

Czerwiec 2025



Polska administracja publiczna w drodze do chmury

Raport z badania wdrożeń technologii cloud w jednostkach polskiej administracji publicznej

Autorzy:



Czerwiec 2025

Polska administracja publiczna w drodze do chmury

Raport z badania wdrożeń technologii cloud
w jednostkach polskiej administracji publicznej

Autorzy:



SPIS TREŚCI

1.	Słowo wstępne.....	3
2.	Wprowadzenie.....	6
3.	O raporcie	9
3.1.	Metodologia	10
4.	Wyniki.....	11
4.1.	Preferowane modele dostarczania usług chmurowych	13
4.2.	Udział dostawców w rynku usług cloud dla administracji publicznej	14
4.3.	Kryteria wyboru dostawcy chmury	20
4.4.	Wydatki na chmurę w administracji publicznej	27
4.5.	Plany i strategie zarządzania chmurą w sferze dostawców	31
5.	Najważniejsze wnioski	37
6.	Załączniki	40
6.1.	Załącznik 1. Lista jednostek administracji publicznej, do których skierowany został wniosek o udostępnienie informacji publicznej	40
6.2.	Okres objęty badaniem, treść wniosku o udostępnienie informacji publicznej oraz przebieg wywiadów bezpośrednich	42

01.

Słowo wstępne



MICHAŁ KANOWNIK

Prezes Związku Cyfrowa Polska

Dane są obecnie postrzegane jako jeden z najcenniejszych aktywów. To nic dziwnego, biorąc pod uwagę, w jakim stopniu współczesne organizacje – zarówno w sektorze publicznym, jak i prywatnym – polegają na nich w swoich codziennych działaniach. Z tego powodu rozwiązania chmurowe zyskują na znaczeniu we wszystkich sektorach gospodarki. Prawidłowo wdrożone, umożliwiają użytkownikom dostęp do danych, ich przechowywanie, przetwarzanie i zarządzanie nimi szybko, bezpiecznie i wygodnie. Pod względem wdrażania technologii cloud przez przedsiębiorstwa, Polska plasuje się już powyżej średniej UE i zamyka pierwszą dziesiątkę krajów członkowskich. Wciąż wyraźna jest jednak różnica w tempie wdrożeń chmurowych pomiędzy firmami zatrudniającymi powyżej 10 osób a najmniejszymi przedsiębiorstwami, a przed nami wciąż jeszcze daleko do realizacji założeń programu „Droga ku cyfrowej dekadzie”, którego cele zakładają, że do 2030 r. 75 proc. przedsiębiorstw w UE powinno korzystać z chmury, AI lub dużych zbiorów danych.

Czy polska administracja publiczna jest na dobrej drodze, by wykorzystać potencjał technologii chmurowych do optymalizacji kosztów, zwiększenia wydajności i szybszego rozwoju e-usług? Dane w chmurze przechowuje nawet 7 na 10 podmiotów administracji publicznej. Podobnie jak w przypadku przedsiębiorstw jednak, krajobraz chmurowy jest wyraźnie podzielony również wśród podmiotów administracji publicznej. Najbardziej otwarte na możliwości chmury są jednostki samorządu terytorialnego.

Co ciekawe, administracja publiczna przy wyborze dostawców kieruje się przede wszystkim tym, jakie umowy podpisywała dotychczas, co potęguje widoczne na rynku zjawisko *vendor lock-in*.

Wygląda na to, że jako kraj dojrzewamy do chmury, ale na naszej drodze nadal napotykamy przeszkody. Badanie, którego wyniki prezentujemy w niniejszym raporcie, pozwoliło nam nie tylko postawić diagnozę na temat poziomu uchmurowienia polskiej administracji publicznej, ale także zidentyfikować najważniejsze wyzwania stojące na drodze wdrażania technologii cloud w sektorze publicznym.

MICHAŁ KANOWNIK

Prezes Związku Cyfrowa Polska



MIKOŁAJ ŚNIATAŁA

Adwokat, Dyrektor Andersen Tax & Legal Matyka i Wspólnicy sp.k.



WERONIKA BARTKOWIAK-TROŚCIANKO

Radca prawny, Associate Andersen Tax & Legal Matyka i Wspólnicy sp.k.

Eksperci Andersen Tax & Legal Matyka i Wspólnicy sp.k. posiadają doświadczenie w obszarze transformacji cyfrowej i implementacji nowych technologii – w tym rozwiązań chmurowych – nabyte w ramach współpracy z sektorem prywatnym. Przekładając nasze obserwacje na sektor publiczny zauważamy, że niezbędne jest opracowanie i przestrzeganie strategii wdrożenia technologii, opartej o prawidłową identyfikację stanu obecnego stosowania chmury w administracji publicznej, a następnie odpowiedzialne i jasne określenie ram stosowania tego rozwiązania. Strategia powinna uwzględniać efektywność procesowych, modelu wdrażania, a także planu migracji i zarządzania ryzykiem stosowania rozwiązania chmurowego. Dla utrzymania bezpieczeństwa rozwiązań chmurowych niezbędne jest wdrożenie systemu bezpieczeństwa informacji zakładającego kontrolę działania – poprzez monitorowanie zasobów, wdrażanie polityk bezpieczeństwa, zarządzanie uprawnieniami i cykliczne audyty – aby zapewnić zgodność z regulacjami oraz uniknąć nieefektywnego wykorzystania zasobów. Bezpieczeństwo informacji będących w posiadaniu administracji publicznej wymaga wprowadzania technologii w sposób odpowiedzialny i planowany. W szczególności, korzystanie z usług dostawców IT zewnętrznych może wiązać się z ryzykiem uzależnienia administracji publicznej od tych podmiotów, zarówno w zakresie zapewnienia ciągłości

działania, jak i zarządzania dostępem do krytycznych danych. Tego rodzaju zależności mogą generować problemy w sytuacjach kryzysowych, a także stwarzać potencjalne zagrożenia dla ochrony danych osobowych i innych wrażliwych informacji przechowywanych przez organy publiczne. Uczestnictwo dostawców usług w procesie budowania infrastruktury publicznej jest konieczne, ale to na Państwie ciąży obowiązek zarządzanie a ryzykiem współpracy i ciężar odpowiedzialności za interes publiczny polegający na bezpieczeństwie i zachowania ciągłości przetwarzania danych.

Celem niniejszego raportu jest przedstawienie aktualnego stanu procesu wdrażania technologii chmurowych w polskiej administracji publicznej – zarówno na szczeblu centralnym, jak i lokalnym. Analiza obejmuje aspekty prawne, organizacyjne, techniczne i finansowe. Wyniki raportu zostały przedstawione i omówione przez autorów, a następnie zostały wzbogacone o komentarz ekspertów. Ponadto eksperci zostali poproszeni o zmierzenie się ze zidentyfikowanymi przez autorów raportu najważniejszymi wyzwaniami, które stoją na drodze do polskiego sukcesu przy przygotowaniu infrastruktury publicznej do nowoczesnego zarządzania zasobami informacyjnymi państwa.

Jednym z wyzwań poddanych szczegółowej analizie były kryteria wyboru dostawców przez organy administracji publicznej oraz struktura kosztów związanych z przechowywaniem danych w chmurze. Raport będzie również próbą odpowiedzi na pytanie, w jaki sposób wzmocnić kontrolę nad przechowywanymi danymi, zapewniając jednocześnie ochronę przed potencjalnymi zagrożeniami związanymi z cyberatakami i utratą niezależności technologicznej.

W części poświęconej wnioskowi z raportu autorzy położyli nacisk na wyjaśnienie zidentyfikowanych w badaniu kluczowych problemów dla adopcji chmury w sektorze publicznym. Zauważono problematykę związaną z funkcjonowaniem Wspólnej Infrastruktury Informatycznej Państwa (WIIP). Ponadto istotnym zagadnieniem w świetle udzielonych odpowiedzi w ramach wywiadu bezpośredniego jest brak realizowania przez sektor publiczny polityki Cloud First, opierającej się na założeniu, że technologie chmurowe, ze względu na ich elastyczność i skalowalność, powinny być kluczową technologią dla realizowania polskiej polityki cyfrowej.

Zapraszamy do zapoznania się z treścią raportu i podzieleniem się opinią co do wniosków z niego płynących poprzez kontakt z mikolaj.sniatala@pl.andersen.com

02.

Wprowadzenie

W obliczu dynamicznych zmian technologicznych oraz rosnących oczekiwań obywateli wobec jakości i dostępności usług publicznych, administracja publiczna w Polsce staje przed koniecznością modernizacji infrastruktury IT. Oczwistym jest, że jednym z kluczowych kierunków transformacji cyfrowej jest wdrożenie rozwiązań chmurowych, które oferują elastyczność, skalowalność oraz oszczędności. Chmura obliczeniowa stanowi odpowiedź na wyzwania związane z zapewnieniem ciągłości działania systemów, bezpieczeństwem danych oraz interoperacyjnością między różnymi instytucjami administracji. Choć technologie chmurowe oferują ogromne możliwości, to ich wdrożenia wymagają starannego planowania oraz odpowiednich kompetencji wśród pracowników jednostek administracji publicznej, aby uniknąć m.in. naruszenia zasad bezpieczeństwa danych.

Chmurą (ang. *cloud*) określa się zwyczajowo przetwarzanie danych w chmurze obliczeniowej (ang. *cloud computing*) stanowiące model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę wewnętrznego lub zewnętrznego. Według Narodowego Instytutu Norm i Technologii, chmura obliczeniowa jest modelem umożliwiającym powszechny, wygodny dostęp sieciowy na żądanie do wspólnej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowej, aplikacji i usług), które mogą być szybko dostarczone i uruchomione przy minimalnym wysiłku zarządczym lub interakcją z dostawcą usług.

Ze względu na charakter dostawcy usług chmurowych, możemy mówić o chmurach:

- prywatnych (ang. *private cloud*) – znajdujących się wewnątrz sieci danej organizacji i służących jedynie użytkownikom wewnętrznym tej organizacji;
- publicznych (ang. *public cloud*) – zapewnianych przez ogólnodostępnego dostawcę zewnętrznego;
- hybrydowych (ang. *hybrid*) – będących połączeniem zasad funkcjonowania chmury prywatnej i publicznej.

Rozróżnia się 3 główne modele świadczenia usług chmurowych:

- Oprogramowanie jako usługa (*Software as a Service, SaaS*) – umożliwia korzystanie z aplikacji z pomocą Internetu;
- Platforma jako usługa (*Platform as a Service, PaaS*) – dostarcza internetową platformę obliczeniową, na której można rozwijać, testować i wdrażać aplikacje;
- Infrastruktura jako usługa (*Infrastructure as a Service, IaaS*) – zapewnia dostęp za pomocą Internetu do zwirtualizowanych zasobów fizycznych, dzięki czemu można rozwijać oprogramowanie bez konieczności zakupu lub konserwacji własnego sprzętu.

Szeroko zakrojona implementacja rozwiązań cloud przez administrację publiczną stanowi istotny krok ku sprostaniu rosnącemu zainteresowaniu obywateli e-usługami publicznymi, ale także ku realizacji celów unijnego programu „Droga ku cyfrowej dekadzie”, wśród celów którego znalazło się udostępnienie wszystkich najważniejszych usług publicznych online do 2030 r.

Tym samym niezbędne jest opracowanie i przestrzeganie strategii wdrożenia tej technologii, opartej o prawidłową identyfikację stanu obecnego stosowania chmury w administracji publicznej oraz odpowiedzialne i jasne określenie ram stosowania tego rozwiązania. Strategia powinna

uwzględniać efektywność procesową modelu wdrażania, a także planu migracji i zarządzania ryzykiem stosowania rozwiązania chmurowego. Dla utrzymania bezpieczeństwa rozwiązań chmurowych niezbędne jest wdrożenie systemu bezpieczeństwa informacji zakładającego kontrolę działania – poprzez monitorowanie zasobów, wdrażanie polityk bezpieczeństwa, zarządzanie uprawnieniami i cykliczne audyty – aby zapewnić zgodność z regulacjami oraz uniknąć nieefektywnego wykorzystania zasobów. Bezpieczeństwo informacji będących w posiadaniu administracji publicznej wymaga wprowadzania technologii w sposób odpowiedzialny i planowany. W szczególności, korzystanie z usług dostawców IT zewnętrznych może wiązać się z ryzykiem uzależnienia administracji publicznej od tych podmiotów, zarówno w zakresie zapewnienia ciągłości działania, jak i zarządzania dostępem do krytycznych danych. Tego rodzaju zależności mogą generować problemy w sytuacjach kryzysowych, a także stwarzać potencjalne zagrożenia dla ochrony danych osobowych i innych wrażliwych informacji przechowywanych przez organy publiczne. Uczestnictwo dostawców usług w procesie budowania infrastruktury publicznej jest konieczne, ale to na Państwie ciąży obowiązek zarządzania ryzykiem współpracy i ciężar odpowiedzialności za interes publiczny polegający na bezpieczeństwie i zachowaniu ciągłości przetwarzania danych.

