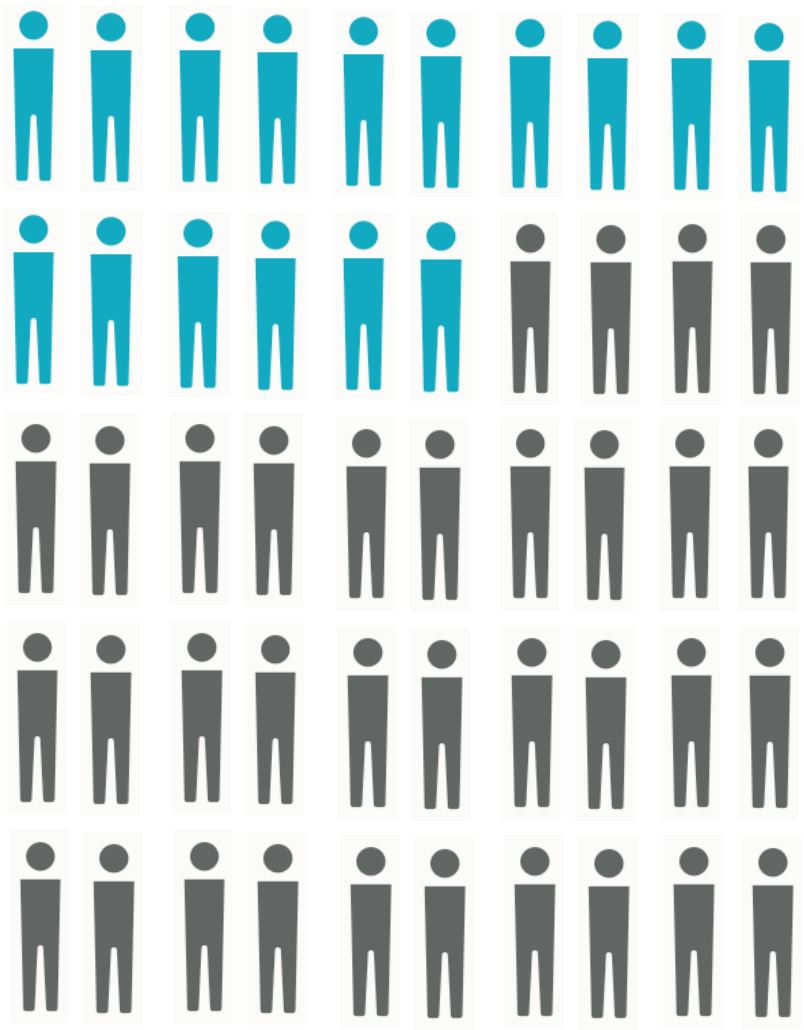
Dla porównania **~62%** spośród tej grupy umożliwia wgląd do wzornika umowy.
A tym samym ...

biuro@bezpiecznachmura.org  beata.marek@cyberlaw.pl

Wnioski

... na uwagę potencjalnego klienta zasługuje zaledwie **32%** spośród wszystkich badanych dostawców. **68%** nie spełnia podstawowych wymagań potencjalnego klienta, gdyż w przedstawionym stanie faktycznym potencjalny klient jako Administrator Danych zobligowany jest do podpisania odpowiedniej umowy powierzenia. Oznacza to zatem, że musi mieć on co najmniej wgląd do umowy i zapoznania się z jej zapisami.

Potencjalny klient spośród ofert 50 dostawców może na poważnie rozważyć tylko 16 z nich



biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Wnioski

22% dostawców (11) deklaruje w swojej ofercie usługi świadczone w modelu cloud computing. Sprawdziliśmy ile z tych usług spełnia wymagania powszechnie stosowanej definicji cloud computingu opracowanej przez amerykańską organizację NIST (ang. National Institute Standards and Technology). NIST definiuje przetwarzanie w chmurze m.in. poprzez określenie 5 istotnych cech:

Szeroki dostęp sieciowy (ang. broad network access) oznacza dostęp do usług z dowolnego miejsca i medium wykorzystującego komukację internetową.