03.

O raporcie

Celem niniejszego raportu jest analiza korzystania z technologii chmury obliczeniowej przez jednostki polskiej administracji publicznej, ze szczególnym uwzględnieniem identyfikacji dostawców usługi, jej kosztów, kryteriów wyboru dostawców oraz planów i strategii rozwoju technologii. Przedstawiamy poniżej aktualny stan procesu wdrażania technologii chmurowych w polskiej administracji publicznej – zarówno na szczeblu centralnym, jak i lokalnym. Analiza obejmuje aspekty prawne, organizacyjne, techniczne i finansowe. W raporcie przyglądamy się także najważniejszym wyzwaniom, które stoją na drodze do polskiego sukcesu przy przygotowaniu infrastruktury publicznej do nowoczesnego zarządzania zasobami informacyjnymi państwa.

Szczegółowej analizie poddaliśmy kryteria wyboru dostawców przez organy administracji publicznej oraz struktury kosztów związanych z przechowywaniem danych w chmurze. Ponadto w raporcie podejmujemy próbę odpowiedzi na pytanie, w jaki sposób wzmocnić kontrolę nad przechowywanymi danymi, zapewniając jednocześnie ochronę przed potencjalnymi zagrożeniami związanymi z cyberatakiem i utratą niezależności technologicznej, przyglądamy się problematyce związanej z funkcjonowaniem Wspólnej Infrastruktury Informatycznej Państwa (WIIP) oraz trudnościom w realizowaniu przez sektor publiczny polityki Cloud First, opierającej się na założeniu, że technologie chmurowe, ze względu na ich elastyczność i skalowalność, powinny być kluczową technologią dla realizowania polskiej polityki cyfrowej.



MAGDALENA DZIEWGUĆ,

Country Director,
Google Cloud Poland

OKIEM EKSPERTA

Chmura to nie tylko techniczna możliwość przechowywania danych, ale również brama do zaawansowanych usług analitycznych, sztucznej inteligencji oraz zaawansowanych narzędzi cyberbezpieczeństwa. Bez szybkiego dostosowania realiów i przepisów prawa do wdrażania chmury ryzykujemy wolniejszy rozwój nowoczesnych usług publicznych dla obywateli.

Obserwujemy, że transformacja cyfrowa w sektorze publicznym, choć postępuje, często opiera się na punktowych wdrożeniach usług chmurowych. Te indywidualne inicjatywy, choć wartościowe, bywają realizowane bez szerszego, zintegrowanego planowania. W rezultacie brakuje nam kompleksowego rejestru kosztów oraz szczegółowych analiz efektywności tych rozwiązań, co utrudnia pełną ocenę ich wpływu.

3.1. Metodologia

Odpowiedzi na pytania dotyczące m.in. typu danych przechowywanych w chmurze, preferowanych przez administrację dostawców, czynników wpływających na ich wybór oraz kosztów korzystania z usług chmurowych zebrane zostały od 82 jednostek administracji publicznej w okresie od stycznia do maja 2025 r. Szczegółowa lista pytań skierowanych do jednostek administracji publicznej na potrzeby badania oraz lista podmiotów, do których zwrócono się z wnioskiem o udzielenie na nie odpowiedzi znajdują się w Załączniku do raportu (str. 40).

04.

Wyniki

Dane w chmurze przechowuje ponad 70 proc. jednostek administracji publicznej w Polsce. Zadeklarowało to 59 z badanych 82 podmiotów. To odsetek wyższy niż w przypadku polskich firm zatrudniających powyżej dziewięciu osób, spośród których niespełna połowa korzysta z chmury. Co ciekawe, praktyka ta nie jest równie powszechna we wszystkich gałęziach administracji.

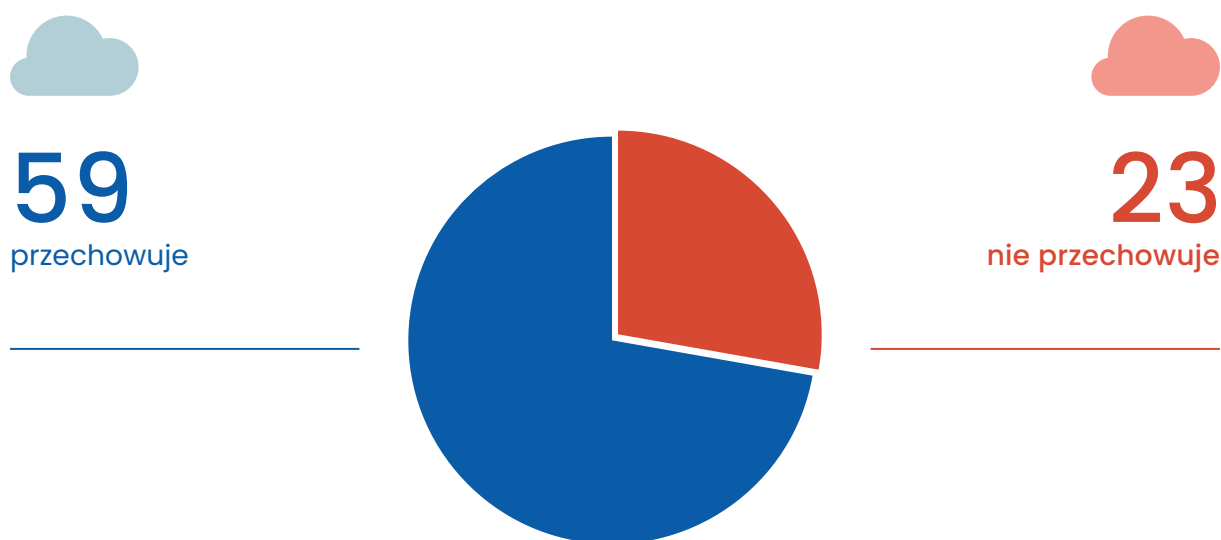
Dane w chmurze przechowuje:

- **71 proc. ministerstw (5 z 7 badanych)**
- **67 proc. centralnych organów administracji rządowej (4 z 6 badanych)**
- **1 z 12 badanych jednostek administracji terenowej rządowej zespolonej**
- **Niemal wszystkie (22 z 23 badanych) jednostki administracji terenowej rządowej niezespolonej**
- **79 proc. jednostek samorządu terytorialnego (27 z 34 badanych)**

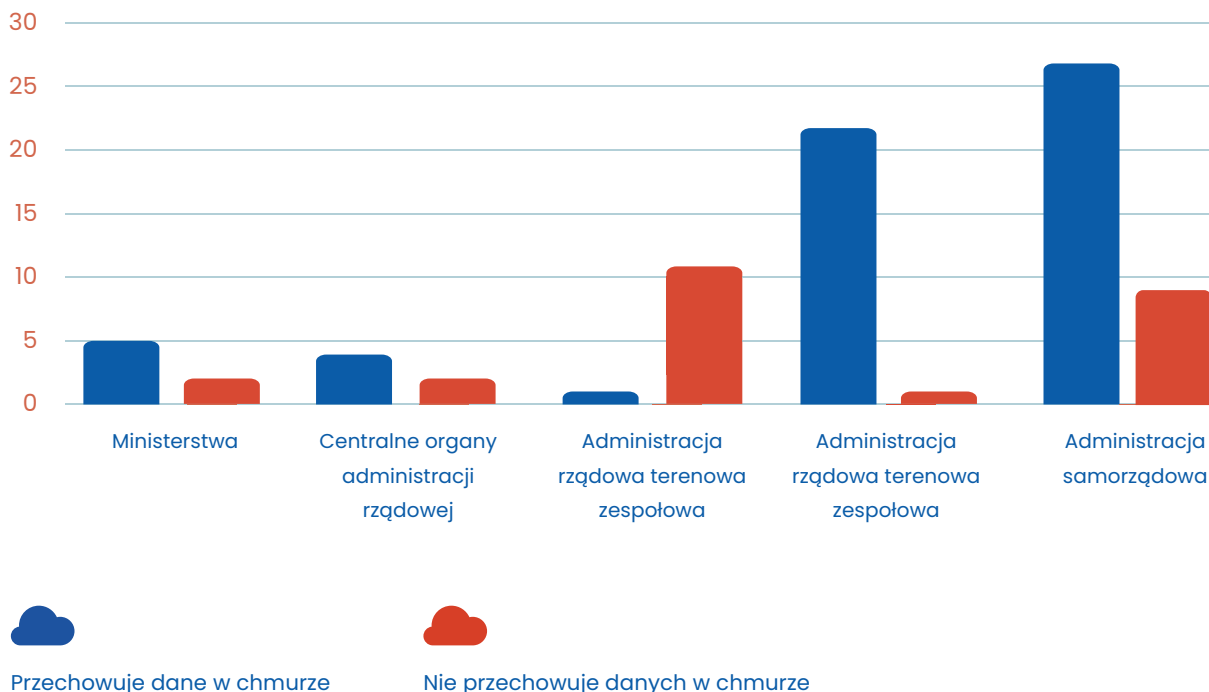
Choć większość jednostek potwierdziło korzystanie z chmury obliczeniowej, nadal istotna grupa – 23 jednostki – pozostaje przy tradycyjnych modelach przechowywania danych. **Warto zauważyć, że największą otwartość na technologie chmurowe wykazują jednostki samorządu terytorialnego**, podczas gdy administracja rządowa na szczeblu centralnym wykazuje większą ostrożność w tym zakresie.

Wśród 23 jednostek administracji publicznej, które nie przechowują danych w chmurze obliczeniowej, znalazły się 2 ministerstwa, 2 centralne organy administracji rządowej, 11 jednostek administracji terenowej rządowej zespolonej, 1 jednostka administracji terenowej rządowej niezespolonej i 7 jednostek samorządu terytorialnego. Należy zaznaczyć, że Ministerstwo Spraw Wewnętrznych i Administracji odpowiedziało, że nie korzysta i nie planuje korzystać z usług żadnego dostawcy rozwiązań chmurowych, preferując wewnętrzne rozwiązania, co nie wyklucza możliwości, że korzystają z chmury obliczeniowej, ale we własnych zasobach.

Przechowywanie danych w chmurze przez jednostki sektora publicznego w liczbach



Przechowywanie danych w chmurze obliczeniowej przez organy administracji publicznej

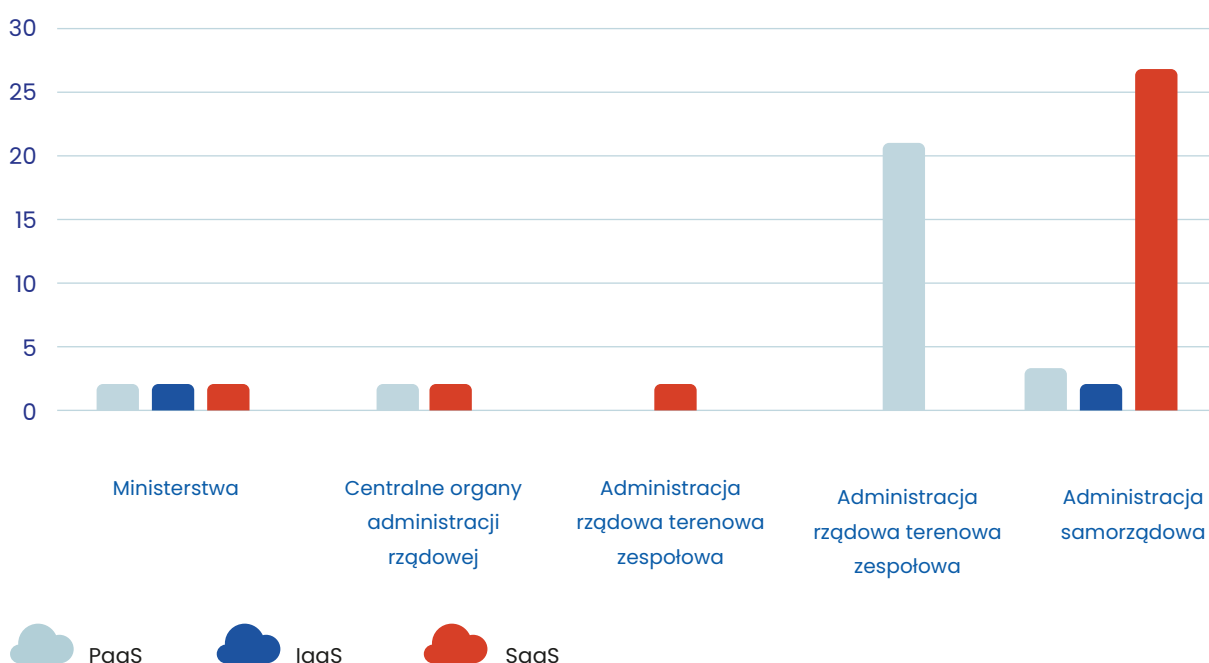


4.1. Preferowane modele dostarczania usług chmurowych

Zróżnicowanym zainteresowaniem administracji publicznej cieszą się poszczególne modele dostarczania usług chmurowych (patrz Ramka 1 na str. 20). Najczęściej wybieranym modelem okazuje się SaaS (*Software as a Service*, *Oprogramowanie jako usługa*), z którego korzysta ponad połowa (32 na 59) jednostek przechowujących dane w chmurze (w tym: 2 ministerstwa, 2 centralne organy administracji rządowej, 1 jednostka administracji terenowej rządowej zespolonej i 27 jednostek samorządu terytorialnego). Wysoką popularnością wśród administracji publicznej cieszy się również model PaaS (*Platforma jako usługa*, *Platform as a Service*), z którego korzysta ok. 44 proc. badanych podmiotów (2 ministerstwa, 2 centralne organy administracji rządowej, 21 jednostek administracji terenowej rządowej niezespolonej, 3 jednostki samorządu terytorialnego). Zaledwie cztery podmioty (2 ministerstwa i 2 JST) deklarują natomiast korzystanie z modelu IaaS (*Infrastruktura jako usługa*, *Infrastructure as a Service*).

Warto zauważyć, że część podmiotów korzysta jednocześnie z więcej niż jednego modelu dostarczania technologii cloud. Szczególnym przykładem jest Urząd Miasta Stołecznego Warszawy, korzystający hybrydowo ze wszystkich 3 modeli usług chmurowych: w zakresie rozwiązań Paas – Azure, Oracle Cloud Infrastructure oraz Amazon Web Services, a w zakresie rozwiązań SaaS – Office365. Urząd rozwija poza tym chmurę prywatną (Miejska Chmura Obliczeniowa – MChO) w modelu IaaS.

Modele przechowywania danych w chmurze obliczeniowej przez organy administracji publicznej



4.2. Udział dostawców w rynku usług cloud dla administracji publicznej

Przyglądając się udziałowi poszczególnych dostawców na rynku usług cloud dla administracji publicznej, łatwo zauważyć dominującą rolę jednego z nich. Aż 46 (78 proc.) jednostek administracji publicznej przechowujących dane w chmurze obliczeniowej korzysta z usług Microsoft. Wynik ten uwzględnia udostępnienie chmury w ramach różnych oferowanych usług zarówno w modelu PaaS, jak i SaaS w ramach pakietu Office 365.

Z usług innych dostawców – o znacznie mniejszym udziale w rynku chmury dla administracji publicznej – korzystają 23 jednostki (1 ministerstwo, 2 centralne organy administracji publicznej oraz 20 organów administracji samorządowej).

Zaledwie jedna jednostka administracji publicznej tj. Ministerstwo Rozwoju i Technologii przechowuje dane w Rządowej Chmurze Obliczeniowej. Robi to na potrzeby utrzymania systemu Export Intelligence.



MATEUSZ JAKUBIK

Compliance Officer w Bonnier Business Polska, wykładowca, Członek Zarządu SABI – Stowarzyszenia Inspektorów Ochrony Danych

OKIEM EKSPERTA

Obecny poziom przygotowania sektora publicznego należy ocenić jako niewystarczający. Administracja działa bez ogólnokrajowej strategii wdrożeń chmurowych. Jednostki często nie dysponują politykami bezpieczeństwa, nie przeprowadzają audytów, nie zarządzają uprawnieniami w sposób cykliczny, co stwarza ryzyka dla danych osobowych i informacji niejawnych.

Brakuje też dostatecznego nadzoru centralnego nad strukturą rynku usług chmurowych dla administracji. Większość jednostek korzysta z rozwiązań jednego globalnego dostawcy, nie analizując innych opcji. Taki model prowadzi do ryzyk technologicznych, operacyjnych i strategicznych – np. w razie awarii lub zmian warunków handlowych przez dostawcę.



ALEKSANDER WOJDYŁA

CISSP, audytor bezpieczeństwa informacji, niezależny ekspert ds. cyberbezpieczeństwa

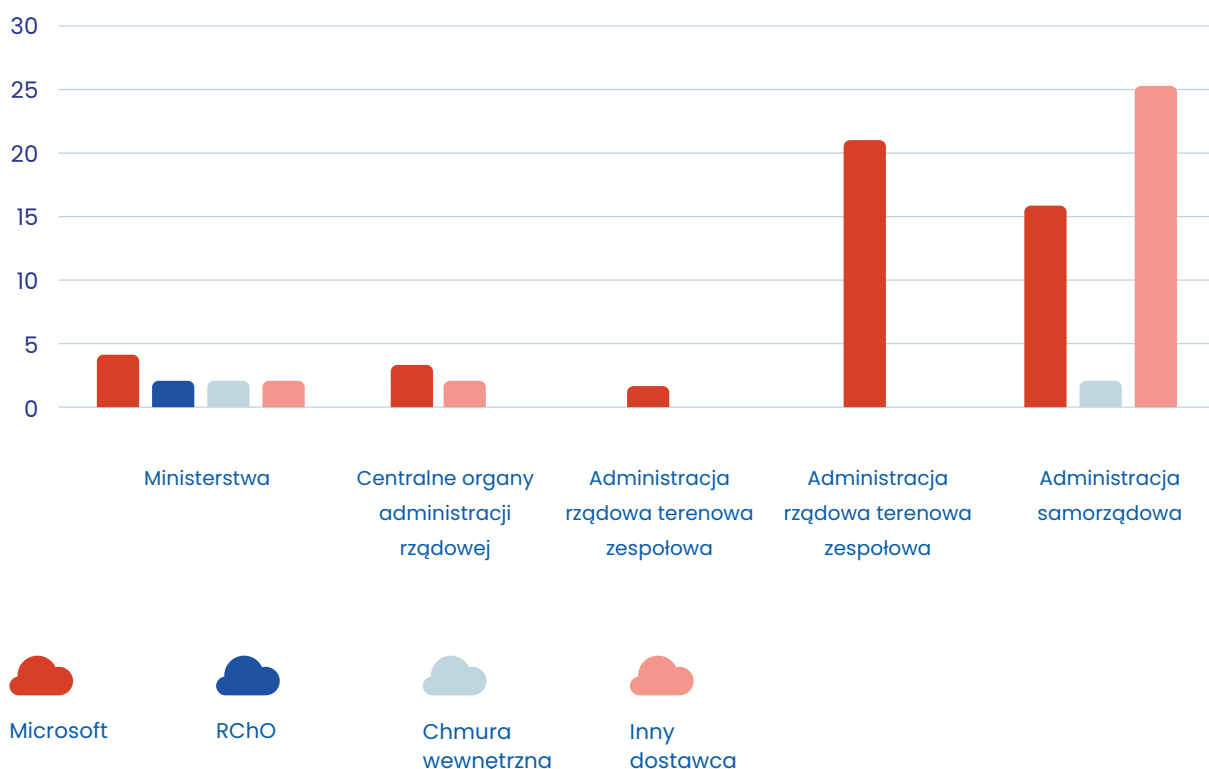
OKIEM EKSPERTA

Poziom przygotowania sektora publicznego w zakresie funkcjonowania usług chmurowych oceniam jako niewystarczający – zwłaszcza w kontekście nadchodzących obowiązków wynikających z aktów takich jak NIS2. Brakuje ujednoliconych polityk zarządzania ryzykiem dostawców (*third-party risk*), mechanizmów oceny zgodności usług z wymaganiami sektorowymi oraz operacyjnych standardów dla wdrażania usług chmurowych. Ryzyko systemowe może wynikać nie tylko z niewłaściwej konfiguracji usług, ale też z braku mechanizmów wymuszenia zgodności na etapie projektowania (*security by design*).

Wykorzystywanie „chmury wewnętrznej” deklarują trzy jednostki administracji publicznej. Są to Ministerstwo Spraw Wewnętrznych i Administracji, które „preferuje własne wewnętrzne rozwiązania”, Urząd Miasta Zielona Góra, który, poza korzystaniem z rozwiązań Microsoft, testuje korzystanie z chmury wewnętrznej oferowanej przez Lubuskie Centrum Cyfryzacji Go Cloud sp. z o.o. oraz Urząd Miasta Stołecznego Warszawy, wykorzystujący Miejską Chmurę Obliczeniową (MChO).

Choć niektóre jednostki korzystają z rozwiązań więcej niż jednego dostawcy, to nie ulega wątpliwości, że głównym dostawcą, z którego usług chmurowych korzysta większość organów administracji publicznej jest Microsoft. Na uwagę zasługuje również brak deklarowanego zainteresowania Rządową Chmurą Obliczeniową oraz ZUCH. Obserwację rażąco niskiej popularności tych dostawców potwierdza także Najwyższa Izba Kontroli, która w wystąpieniu pokontrolnym z dnia 16 marca 2025 r. wskazała, że w latach 2020–2022 w bazie ZUCH, było zaledwie 9 podmiotów, które podjęły aktywność w systemie.

Udział w rynku poszczególnych dostawców chmury obliczeniowej dla administracji





MARCIN WYSOCKI

zastępca dyrektora
Departamentu
Cyberbezpieczeństwa,
Ministerstwo Cyfryzacji

OKIEM EKSPERTA

Administracja publiczna powinna rozwijać swoje usługi dla obywateli, czyniąc je jak najbardziej dostępnymi, wygodnymi i niezawodnymi. Chmura obliczeniowa jest sposobem na realizację tego założenia. Jednocześnie przyczynia się do obniżenia kosztów, odciążenia kadr i wzmocnienia bezpieczeństwa. Obecny sposób finansowania Rządowej Chmury Obliczeniowej nie pozwala na to, żeby była jedyną opcją dla podmiotów administracji z uwagi na niewystarczające środki, które wstrzymują rozwój RChO i przyłączanie do niej usług. Nie każdy rodzaj danych wymaga również bezwzględnego korzystania z RChO, a coraz więcej dostawców komercyjnych wprowadza do swojego katalogu usług ofertę skierowaną konkretnie do administracji, która gwarantuje wysoki poziom bezpieczeństwa i suwerenności danych. Natomiast, tak jak w każdej innej dziedzinie, nie należy dążyć do monopolizmu danego dostawcy na rynku. Dla zapewnienia konkurencyjności usług – zarówno w rozumieniu oferty, wsparcia i finansów – niezbędne jest, aby dywersyfikować dostawców zewnętrznych. Konkurencyjny rynek, oferujący zróżnicowane produkty i usługi jest istotną wartością także w aspekcie jakości i innowacyjności. Jednocześnie należy mieć na uwadze, że praktyki, które mogłyby ograniczać konkurencję, mogą być przedmiotem działań Prezesa UOKiK.