Błyskawiczna elastyczność (ang. rapid elasticity) oznacza, że usługi mogą być błyskawiczne i elastycznie dostarczane (czasem automatycznie). Dla klienta zasoby dostarczane w modelu chmury powinny być możliwe do wykorzystania/zakupienia w dowolnej ilości i w dowolnym czasie. Oznacza to możliwość skalowania i kontraktowania infrastruktury w dowolnym czasie.

Mierzalność usług (ang. measured service) oznacza:
– automatycznie kontrolowane i optymalizowane wykorzystanie zasobów,
– wykorzystywanie możliwości dozowania na pewnym poziomie abstrakcji,
– płatność za faktyczne wykorzystanie zasobów.

Zasoby mogą być monitorowane, kontrolowane i raportowane – dostarczając przejrzystości zarówno dla dostawcy jak i odbiorcy usługi. Kryteria mierzalności zasobów powinny być właściwe do typu usługi np. ilość przestrzeni dyskowej, moc obliczeniowa, pamięć, przepustowość, liczba aktywnych użytkowników.

Usługa na żądanie (ang. on-demand service) oznacza, że klient może jednostronnie skorzystać z oferowanych zasobów zgodnie ze swoimi potrzebami w sposób zautomatyzowany, bez konieczności interakcji z dostawcą

Agregacja zasobów (ang. resource pooling). Idea polega na tym, że dostawca usługi posiada różne zasoby (jednostki mocy obliczeniowej CPU, przestrzeń składowania, zasoby sieciowe itp.), zlokalizowane w jednym lub w wielu centrach danych

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

i obszarach geograficznych. Dla klienta najważniejsze jest to, aby zasoby (obliczeniowe, sieciowe, do składowania) jakie są mu potrzebne były dostępne i współdziałały ze sobą. Zatem dostawcy łączą zasoby w tzw. pule i dostarczają je klientom zgodnie z ich oczekiwaniami i wymaganiami aplikacji.

Najwięcej problemów wśród przebadanych dostawców sprawia wykazanie cech świadczących o tym, że oferowane przez nich usługi świadczone są w modelu cloud computing. Zauważa się brak błyskawicznej elastyczności i możliwości skalowania zasobów oraz mierzalności usług i płatności za faktyczne wykorzystanie. Większość usług nazwanych cloudowymi są świadczone w modelu hostingowym – płatność za określoną pulę zasobów w abonamencie miesięcznym. Dla porównania w modelu cloud computing użytkownik może dynamicznie skalować zasoby i płaci za ich faktyczne wykorzystanie.

Spośród dostawców deklarujących w swojej ofercie świadczenie usług w modelu cloud zaledwie **45%** (5) spełnia wymagania definicji.

Tematyka cloud computing jest Ci bliska?
Chcesz wymieniać się doświadczenami i wiedzieć co dzieje się na rynku?

Dołącz do nas.

Odwiedź także nasz profil na LinkedIn

biuro@bezpiecznachmura.org  beata.marek@cyberlaw.pl

Beata Marek: W jakich przypadkach dostawca jest przetwarzającym i zachodzi obowiązek podpisania umowy powierzenia przetwarzania danych osobowych?

Dr Wojciech Rafał Wiewiórowski - GIODO:

Dostawca usług chmurowych na początek powinien zastanowić się, czy jest tylko przetwarzającym, czy może staje się de facto administratorem danych osobowych.

W przypadku usług SaaS, gdzie dostawca dostarcza rozwiązanie w chmurze może tak się okazać. Trzeba bowiem pamiętać, że przetwarzanie danych osobowych to wykonywane na nich jakichkolwiek operacji, w tym takich jak ich gromadzenie.