W przypadku usług chmurowych niezbędne jest zagwarantowanie, że nie dojdzie do zjawiska *vendor lock-in*, czyli uzależnienia się od jednego dostawcy. Powinny gwarantować to zarówno umowy z dostawcą jak i procedura migracyjna oraz plan wyjścia. Jednocześnie podkreślić należy, że nie oznacza to, że podmioty administracji powinny bez żadnego powodu zmieniać dostawcę tylko i wyłącznie z tego względu, że korzystają z jego usług już od dłuższego czasu. Istotnym jest, by dostawca spełniał wymagania określone w uchwale WIIP i SCCO oraz umowie zawartej pomiędzy podmiotem administracji a tym dostawcą. W szczególności kluczowe jest, by warunki umowne, określające prawa i obowiązki obu stron umowy, obejmowały procedurę migracji i wyjścia z chmury.

MARCIN WYSOCKI

Odnosząc się do kwestii monopolizacji rynku, należy z całą mocą podkreślić, że nie jest to zjawisko pozytywne, ponieważ im większa konkurencja na rynku, im większy udział różnych przedsiębiorstw, tym lepsza jest sytuacja podmiotu, nie tylko w aspekcie finansowym, ale też jakości i innowacyjności oferowanych usług.



MAGDALENA DZIEWGUĆ

Country Director,
Google Cloud Poland

OKIEM EKSPERTA

Zarówno Rządowa Chmura Obliczeniowa (RChO), jak i Zintegrowana Usługa Chmurowa (ZUCH), to stosunkowo nowe inicjatywy mające na celu wspieranie transformacji cyfrowej w polskiej administracji. Na obecnym etapie ich praktyczne znaczenie może wydawać się ograniczone, a szeroka adopcja jeszcze przed nami. Wyzwania, z którymi mierzą się te projekty, obejmują zapewnienie większej elastyczności oraz efektywniejszej komunikacji korzyści, co jest kluczowe do zachęcenia kolejnych jednostek do ich wykorzystania. Dodatkowo, pełne wdrożenie i integracja z RChO czy ZUCH często wymaga odpowiedniego przygotowania technicznego po stronie beneficjentów, a to z kolei proces, który wymaga czasu i inwestycji.

Niemal żadna z jednostek administracji publicznej nie planuje zbadać możliwości wykorzystania innych dostawców chmurowych, ani zmienić dostawców cloud dla starszych typów oprogramowania (*legacy software*). Tylko jeden podmiot deklaruje, że rozważa takie działania w przyszłości ze względu na czynniki takie jak oszczędności kosztów, obawy o suwerenność, zwiększona elastyczność czy obawy o uzależnienie od dostawcy.

Dane wskazują na powszechny wśród jednostek administracji publicznej brak planów i długofalowych strategii poszukiwania nowych rozwiązań chmurowych od nowych dostawców. Bez wątpienia będzie miało to wpływ na utrzymanie się zidentyfikowanego zjawiska *vendor lock-in* w tym segmencie rynku. Należy jednak wskazać, że wiele z badanych jednostek odmówiło odpowiedzi na pytania dotyczące planów i zamierzeń, argumentując, że nie dotyczą one sfery czystych faktów, a zatem nie stanowią informacji publicznej.

MAGDALENA DZIEWGUĆ

Warto podkreślić również, że żadna z jednostek, które nie korzystają obecnie z chmury, a które udzieliły odpowiedzi na pytanie dotyczące strategii, nie planuje zbadać możliwości korzystania z usług dostawców chmurowych.

Obecnie wciąż brakuje spójnej polityki Cloud First, która mogłaby znacząco przyspieszyć proces cyfryzacji. Zadanie określone w uchwale o Wspólnej Infrastrukturze Informacyjnej Państwa (WIIP), dotyczące zapewnienia podmiotom administracji publicznej możliwości nabywania usług przetwarzania w publicznych chmurach obliczeniowych, wciąż pozostaje niezrealizowane, między innymi z uwagi na brak efektywnego mechanizmu zakupowego. Docelowo, funkcjonująca już platforma ZUCH powinna pełnić rolę centralnej platformy zakupowej, która umożliwi nabywanie komercyjnych usług chmurowych. Co więcej, kluczowe jest, aby to działanie było ściśle powiązane z aktywną, centralnie zaprojektowaną kampanią edukacyjną oraz wymiernymi zachętami dla organów administracji publicznej i samorządowej. Celem jest dywersyfikacja dostępnych metod przechowywania i przetwarzania danych, w tym wprowadzenie postulowanej rekomendacji Cloud First, wzorem doświadczeń Wielkiej Brytanii.

Biorąc pod uwagę, że są to inicjatywy stosunkowo młode, zbyt wcześnie na jednoznaczne oceny ich długofalowego sukcesu. Potrzeba więcej czasu, aby w pełni ocenić ich efektywność i wpływ na cyfryzację polskiej administracji.

Inni wiodący dostawcy chmury dla administracji publicznej

Wiodące podmioty wśród innych dostawców rozwiązań cloud (głównie w modelu SaaS) to przede wszystkim:

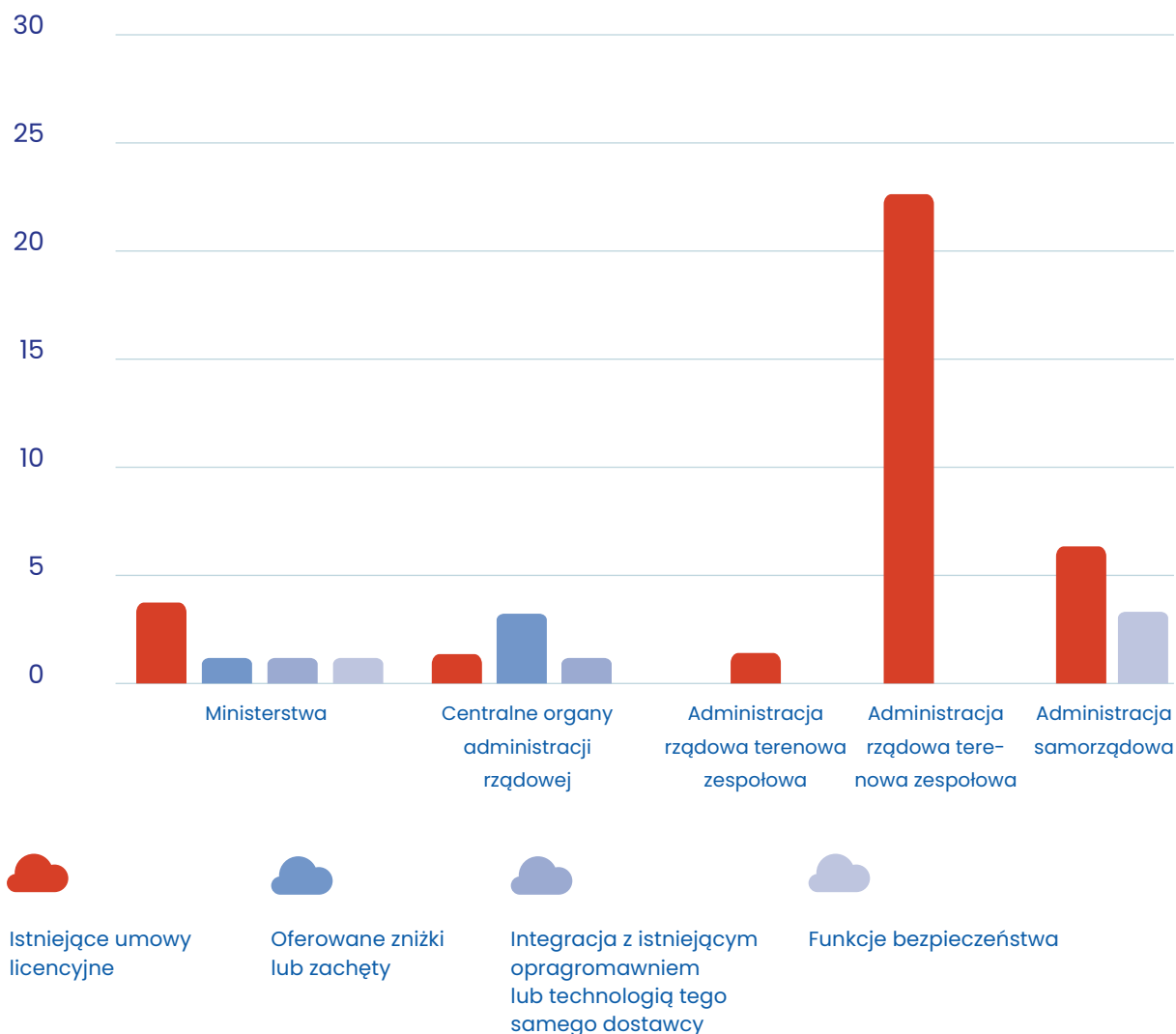
- Instytut Chemii Bioorganicznej PAN Poznańskie Centrum Superkomputerowo-Sieciowe (3 jednostki zawarły umowę)
- KrakFin Spółka Cywilna Jan Filas Barbara Cieślik Marek Sujdak (3 jednostki zawarły umowę)
- COIG S. A. (2 jednostki zawarły umowę)
- Vulcan sp. z o.o. (2 jednostki zawarły umowę)
- Oracle Cloud Service (2 jednostki zawarły umowę)

4.3. Kryteria wyboru dostawcy chmury

Warto się zastanowić, według jakich kryteriów administracja publiczna podejmuje decyzje o wyborze dostawcy usług chmurowych. **Okazuje się, że kluczowym czynnikiem wyboru dostawcy usług cloud są istniejące umowy licencyjne. Jako najważniejsze kryterium ocenia je aż 33 podmioty (ponad połowa korzystających z chmury).**

Kolejnymi najczęściej branymi pod uwagę jako główne kryteriami wyboru dostawcy są oferowane zniżki lub zachęty (te jako najważniejsze wskazuje 10 proc. jednostek administracji publicznej) oraz względy bezpieczeństwa (stawiane na pierwszym miejscu przez 4 z 59 podmiotów). Dwie jednostki administracji publicznej wskazały jako główny czynnik wyboru dostawcy kwestię integracji z istniejącym oprogramowaniem lub technologią tego samego dostawcy.

Główny czynnik wyboru dostawcy usług w zakresie chmury obliczeniowej przez jednostki sektora publicznego



Wskazane przez administrację publiczną najważniejsze czynniki decydujące o wyborze dostawcy chmury są spójne z opisanymi wyżej obserwacjami dotyczącymi udziału dostawców w rynku cloud dla jednostek administracji. Dane sugerują m.in., że oferowane zniżki i promocje mają nieznaczną wagę przy podejmowaniu decyzji o wyborze dostawcy cloud w skali kraju. Powyższa sytuacja może być rozważana w kontekście funkcjonowania dominacji jednego podmiotu na rynku oraz występowania zjawiska uzależnienia sektora publicznego od tego dostawcy poprzez istniejące umowy licencyjne (tzw. *vendor lock-in*).

Na szczególną uwagę zasługuje również to, jak mały odsetek (niepełna 7 proc.) jednostek sektora publicznego stawia na pierwszym miejscu względy bezpieczeństwa, mimo stale rosnącej liczby ataków cyfrowych na administrację publiczną w kraju.



ALEKSANDER WOJDYŁA

CISSP, audytor bezpieczeństwa informacji, niezależny ekspert ds. cyberbezpieczeństwa

OKIEM EKSPERTA

Monopolizacja nie tylko ogranicza konkurencję, ale stwarza też poważne ryzyko braku zdolności do migracji danych i aplikacji – szczególnie tam, gdzie brakuje odpowiednio zaprojektowanego planu wyjścia (*exit plan*) lub kontraktowych zabezpieczeń dotyczących interoperacyjności. Zjawisko *vendor lock-in* nie wynika tylko z umów, ale również z architektonicznych decyzji po stronie jednostek publicznych, które wybierają zamknięte technologie. W praktyce brak kompatybilnych interfejsów (API) i niedostateczna dokumentacja migracyjna uniemożliwia swobodne przenoszenie usług między środowiskami.



RAFAŁ PRABUCKI

dr inż., WPiA UŚ, adiunkt

OKIEM EKSPERTA

Aktualny poziom przygotowania sektora publicznego w zakresie funkcjonowania usług chmurowych powoduje ryzyko lub zagrożenia, i to znaczne. W obecnej formie sektor publiczny naraża się na długofalowe ryzyko braku suwerenności technologicznej, niekontrolowanego wzrostu kosztów, słabego zabezpieczenia danych oraz niemożności szybkiego reagowania na zmiany regulacyjne lub incydenty cyberbezpieczeństwa. Pasywność prawna może prowadzić do sytuacji, w której jednostka nie będzie zdolna do szybkiego reagowania w przypadku kontroli lub incydentu. Przejawia się ona brakiem reakcji na pytania dot. planów i strategii, wskazuje na brak formalizacji obowiązków w zakresie zgodności prawnej usług chmurowych, bra-

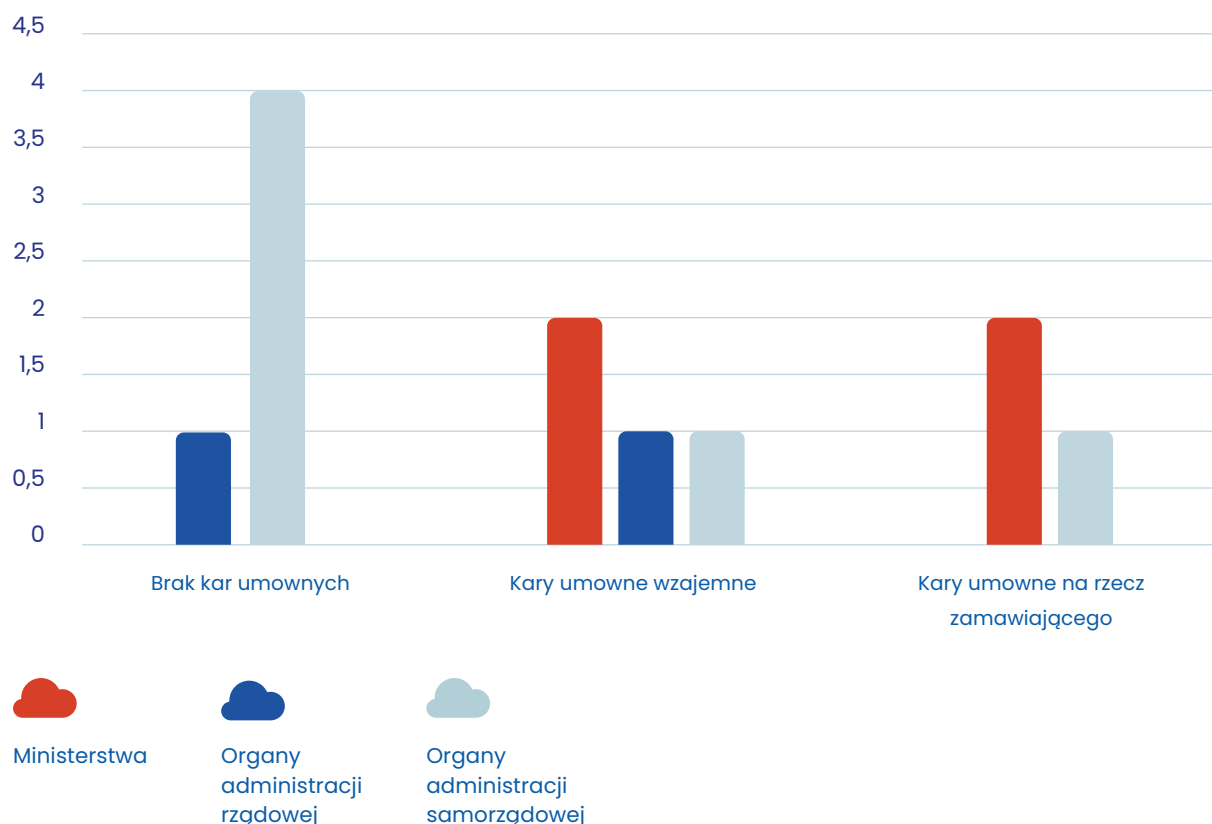
kuje ustandaryzowanych wzorów umów, zawierających klauzule o kontroli lokalizacji danych, audytach, przenoszalności czy wyjściu z umowy. Jednostki raczej nie analizują aktywnie ryzyka naruszeń RODO, NIS2 czy innych przepisów sektorowych.

Ponadto tylko nieliczne jednostki wskazują bezpieczeństwo jako kluczowy czynnik wyboru dostawcy. Większość jednostek nie potrafi wskazać szczegółowych mechanizmów kontroli kosztów ani SLA. Tylko pojedyncze umowy zawierają kary umowne za utratę danych lub niedostępność usług, co oznacza słabą ochronę interesu publicznego. Przypadki jak Warszawa czy Katowice pokazują dobre praktyki, ale są to wyjątki, nie reguła.

Wiedząc, na jakie modele usług chmurowych, od jakich dostawców i z jakich względów decydują się jednostki administracji publicznej, warto przyrzeć się następnie konstrukcji zawieranych przez nie umów. Jednym z elementów tych umów są zapisy dotyczące kar umownych. Istnienie zapisów o karach za zmianę dostawcy usług chmurowych bądź równoległe zawarcie umowy z innym dostawcą (klauzule wyłączności) mogą stanowić istotny czynnik wpływający na sytuację obserwowaną na rynku cloud dla administracji.

Odpowiedzi na ten temat udzieliło 12 podmiotów (4 ministerstwa, 1 organ centralnej administracji rządowej, 1 organ administracji terenowej rządowej zespolonej i 6 organów administracji samorządowej). Blisko połowa z tych jednostek (5 z 12) nie stosuje kar umownych w swoich umowach. Wśród podmiotów stosujących je, trzy jednostki posługują się zapisami mówiącymi o wzajemnych karach umownych. W przypadku umów zawartych przez cztery jednostki kary umowne zastrzeżone są na rzecz zamawiającego.

Stosowanie kar umownych z dostawcami usług chmurowych



Jako podstawę do naliczania kar w umowach z dostawcami usług chmurowych jeden podmiot wymienił rozwiązanie umowy przez którąkolwiek ze stron. Również tylko jedna jednostka dysponuje w swojej umowie zapisem o karze za nienależyte świadczenie usług chmurowych (w tym utratę danych bądź ponadnormatywny brak dostępności do usług chmurowych). Zapisy o karach za odstąpienie od umowy lub wypowiedzenie umowy przez wykonawcę i zwłokę w wykonaniu przedmiotu umowy przez wykonawcę posiada w swoich umowach sześć z podmiotów, które udzieliły odpowiedzi na pytanie na ten temat.

Żaden z organów udzielających odpowiedzi nie wskazał jednak, by umowy na dostawę usług chmurowych przewidywały kary umowne za zmianę dostawcy usług chmurowych bądź równoległe zawarcie umowy na dostawę usług chmurowych z innym dostawcą. Spośród przedstawionych odpowiedzi szczególną uwagę zwraca informacja przedstawiona przez Urząd Miasta Poznania o przewidywaniu kar za utratę danych bądź brak dostępności do usług przez dłuższy czas, co świadczyć może o zrozumieniu funkcji zawieranej umowy na etapie jej negocjowania.



MARCIN WYSOCKI

zastępca dyrektora
Departamentu
Cyberbezpieczeństwa,
Ministerstwo Cyfryzacji

OKIEM EKSPERTA

Rządowa Chmura Obliczeniowa oraz System ZUCH stanowią istotny wkład w rozwój cyfrowy administracji. Największym problemem, z którym związana jest również niska popularność wskazanych rozwiązań, jest nieefektywny sposób finansowania wynikający z uchwały WIIP. Finansowanie RChO i ZUCH odbywa się bowiem na zasadzie rezerwy celowej, a zapotrzebowanie administracji na usługi w RChO przekracza wartość rezerwy celowej. Podobne zmiany w funkcjonalności systemu ZUCH wymagają dużych nakładów finansowych, których nie sposób pokryć w ramach rezerwy celowej. Jednocześnie istotnym aspektem braku popularności usług chmurowych jest niska świadomość podmiotów administracji w tym zakresie. Należy także zwrócić uwagę na stosunkowo krótki okres funkcjonowania tych usług i jeszcze krótszy okres od kiedy nastąpiła nowelizacja uchwały, która w pewnym stopniu poszerzyła dostęp do chmury przez podmioty sektor publiczny. Takie procesy nie następują z dnia na dzień i często wymagają czasu, choćby z uwagi na procedury i regulacje, ale też takie czynniki jak choćby uzgadnianie umów.



RAFAŁ PRABUCKI

dr inż., WPiA UŚ, adiunkt

OKIEM EKSPERTA

Tylko nieliczne jednostki zawierają umowy z karami za brak dostępności lub utratę danych. Brakuje również analiz dotyczących konsekwencji rozwiązania umowy lub zmiany dostawcy. Wskazuje to na niski poziom świadomości prawnej i kontraktowej w zakresie usług chmurowych.



MATEUSZ JAKUBIK

Compliance Officer w Bonnier
Business Polska, wykładowca,
Członek Zarządu SABI –
Stowarzyszenia Inspektorów
Ochrony Danych

OKIEM EKSPERTA

Analiza wykazała wyraźne uzależnienie administracji publicznej od jednego dostawcy (Microsoft), co tworzy zjawisko *vendor lock-in*. Istniejące umowy licencyjne często stanowią główny czynnik wyboru dostawcy – przed względami bezpieczeństwa czy kosztowymi. Zjawisko to ogranicza konkurencję, utrudnia elastyczne planowanie i może prowadzić do nieuzasadnionego wzrostu kosztów w przyszłości.

Brakuje mechanizmów standaryzujących umowy, procedur migracji między dostawcami oraz wymogów zapewniających możliwość interoperacyjności lub działania w modelu *multicloud*. Ograniczona liczba umów zawiera jakiegokolwiek kary umowne zabezpieczające interes publiczny w przypadku niewywiązywania się z usług lub wystąpienia incydentu.

Opowiadam się za modelem dywersyfikacji dostawców i wdrożeniem elementów polityki *multicloud*. Państwo powinno równolegle rozwijać Rządową Chmurę Obliczeniową jako gwaranta bezpieczeństwa dla wybranych krytycznych usług i danych, jednak nie powinno dążyć do stworzenia monopolu (publicznego lub prywatnego).



MAGDALENA DZIEWGUĆ

Country Director,
Google Cloud Poland

OKIEM EKSPERTA

Dodatkowym wyzwaniem są długoterminowe warunki umowne z dostawcami chmury lub oprogramowania biurowego. Zobowiązania te, wiążące wiele podmiotów na lata, mogą ograniczać elastyczność administracji w zakresie szybkiej zmiany dostawców, adaptacji do nowych technologii czy optymalizacji kosztów. Ostatnie dyskusje w Komisji Europejskiej jasno pokazują rosnące obawy dotyczące zależności od części wieloletnich dostawców oprogramowania biurowego i chmurowego. Wskazuje się, że może to prowadzić do naruszeń unijnych przepisów o ochronie danych, a także budzić poważne pytania o bezpieczeństwo i prywatność wrażliwych informacji.

MAGDALENA DZIEWGUĆ

Europejski Inspektor Ochrony Danych (EDPS) już wcześniej zalecił Komisji dostosowanie praktyk korzystania z tych produktów i szerszą dywersyfikację źródeł. Brak znaczących postępów w tym obszarze podkreśla skalę i złożoność tego wyzwania, z którym mierzą się instytucje unijne.