Zatem jeśli np. tworzymy tylko kopie zapasowe materiałów zawierających dane osobowe, to zapewne jesteśmy jedynie przetwarzającym.

Nie jesteśmy w ogóle przetwarzającym tylko wtedy, gdy nie przetwarzamy danych osobowych.

BM: Co w sytuacji, gdy klient informuje dostawcę o tym, że będą przetwarzane dane osobowe? Czy dostawca może się tłumaczyć tak jak niektórzy ankietowani, że nie ma wiedzy co do zakresu przetwarzanych danych?

GIODO: Brak poinformowania ze strony klienta, brak kontrolowania tego, co znajduje się na udostępnionej klientowi powierzchni serwerowej może wyłączać odpowiedzialność dostawcy. W tym momencie jednak administrator danych będzie ponosił odpowiedzialność za to, że nie poinformował hostera o tym, że te dane przetwarza.

Celowo używam słowa „hoster", bo wyłączenia odpowiedzialności, o których mowa w ustawie o świadczeniu usług drogą elektroniczną, czyli hosting, mere conduit i cashing, odnoszą się do różnych rozwiązań. Nie tylko do klasycznego hostingu, ale i różnych rodzajów outsourcingu, w tym rozwiązań cloud computingu.

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

Mając na uwadze art. 12 – 15 tejże ustawy, dostawca nie ma obowiązku sprawdzać, jakie dane są przechowywane, ale jeżeli otrzyma od klienta informację, że są albo będą przechowywane dane osobowe, to jest już wystarczające do tego, żeby po stronie dostawcy pojawiły się obowiązki wynikające z ustawy o ochronie danych osobowych.

Oczywiście może też zdarzyć się takie rozwiązanie, że dostawcy przekazywane są materiały, które zawierają dane osobowe, ale dostawca nie ma do nich dostępu. Taka sytuacja będzie miała miejsce wtedy, gdy jesteśmy hosterem, który przechowuje dane, lecz są one zaszyfrowane. Wtedy rzeczywiście możemy powiedzieć, że jeżeli wśród tych danych, które są zaszyfrowane, znajdują się dane osobowe, a my nie mamy możliwości ich odczytania, to nie przetwarzamy danych osobowych. Dane te bowiem nie są danymi osobowymi (nie mamy klucza, nie mamy możliwości zadziałania na nie w żaden sposób).

BM: **Dla dostawcy zatem ważne jest szyfrowanie danych przez jego klientów.**

GIODO: Tak, ale pamiętajmy, że to właściwie można odnosić do IaaS, gdzie infrastruktura jest wykorzystawana do tego, by użytkownik wprowadzał własne zasoby. W takiej sytuacji można faktycznie powiedzieć, że hoster nie jest przetwarzającym dane osobowe, mimo iż wie o tym, że w zaszyfrowanym materiale znajdują się dane osobowe.

BM: **A jeżeli nie mamy takiej sytuacji, że dane są szyfrowane, tylko dostawca tłumaczy się tym, że udostępnia zasób infrastruktury, ale nie administruje, nie zarządza, fizycznie nic nie robi z tymi danymi?**

GIODO: Jestem w stanie wyobrazić sobie, choć nie jest to dla mnie łatwe, taką sytuację, w której udostępnianie zasobu będzie powodowało, że fizycznie dostarczyciel chmury nie jest w stanie do niego zajrzeć.