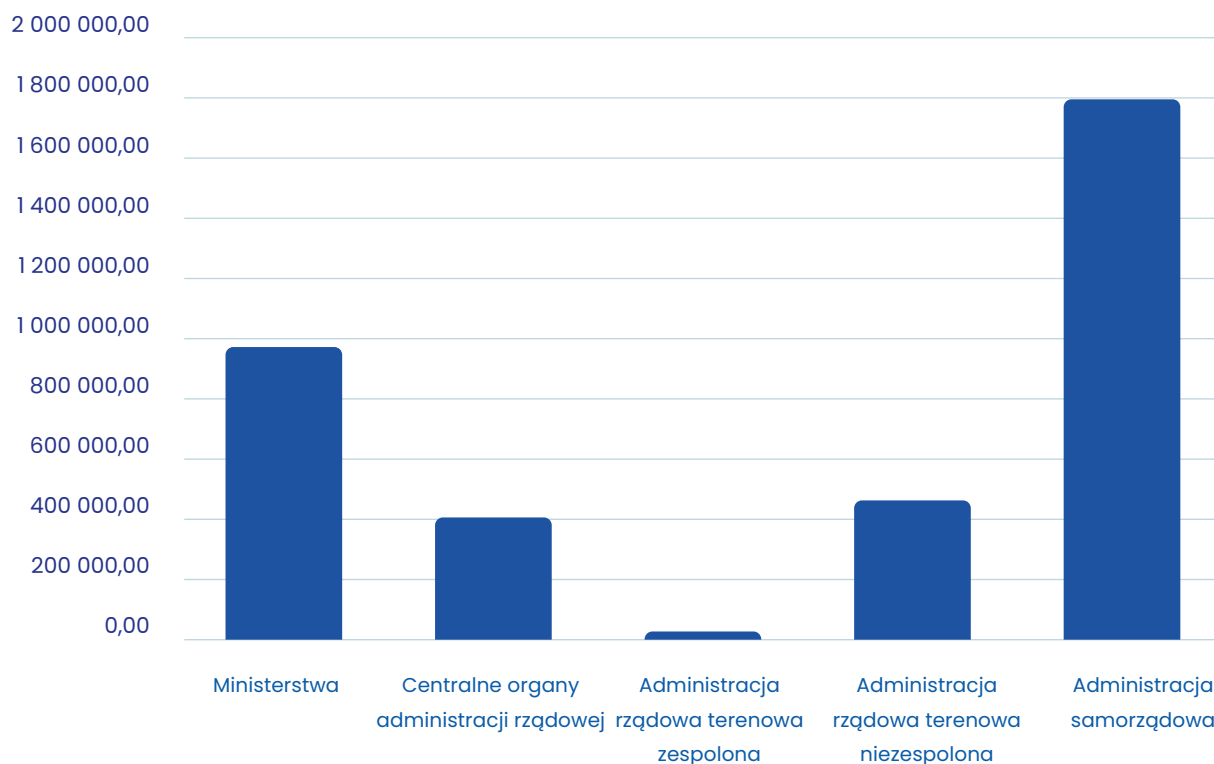
Pomimo dostrzegania korzyści płynących z dywersyfikacji dostawców, obserwujemy pewną bierność instytucji w planowaniu lub nawet rozważaniu takich zmian. Taka sytuacja może sugerować niedobór kompetencji lub zasobów niezbędnych do skutecznego zarządzania złożonym procesem transformacji technologicznej.

4.4. Wydatki na chmurę w administracji publicznej

Aby w pełni zrozumieć ekosystem usług chmurowych w administracji publicznej, należy spojrzeć również na koszty ponoszone przez jej jednostki z tytułu korzystania z technologii cloud. **Średni roczny koszt brutto korzystania z usług chmurowych przez wszystkie grupy jednostek sektora publicznego w 2024 roku wyniósł 2 799 555,79 zł.**

Wydatki te znacznie różnią się jednak dla poszczególnych grup podmiotów. **Średni koszt brutto korzystania z usług chmurowych przez wszystkie grupy jednostek sektora publicznego w 2024 r.** (z pominięciem Ministerstwa Finansów; objaśnienie poniżej) **wynosił 1,42 mln zł.** Największy średni koszt korzystania z usług chmurowych (za ubiegły rok) deklaruują jednostki administracji samorządowej (ok. 1,79 mln zł). Średnio 952 tys. zł kosztowało w 2024 r. korzystanie z chmury ministerstwa. Znacznie mniej na chmurę wydały natomiast jednostki administracji terenowej rządowej niespolonej (ok. 455 tys. zł), centralne organy administracji rządowej (ok. 397 tys. zł) oraz jednostki administracji terenowej rządowej zespolonej, które na ten cel wydawały zdecydowanie najmniej – po średnio 28,5 tys. zł.

Średni koszt usług chmurowych w administracji publicznej w zł (z pominięciem Ministerstwa Finansów)

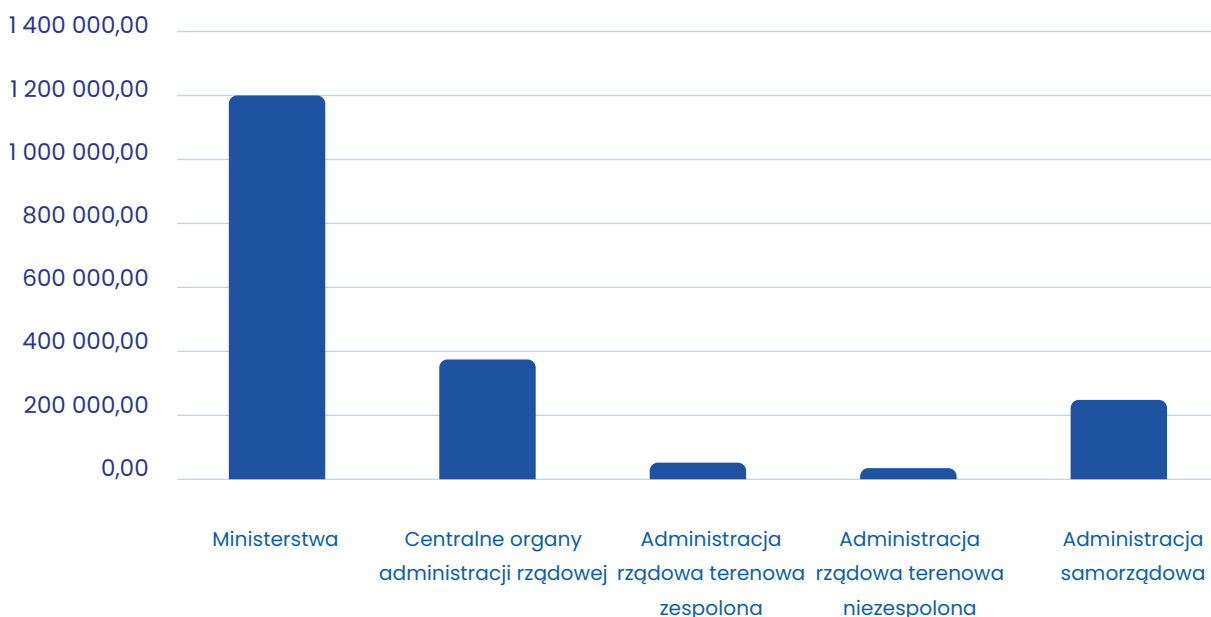


Należy zauważyć, że koszty ponoszone przez jedno z ministerstw – Ministerstwo Finansów, wynoszące prawie 47 mln zł, znacząco zawyżają średnią dla tej grupy organów sektora publicznego. Wysokość kosztów ponoszonych przez Ministerstwo Finansów wiązać się może z kwestią zapewniania przez podlegające ministerstwu Centrum Informatyki Resortu Finansów usług chmurowych nie tylko na własne potrzeby, ale również dla całego systemu Krajowej Administracji Skarbowej, której wybrane jednostki również zostały ujęte w raporcie. Jeśli uwzględnić MF w analizie, to średni koszt korzystania z usług chmurowych (za ubiegły rok) dla ministerstw wyniósłby ok. 8,2 mln zł.

Analiza udzielonych przez podmioty administracji publicznej wskazuje także, że znaczące rozbieżności w wysokościach kosztów występują nie tylko pomiędzy poszczególnymi grupami organów administracji publicznej, ale również wewnątrz tych grup. Obraz kosztów ponoszonych w związku z korzystaniem z chmury przez administrację publiczną uzupełnić należy zatem o ich medianę. Mediana kosztów korzystania z usług chmurowych przez jednostki sektora publicznego w 2024 r. wynosi 1,2 mln zł dla

ministerstw, 377 tys. zł dla centralnych organów administracji rządowej, 214 tys. zł dla jednostek samorządu terytorialnego, 38 tys. zł w przypadku jednostek administracji terenowej rządowej zespolonej oraz 16,5 tys. zł dla jednostek administracji terenowej rządowej niezespolonej.

Mediana kosztów związanych z usługami chmurowymi ponoszonych przez administrację publiczną



Zdecydowana większość jednostek nie ewidencjonuje szczegółowo elementów składowych oferty, składających się na całkowitą kwotę kosztów, o których informacje udostępniono na potrzeby naszego raportu. Więcej o strukturze kosztów (za ubiegły rok) związanych z chmurą możemy jednak dowiedzieć się na przykładzie Ministerstwa Infrastruktury, które na opłaty za licencje oprogramowania wydało 777 tys. zł, a na wdrożenia 16 tys. zł. Wydatki Urzędu Miasta Katowice z kolei wynosiły 326 tys. zł na opłaty licencyjne oraz 88 tys. zł na koszty infrastruktury w chmurze. Urząd ten wskazał też, że ponosi też koszty w zakresie wsparcia i szkolenia, lecz nie określił szczegółowo wysokości tych składowych. Koszty poniesione w roku 2024 przez Urząd Miasta Stołecznego Warszawy w zakresie chmury prywatnej (koszty usług aplikacyjnych i infrastruktury) wyniosły ok. 9,5 mln zł, w zakresie usług bazodanowych ok. 618 tys. zł, oraz w zakresie chmury publicznej (koszty infrastruktury) ok. 1,7 mln zł.



RAFAŁ PRABUCKI

dr in.ż, WPiA UŚ, adiunkt

OKIEM EKSPERTA

Roczny koszt chmury waha się od kilkunastu tysięcy zł do nawet 47 mln zł. Przykłady (Warszawa, Katowice, Ministerstwo Infrastruktury) pokazują zupełnie różne podejścia do inwestycji i ewidencjonowania kosztów. Brak ujednoliconego podejścia do budżetowania i monitoringu kosztów. Raport wskazuje, że polska administracja publiczna jest na wczesnym etapie adaptacji technologii chmurowych, z dominującym podejściem reaktywnym, a nie strategicznym. Główne ryzyka to brak suwerenności technologicznej, *vendor lock-in*, brak analizy kosztów oraz słabe zarządzanie kontraktami i bezpieczeństwem.



MAGDALENA DZIEWGUĆ

Country Director,
Google Cloud Poland

OKIEM EKSPERTA

Poziom przygotowania sektora publicznego do wdrażania chmury może budzić wątpliwości – zwłaszcza w kontekście nadchodzących obowiązków wynikających z aktów takich jak NIS2. Można zaobserwować luki w zakresie ujednoliconych polityk zarządzania ryzykiem dostawców (*third-party risk*), mechanizmów oceny zgodności usług z wymaganiami sektorowymi oraz operacyjnych standardów dla wdrażania usług chmurowych. Należy bowiem pamiętać, że ryzyko systemowe może wynikać nie tylko z niewłaściwej konfiguracji usług, ale też z braku mechanizmów wymuszenia zgodności na etapie projektowania (*security by design*).

Biorąc pod uwagę obserwowany obecnie stan prawny i organizacyjny, można zakładać, że sektor publiczny musi być przygotowany na ryzyko niekontrolowanego wzrostu kosztów, słabego zabezpieczenia danych oraz niemożności szybkiego reagowania na zmiany regulacyjne lub incydenty cyberbezpieczeństwa.

Niedobór wyczerpujących odpowiedzi na pytania dotyczące części składowych kosztów związanych z usługami chmurowymi może wynikać z faktu, że nie wszystkie jednostki sektora publicznego prowadzą ewidencję i analizę tych kosztów. Przykład Warszawy wskazuje natomiast, że istnieją jednostki które podjęły próbę zbudowania nowoczesnej infrastruktury przetwarzania danych i dobrze identyfikują rodzaje rozwiązań chmurowych, modeli korzystania z chmury, a także prawidłowo przypisują koszty do poszczególnych rodzajów wydatków.

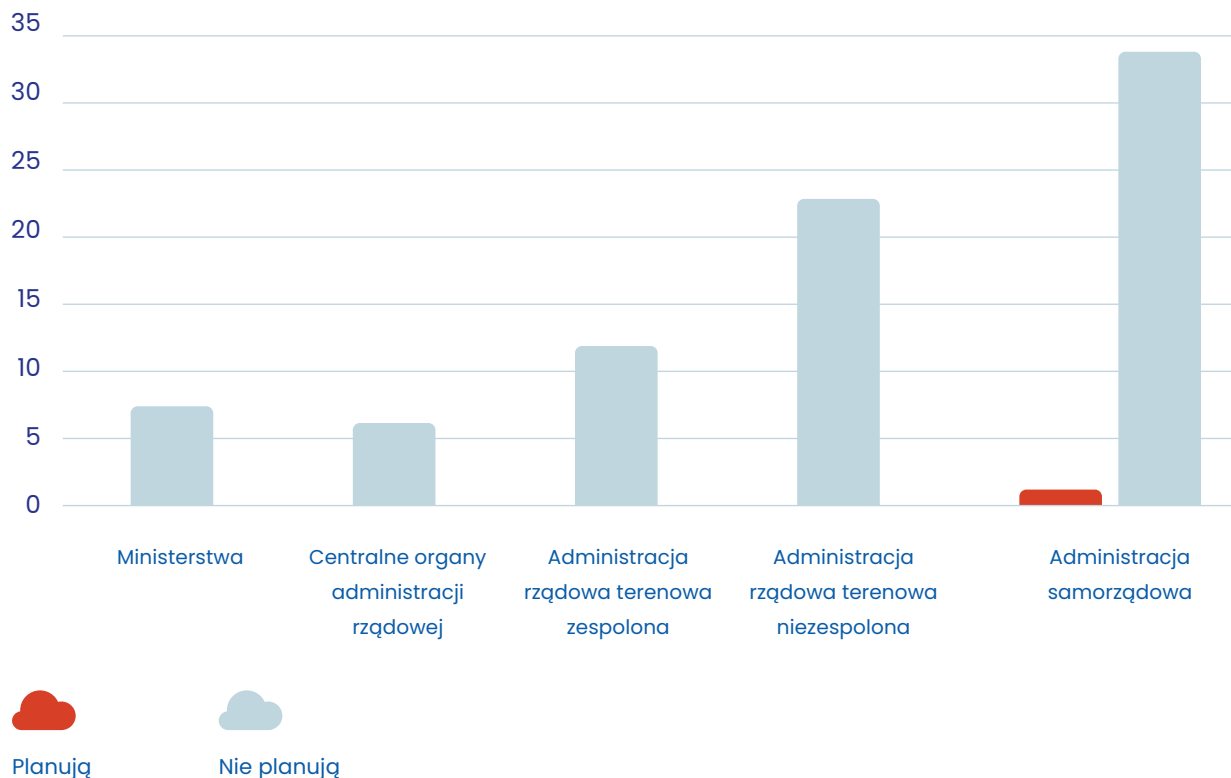
4.5. Plany i strategie zarządzania chmurą w sferze dostawców

Niemal żadna z jednostek administracji publicznej nie planuje zbadać możliwości wykorzystania innych dostawców chmurowych, ani zmienić dostawców cloud dla starszych typów oprogramowania (*legacy software*). Tylko jeden podmiot deklaruje, że rozważa takie działania w przyszłości ze względu na czynniki takie jak oszczędności kosztów, obawy o suwerenność, zwiększona elastyczność czy obawy o uzależnienie od dostawcy.

Dane wskazują na powszechny wśród jednostek administracji publicznej brak planów i długofalowych strategii poszukiwania nowych rozwiązań chmurowych od nowych dostawców. Bez wątpienia będzie miało to wpływ na utrzymanie się zidentyfikowanego zjawiska *vendor lock-in* w tym segmencie rynku. Należy jednak wskazać, że wiele z badanych jednostek odmówiło odpowiedzi na pytania dotyczące planów i zamierzeń, argumentując, że nie dotyczą one sfery czystych faktów, a zatem nie stanowią informacji publicznej.

Warto podkreślić również, że żadna z jednostek, które nie korzystają obecnie z chmury, a które udzieliły odpowiedzi na pytanie dotyczące strategii, nie planuje zbadać możliwości korzystania z usług dostawców chmurowych.

Plany zbadania przez organy administracji publicznej wykorzystania innych dostawców technologii chmurowych



KRZYSZTOF SZUBERT

Senior Associate Member & Advisor
– University of Oxford, Pełnomocnik
Dyrektora ds. Komercjalizacji
i Współpracy Międzynarodowej –
Instytut Łączności

OKIEM EKSPERTA

Rozwój usług chmurowych w administracji publicznej to kierunek nie tylko pożądaný, ale wręcz niezbędny z perspektywy modernizacji państwa. Należy jednak podkreślić, że kluczowe znaczenie mają tu kwestie bezpieczeństwa i suwerenności cyfrowej. W szczególności dane wrażliwe powinny być przechowywane w suwerennych środowiskach chmurowych – najlepiej zarządzanych przez krajowych dostawców. Optymalnym rozwiązaniem wydaje się model hybrydowy, łączący możliwości chmur publicznych i prywatnych, ale z wyraźnym priorytetem dla rozwiązań krajowych.

KRZYSZTOF SZUBERT

W tym kontekście istotnym krokiem było przyjęcie w 2025 roku Standardów Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO). Dzięki nim administracja publiczna może korzystać z chmur publicznych, pod warunkiem spełnienia jasno określonych i rygorystycznych wymagań bezpieczeństwa. Równolegle należy wzmacniać krajowe kompetencje chmurowe, traktując je jako fundament technologicznej niezależności kraju.

Cyfryzacja administracji to integralny element tej strategii – przykładem jest projekt EZD RP, który zakłada wdrożenie elektronicznego zarządzania dokumentacją w tysiącach urzędów. Chmura pełni tu rolę narzędzia zwiększającego efektywność, dostępność i jakość usług publicznych.

Warto również zwrócić uwagę na rozwój Chmury Rządowej, realizowanej w ramach Wspólnej Infrastruktury Informatycznej Państwa (WIIP). Platforma ta, działająca od lutego 2023 roku, obsługuje już kilkanaście systemów administracyjnych i oferuje usługi w modelach IaaS, PaaS i SaaS. Do 2026 roku planowana jest rozbudowa infrastruktury o nowe centra danych oraz integracja z wybranymi chmurami komercyjnymi – przy zachowaniu najwyższych standardów bezpieczeństwa i kontroli nad lokalizacją danych. Celem tych działań jest stworzenie nowoczesnego, bezpiecznego i efektywnego środowiska IT dla sektora publicznego – odpowiadającego na wyzwania cyfrowej transformacji i wzmacniającego cyfrową suwerenność państwa.



MATEUSZ JAKUBIK

Compliance Officer w Bonnier
Business Polska, wykładowca,
Członek Zarządu SABI –
Stowarzyszenia Inspektorów
Ochrony Danych

OKIEM EKSPERTA

Z raportu wyłania się obraz braku strategicznego podejścia państwa do transformacji cyfrowej opartej na technologiach chmurowych. Wiele jednostek nie prowadzi rejestru szczegółowych kosztów, nie analizuje efektywności wdrożonych rozwiązań, ani nie rozważa alternatyw. Poważnym ograniczeniem jest także brak jednolitych standardów dotyczących wdrażania i monitorowania rozwiązań chmurowych – zarówno w aspekcie prawnym, jak i bezpieczeństwa informacji.

MATEUSZ JAKUBIK



ALEKSANDER WOJDYŁA,

CISSP, audytor bezpieczeństwa informacji, niezależny ekspert ds. cyberbezpieczeństwa

Niepokojąca jest też praktyczna bierność jednostek, które nawet przy uznaniu korzyści płynących z dywersyfikacji, nie planują ani nie rozważają zmiany dostawców. Może to wskazywać na deficyt kompetencji lub zasobów do zarządzania zmianą technologiczną.

OKIEM EKSPERTA

Najbardziej racjonalnym modelem rozwoju usług chmurowych w mojej ocenie byłby model federacyjny – tj. certyfikowany katalog usługodawców chmurowych (również prywatnych), którzy spełniają jednolite wymagania bezpieczeństwa i zgodności. Takie podejście łączy korzyści konkurencji z kontrolą państwa nad danymi strategicznymi. Model monopolu państwowego (ZUCH) w obecnej formie jest zbyt nieefektywny, natomiast pełna komercjalizacja dostępu do zasobów cyfrowych może pozbawić państwo kontroli nad danymi krytycznymi. Dywersyfikacja powinna być poparta realnymi procedurami audytowalności, egzekwowalnymi SLA i zgodnością z regulacjami.

Z perspektywy bezpieczeństwa informacji kluczowe jest przesunięcie akcentu z samej dostępności usług chmurowych na ich przewidywalność, kontrolowalność i zgodność z wymogami prawa. Niezbędne jest stworzenie mechanizmu weryfikującego zgodność usług chmurowych ze zdefiniowanymi poziomami bezpieczeństwa (*security tiers*) oraz mechanizmu rejestracji incydentów w środowisku chmurowym. W raporcie brakuje również oceny jakości audytów usług chmurowych – zarówno tych prowadzonych przez samych dostawców, jak i przez organy administracji. Wdrożenie polityki Cloud First powinno iść w parze z ustanowieniem państwowego katalogu minimalnych wymagań bezpieczeństwa i zgodności, obowiązującego wszystkich dostawców chmurowych, współpracujących z administracją publiczną.



DR INŻ. RADOSŁAW NIELEK

Dyrektor NASK-PIB

OKIEM EKSPERTA

Wykorzystanie usług chmurowych w administracji publicznej może być rozwiązaniem problemu skalowalności i elastyczności usług publicznych. Praktycznie natychmiastowy dostęp do najnowszych technologii bez konieczności ponoszenia znacznych nakładów na zakup infrastruktury pozwala podmiotom publicznym testować rozwiązania i wdrażać narzędzia w ciągu dni zamiast miesięcy. Wysoka specjalizacja i profesjonalne zarządzanie infrastrukturą przez dostawców usług to także, zwłaszcza dla mniejszych instytucji, gwarancja przestrzegania najwyższych standardów w zakresie bezpieczeństwa fizycznego centrów danych czy polityki tworzenia kopii zapasowych.

Coraz więcej podmiotów publicznych już to rozumie, bo badania pokazują, że ponad 70% z nich korzysta aktywnie z usług chmurowych. Wciąż jednak jest przestrzeń do dalszej edukacji i promocji. Mądre korzystanie z usług chmurowych pozwala na znaczną poprawę jakości świadczonych usług publicznych i optymalizację kosztów



AGNIESZKA OLSZEWSKA

Prezes Urzędu Zamówień
Publicznych

OKIEM EKSPERTA

Z zainteresowaniem i uwagą zapoznałam się z treścią raportu dotyczącego wykorzystania technologii chmurowych przez jednostki polskiej administracji publicznej. Przedstawione dane i wnioski stanowią istotny wkład w debatę o cyfryzacji sektora publicznego oraz o bezpieczeństwie i efektywności realizowanych zamówień publicznych w obszarze IT.

Z punktu widzenia Urzędu Zamówień Publicznych, szczególnie istotne są konkretne dane przedstawione w raporcie. **Spośród 59 jednostek administracji publicznej korzystających z chmury obliczeniowej, aż 46 wybrało jednego dostawcę, co oznacza 78% udziału w rynku jednego podmiotu.** Należy zwrócić również uwagę, że **33 jednostki wskazały istniejące umowy licencyjne jako główny czynnik wyboru dostawcy**, podczas gdy tylko 4 jednostki postawiły na pierwszym miejscu względy bezpieczeństwa, a zaledwie **6 jednostek kierowało się oferowanymi zniżkami.**

Raport, nawet przy przyjętych w nim założeniach metodologicznych, sygnalizuje zjawisko *vendor lock-in* w polskiej administracji. **Żadna z badanych jednostek nie potwierdziła zamiaru zmiany dostawcy, a tylko jedna jednostka samorządowa weryfikuje możliwości korzystania z innych dostawców.** Taka sytuacja wskazywać może na istotny potencjał do wykorzystania w większym stopniu strategii zarządzania dostawcami.

Pozytywnie należy ocenić fakt, że **żaden z organów nie wskazał stosowania kar umownych za zmianę dostawcy lub równoległe korzystanie z usług innych podmiotów.** Jednocześnie jednak **tylko 12 jednostek udzieliło odpowiedzi na pytania o kary umowne,** co może świadczyć o konieczności zwiększenia świadomości w zakresie zabezpieczeń kontraktowych.