Jeśli byłoby tak, że faktycznie nie ma on możliwości zajrzenia do tych danych, to musimy to potraktować jako sytuację podobną do zaszyfrowania danych (przekazałem komuś miejsce, ale nie jestem w stanie zajrzeć do tego miejsca).

biuro@bezpiecznachmura.org  beata.marek@cyberlaw.pl

BM: **Dwóch dostawców tłumaczyło się właśnie w ten sposób. Co w sytuacji klienta, na którym ciążą przepisy ustawy o ochronie danych osobowych? Czy w toku kontroli GIODO przekazanie takiej informacji, że dostawca nie ma fizycznej możliwości wglądu do danych, będzie dla niego wystarczające?**

GIODO: Jakoś słabo wierzę, że to jest możliwe, ale tak jak powiedziałem, jestem to sobie w stanie wyobrazić. W takim przypadku jeżeli umowa zawarta między użytkownikiem chmury a jej dostarczycielem zawierałaby wyraźne zapisy o tym, że z jednej strony to miejsce jest udostępniane, a z drugiej, że dostarczyciel nie ma prawa tam zaglądać, nie ma także technicznej możliwości, by tego dokonać, to wówczas potraktowalibyśmy to jako sytuację, która wyłącza możliwość dostępu, co oznacza, że dostarczyciel nie byłby przetwarzającym.

Trzeba jednak pamiętać, że tu nie chodzi tylko o sytuację prawnego zabezpieczenia na zasadzie „ja naprawdę nie będę miał dostępu do danych", tylko również o to, co się stanie w sytuacji kryzysowej, np. awarii. Czy sytuacja awaryjna umożliwia dostarczycielowi chmury zajrzenie do zasobów, żeby np. coś naprawić.

Testem na to, czy rzeczywiście nie ma on możliwości zajrzenia do danych, jest sytuacja, gdy przychodzi do niego policja i twierdzi, że zostało popełnione przestępstwo i potrzebny jest dostęp do danych. Jeżeli na takie twierdzenie policji dostarczyciel chmury odpowie, ale ja nie mam możliwości dostępu do zasobów, to wówczas można go uznać za podmiot, który nie jest przetwarzającym, bo faktycznie takiego dostępu nie ma.

Dla dostawcy jest zatem ważne, by zadać sobie takie np. pytanie: „gdyby przyszło do mnie ABW, czy byłbym w stanie im dany materiał pokazać i czy ten materiał zawierałby dane osobowe?". Jeżeli materiał jest zaszyfrowany, to problemu nie ma.

BM: **Z szyfrowaniem jest pewien problem u dostawców. Osobiście mnie to dziwi, że mało dostawców szyfruje dane, choć z ich punktu widzenia i ich klientów byłoby to korzystne.**

GIODO: I tak, i nie. W IaaS jest to możliwe. W SaaS tylko teoretycznie, gdyż jedynie teoretycznie wyobrażalne jest, że zaszyfrowany materiał będzie odszyfrowywany w momencie transportowania go na zewnątrz i zaszyfrowywany w momencie, gdy ponownie trafia do dostawcy. W pozostałych przypadkach twórca rozwiązań SaaS zazwyczaj decyduje o osposobach i celach przetwarzania danych, czyli nie tylko jest przetwarzającym dane

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl

, ale nawet ich administratorem.

W przypadku IaaS w sytuacji użytkowników, którzy współdzielą serwer z innymi, czyli korzystają z fragmentów zasobu, nie są oni zainteresowani tym, żeby go zaszyfrować, cały ściągnąć do siebie i u siebie odszyfrowywać. To może się przydać gdy mówimy o kopiach zapasowych.

BM: **A co w przypadku PaaS, czyli w sytuacji, gdy dostawca udostępnia coś więcej aniżeli infrastrukturę, wręcz całe środowisko aplikacyjne dla np. programistów? Przykładowo heroku, którym zarządza amerykański dostawca. Jak w takiej sytuacji powinien zachować się programista?**

GIODO: Nie ukrywam, że PaaS jest modelem najmniej zbadanym przez rzeczników ochrony danych osobowych. Bardzo trudno jest nam wyjaśnić, czy w modelu PaaS w ogóle mogą się pojawić dane osobowe.

Wolałbym, żeby w takim środowisku były wpisywane dane testowe, które mają charakter zbliżony do danych osobowych, a nie prawdziwe dane osobowe.