Zgodnie z obowiązującymi przepisami Prawa zamówień publicznych, instytucje zamawiające mają obowiązek tak formułować warunki postępowań, by zapewniać realny dostęp do rynku jak najszerszemu gronu wykonawców, przy jednoczesnym uwzględnieniu zasad efektywności i gospodarności.

Raport potwierdza potrzebę dalszych działań edukacyjnych i regulacyjnych w zakresie zakupów technologii informatycznych, w tym w szczególności usług chmurowych. Deklarujemy pełną gotowość do dalszej współpracy z organami administracji publicznej, instytucjami kontrolnymi oraz sektorem prywatnym na rzecz budowy bezpiecznej, otwartej i nowoczesnej infrastruktury cyfrowej państwa.

5.

Najważniejsze fakty i wnioski z badania

- Ponad 70% jednostek administracji publicznej w Polsce korzysta z chmury – w szczególności jednostki samorządowe (79%) są bardziej otwarte na chmurę niż administracja centralna.
- Model SaaS (*Software as a Service*) cieszy się wśród administracji publicznej największą popularnością – korzysta z niego ponad połowa jednostek używających chmury.

- Microsoft jest liderem rynku chmurowego dla administracji publicznej – 78% jednostek korzystających z chmury używa usług tego dostawcy.
- W obszarze chmury dla administracji publicznej w Polsce obserwujemy zjawisko *vendor lock-in* (uzależnienia od jednego dostawcy) – głównym kryterium wyboru dostawcy są istniejące umowy licencyjne.
- Bezpieczeństwo nie jest priorytetem – tylko 7% jednostek wskazuje je jako główne kryterium wyboru dostawcy usług cloud.
- Większość jednostek nie planuje zmiany dostawcy ani dywersyfikacji usług – brak strategii ogranicza elastyczność i odporność systemu.

- Powszechny jest brak przejrzystej strategii wdrażania chmury – większość jednostek nie planuje migracji, nie analizuje ryzyk ani nie bada nowych rozwiązań.
- Tylko nieliczne jednostki stosują kary umowne za jakość usług.
- Niektóre jednostki (np. MSWiA) deklarują całkowitą rezygnację z rozwiązań zewnętrznych – preferując wewnętrzne zasoby IT.

6.

Załączniki

6.1. Załącznik 1. Lista jednostek administracji publicznej, do których skierowany został wniosek o udostępnienie informacji publicznej

Administracja centralna:

Ministerstwa: Ministerstwo Aktywów Państwowych, Ministerstwo Cyfryzacji, Ministerstwo Finansów, Ministerstwo Infrastruktury, Ministerstwo Nauki i Szkolnictwa Wyższego, Ministerstwo Rozwoju i Technologii, Ministerstwo Sprawiedliwości, Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Spraw Zagranicznych

Centralne organy administracji rządowej: Generalna Dyrekcja Dróg Krajowych i Autostrad, Główny Urząd Statystyczny, Naczelna Dyrekcja Archiwów Państwowych, Urząd Ochrony Konkurencji i Konsumentów, Urząd Patentowy Rzeczypospolitej Polskiej, Urząd Zamówień Publicznych

Administracja terenowa rządowa:

Administracja zespolona – jednostki podporządkowane wojewodzie: Podkarpacki Urząd Wojewódzki w Rzeszowie, Mazowiecki Urząd Wojewódzki w Warszawie, Małopolski Urząd Wojewódzki w Krakowie, Wojewódzki Inspektorat Nadzoru Budowlanego w Gdańsku, Wojewódzki Inspektorat Nadzoru Budowlanego w Lublinie, Wojewódzki Urząd Ochrony Zabytków w Szczecinie, Wojewódzki Inspektorat Inspekcji Handlowej w Krakowie, Wojewódzki Inspektorat Inspekcji Handlowej w Bydgoszczy;

Administracja niezespolona:

Urząd Skarbowy w Wałbrzychu, Urząd Skarbowy w Suwałkach, Urząd Skarbowy w Wałczu, Urząd Skarbowy w Zakopanem, Śląski Urząd Celno-Skarbowy w Katowicach, Izba Administracji Skarbowej w Lublinie, Izba Administracji Skarbowej w Łodzi, Izba Administracji Skarbowej w Gdańsku, Izba Administracji Skarbowej w Olsztynie, Izba Administracji Skarbowej w Szczecinie, Izba Administracji Skarbowej w Bydgoszczy, Izba Administracji Skarbowej w Zielonej Górze, Izba Administracji Skarbowej w Białymstoku, Izba Administracji Skarbowej w Krakowie, Izba Administracji Skarbowej w Rzeszowie, Izba Administracji Skarbowej w Opolu, Izba Administracji Skarbowej w Katowicach, Izba Administracji Skarbowej we Wrocławiu, Izba Administracji Skarbowej w Poznaniu, Izba Administracji Skarbowej w Kielcach, Izba Administracji Skarbowej w Warszawie;

Administracja samorządowa:

Samorząd wojewódzki (szczebel regionalny): Pomorski Urząd Marszałkowski w Gdańsku, Kujawsko-Pomorski Urząd Marszałkowski w Toruniu;

Samorząd powiatowy (szczebel lokalny): Starostwo Powiatowe Poznań, Starostwo Powiatowe we Wrocławiu;

Samorząd gminny (szczebel podstawowy): Urząd Miasta Krakowa, Urząd Miejski w Gnieźnie, Urząd Miasta Sieradza, Urząd Miejski w Tczewie, Urząd Miejski we Wrocławiu, Urząd Miasta Torunia, Urząd Miasta Bydgoszczy, Urząd Miasta Przemyśl, Urząd Miasta Sopotu, Urząd Miasta Zielona Góra, Urząd Dzielnicy Praga-Południe m.st. Warszawy, Urząd Miasta Stołecznego Warszawy, Urząd Miasta Białegostoku, Urząd Miasta Gdańska, Urząd Miasta Gorzowa Wielkopolskiego, Urząd Miasta Katowice, Urząd Miasta Kielce, Urząd Miasta Lublina, Urząd Miasta Łodzi, Urząd Miasta Olsztyna, Urząd Miasta Opola, Urząd Miasta Poznania, Urząd Miasta Rzeszowa, Urząd Miasta Szczecina, Urząd Miejski w Koninie, Urząd Miasta Leszna, Urząd Miasta Kalisza, Urząd Miasta Włocławek, Urząd Miasta Chorzów, Urząd Miasta Gliwice, Urząd Miejski w Radomiu, Urząd Miasta Gdyni.

82 jednostki administracji publicznej udzieliło odpowiedzi na wniosek, w tym: 7 ministerstw, 6 centralnych organów administracji rządowej, 12 jednostek administracji terenowej rządowej zespolonej, 23 jednostki administracji terenowej rządowej niezespolonej, 34 jednostki samorządu terytorialnego.

Pięć jednostek administracji publicznej nie udzieliło odpowiedzi na skierowane do nich pytania (były to Ministerstwo Sprawiedliwości, Ministerstwo Spraw Zagranicznych, Powiatowy Inspektorat Weterynarii w Radomsku, Urząd Miasta Sieradza oraz Urząd Miasta Rzeszowa)

6.2. Okres objęty badaniem, treść wniosku o udostępnienie informacji publicznej oraz przebieg wywiadów bezpośrednich

Dane będące przedmiotem zasadniczej części Raportu zostały pozyskane poprzez skierowanie do jednostek administracji publicznej, objętych niniejszym Raportem, wniosków o udostępnienie informacji publicznej, zgodnie z art. 2 ust.1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764). Nadto źródło informacji na potrzeby raportu stanowiło wystąpienie pokontrolne Najwyższej Izby Kontroli z dnia 16 marca 2025 r. I/22/008 – Funkcjonowanie Systemu Zapewniania Usług Chmurowych w ramach Wspólnej Infrastruktury Informatycznej Państwa, a także pozyskane umowy licencyjne, do których otrzymaliśmy wgląd w odpowiedzi na złożony wniosek o udostępnienie informacji publicznej.

Wnioski o udostępnienie informacji publicznej przesyłane były za pomocą środków komunikacji elektronicznej w terminie od dnia 7 stycznia 2025 roku do 4 marca 2025 roku. Zbieranie udzielonych odpowiedzi na złożone wnioski trwało od dnia 8 stycznia 2025 roku do dnia 5 maja 2025 roku.

Zapytania przesyłane do podmiotów administracji publicznej zawierały następujące pytania:

1. Jakie dane są przechowywane obecnie w chmurze i z którego/których dostawców korzysta jednostka?
2. Jakie były kluczowe czynniki wpływające na wybór dostawcy(-ów) chmury przez organizację? Proszę uszeregować poniższe czynniki według ważności:
 - a. Istniejące umowy licencyjne

- b. Oferowane zniżki lub zachęty
- c. Integracja z istniejącym oprogramowaniem lub technologią tego samego dostawcy
- d. Funkcje bezpieczeństwa
- e. Inne (proszę określić)

3. Jakie są roczne koszty korzystania z usług chmurowych w jednostce? Czy dostawca wskazuje podział kosztów na konkretne usługi, jeśli tak prosimy o wskazanie kosztów w podziale na usługi. Przykładowo:

- a. Opłaty za licencje oprogramowania
- b. Koszty infrastruktury w chmurze
- c. Inne powiązane koszty (np. wsparcie, szkolenie)

4. Czy jednostka ma plany zbadania możliwości wykorzystania innych dostawców chmurowych? Jeśli tak, prosimy o wskazanie:

- a. alternatywnych rozważanych dostawców chmury,
- b. czynników skłaniających do dywersyfikacji dostawców (np. oszczędności kosztów, obawy o suwerenność, zwiększona elastyczność, obawy o uzależnienie od dostawcy).

5. Czy rozważano zmianę dostawców usług chmurowych dla któregośkolwiek ze starszych typów oprogramowania (legacy software)? Jeśli tak, jakie czynniki uniemożliwiły lub zniechęciły do dokonania zmiany?

Następnie pogłębiono badanie o wywiad bezpośredni z osobami pracującymi w komórkach merytorycznych zajmujących się infrastrukturą IT, w celu weryfikacji udzielonych odpowiedzi oraz weryfikacji komunikacji założeń kierowników jednostek z osobami odpowiedzialnymi za ich realizację.

W dalszej kolejności przeprowadzono dodatkowe rozpytanie mające na celu doprecyzowanie odpowiedzi w zakresie elementów składowych ponoszonych przez organów kosztów oraz kwestii ewentualnych zapisów w umowach z dostawcami przewidujących kary umowne za wypowiedzenie umowy. Wnioski o udzielenie informacji publicznej przesyłane były

za pomocą środków komunikacji elektronicznej w terminie od dnia 7 stycznia 2025 roku do 5 maja 2025 roku.

Zbieranie udzielonych odpowiedzi na złożone wnioski trwało od dnia 8 stycznia 2025 roku do dnia 13 maja 2025 roku.

Dane objęte pytaniem 3., tj. Koszty usług chmurowych zostają w niniejszym raporcie podane w kwotach brutto w walucie PLN. W przypadku uzyskania od organu kwot w walucie EUR, dokonano przeliczenia kwot po kursie 1 EUR = 4,2 zł, co w zaokrągleniu odpowiada średniemu kursowi za poprzedni miesiąc.

Wszystkie dodatkowe zapytania przesyłane do podmiotów administracji publicznej zawierały następujące pytania:

1. Jakie są roczne koszty korzystania z usług chmurowych oferowanych przez dostawcę Microsoft w jednostce? Jakie opłaty przewiduje umowa z dostawcą? Czy dostawca wskazuje podział kosztów na konkretne usługi i/lub uzasadnienie ich wysokości jeśli tak prosimy o wskazanie kosztów w podziale na usługi. Przykładowo:

- opłaty za licencje oprogramowania,
- koszty infrastruktury w chmurze,
- inne powiązane koszty (np. wsparcie, szkolenie).

2. Czy jednostka zawarła umowę na dostawę usług chmurowych przewidującą karę pieniężną lub dodatkowe opłaty związane z rozwiązaniem umowy, zmianą dostawcy usług chmurowych lub równoległym zawarciem umowy z innym dostawcą?