BM: **Może rozwiązaniem byłoby oparcie się na rozwiązaniach technicznych jednego dostawcy, a posiadanie bazy danych na zasobach dostawcy, z którym jest podpisana umowa powierzenia?**

GIODO: Tak. Niemniej na środowisku PaaS nie skupialiśmy tak dużej uwagi, jak na IaaS i SaaS, przyjmując, że jest to środowisko developerskie i nie są tam przetwarzane dane osobowe.

BM: **Jaki obecnie poważny problem dostrzega GIODO w kontekście dostawców i odbiorców usług chmurowych?**

GIODO: Najtrudniejsze jest przesądzenie, czy mamy do czynienia z przetwarzającym, czy już z drugim administratorem danych. To jest sytuacja najtrudniejsza, a jednocześnie wydaje nam się, że najbardziej powszechna w modelach, które już są i będą stosowane.
Takim klasycznym przykładem, który można podać, jest jednoosobowy gabinet lekarski.

biuro@bezpiecznachmura.org  beata.marek@cyberlaw.pl

Jeżeli mamy przepisy mówiące o przechowywaniu danych w postaci elektronicznej, to proszę sobie wyobrazić, ilu lekarzy prowadzących samodzielnie gabinety lekarskie jest przygtowywanych do tego, by samodzielnie to robić.

BM: **Więc powstają usługi.**

GIODO: Tak. Jeżeli powstają takie usługi SaaS, czyli lekarz ma tylko przeglądarkę internetową, w którą wpisuje różnego rodzaju dane, a te dane przetwarzane są po stronie dostarczyciela usługi chmurowej czy jakiejś innej, to powstaje ptanie, jaką tak naprawdę rolę pełni ten dostawca.

W przypadku prawników i programów do obsługi kancelarii prawnych jest podobnie. Jeżeli dane składowane są na zewnętrznych serwerach, to proszę mi powiedzieć, jaką kontrolę nad tymi danymi ma prawnik? Mamy tak naprawdę dwóch administratorów. Jednym jest prawnik, drugim - dostarczyciel usługi. Dlaczego? W przypadku awarii prawnik dzwoni do serwisu i to serwisant przejmuje kontrolę nad systemem. Można wówczas patrzeć na ekran własnego komputera i widzieć, jak naszą myszkę prowadzi serwisant, wykonujący czynności niezbędne do usunięcia usterki. I on tego nie robi na komputerze prawnika w jego biurze, tylko na serwerze, który stoi w dowolnym miejscu na świecie. O ile jeszcze prawnik może upoważnić tego informatyka do wykonywania określonych czynności, to lekarz takiego prawa nie ma. On może jedynie upoważnić innego lekarza prowadzącego leczenie pacjenta. To jest problem, na który zwracają uwagę organy do spraw ochrony danych osobowych, bo tu nie wystarczy umowa powierzenia przetwarzania danych.

BM: **W przypadku SaaS.**

GIODO: W przypadku SaaS.

BM: **Nawet jeżeli określimy dokładnie zakres i cel przetwarzania danych...?**

GIODO: Możemy sobie wyobrazić, że zapisy umowy będą tak szczegółowe, że zostanie dokładnie określone, co jest wykonywane oraz dostarczyciel chmury zobowiąże sie do tego, że on niczego innego z tymi danymi nie będzie robił, poza tym co robi program.

biuro@bezpiecznachmura.org  beata.marek@cyberlaw.pl

Dobrze jeśli taką umowę zawrzemy.

Jeżeli jednak tak naprawdę o celach i sposobach przetwarzania danych decyduje ten, kto wytworzył oprogramowanie, to mamy drugiego administratora.

W umowach też należy zwrócić uwagę na prawo do jednostronnej zmiany umowy. Takiego zapisu nie powinno być.

BM: **Dziękuję za rozmowę.**

GIODO: Dziękuję.

biuro@bezpiecznachmura.org beata.marek@cyberlaw.pl