MARUTA \

Warszawa, 4 lipca 2017 r.

**Ministerstwo Cyfryzacji**

ul. Królewska 27

00 - 060 Warszawa

**DOTYCZY:** zlecenia na przygotowanie opinii prawnej o dopuszczalności używania w jednostkach administracji publicznej rozwiązania chmurowego w modelu SaaS wspierającego komunikację wewnętrzną i zarządzanie dokumentami w zakresie prac wewnętrznych i projektów ministerstwa.

Szanowni Państwo,

w wykonaniu umowy zawartej w dniu 5 lutego 2017 roku przez kancelarię Maruta Wachta sp. j. (dalej „**Kancelaria**") ze Skarbem Państwa, w imieniu którego działa Ministerstwo Cyfryzacji, przedstawiamy poniżej opinię w przedmiocie dopuszczalności używania w jednostkach administracji publicznej rozwiązania chmurowego w modelu SaaS wspierającego komunikację wewnętrzną i zarządzanie dokumentami w zakresie prac wewnętrznych i projektów ministerstwa (dalej „**Opinia**").

**OPINIA PRAWNA**

**w przedmiocie**

**dopuszczalności używania w jednostkach administracji publicznej rozwiązania chmurowego w modelu SaaS wspierającego komunikację wewnętrzną i zarządzanie dokumentami w zakresie prac wewnętrznych i projektów ministerstwa**



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

## Spis treści





Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

# I. WSTĘP

[Wprowadzenie i zakres opinii]

(1) Przedmiotem Opinii jest ocena dopuszczalności stosowania w jednostkach administracji publicznej rozwiązań chmurowych w modelu SaaS wspierających komunikację wewnętrzną i zarządzanie dokumentami – w zakresie prac wewnętrznych i projektów Ministerstwa.

(2) Dokonanie powyższej oceny wymaga w pierwszej kolejności zdefiniowania i scharakteryzowania pojęcia rozwiązania chmurowego – także w świetle prawa. W drugiej kolejności konieczne jest przeprowadzenie analizy aktów prawnych – zarówno polskich, jak i europejskich, mogących potencjalnie dotyczyć *cloud computingu*.

[Akty prawne]

(3) Opinia została sporządzona w oparciu o następujące akty prawne, w brzmieniu obowiązującym na dzień sporządzenia Opinii:

(a) Ustawę z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz. U. z 2017 r. poz. 459 ze zm. (dalej: „**Kodeks cywilny**" lub „**k.c.**");

(b) Ustawę z dnia z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, z dnia 16 kwietnia 1993 r., Dz.U. Nr 47, poz. 211 ze zm. (dalej: „**ustawa o zwalczaniu nieuczciwej konkurencji**" albo „**u.z.n.k.**");

(c) Ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U. 1994 Nr 24 poz. 83 ze zm. (dalej: „**prawo autorskie**" albo „**pr.aut.**");

(d) Ustawę z dnia 29 sierpnia 1997 r. Prawo bankowe, Dz.U. Nr 140, poz. 939 ze zm. (dalej: „**prawo bankowe**" albo „**p.b.**");

(e) Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922; (dalej: „**UODO**");

(f) Ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.u. 2002 Nr 144 poz. 1204 ze zm. (dalej: „**ustawa o świadczeniu usług drogą elektroniczną**" albo „**u.ś.u.d.e.**");



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(g) Ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, Dz. U. z 2015 r. poz. 2164 ze zm. (dalej: „**prawo zamówień publicznych**" albo „**p.z.p.**");

(h) Ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010 Nr 182 poz. 1228 ze zm. (dalej: „**ustawa o ochronie informacji niejawnych**" albo „**u.o.i.n.**");

(i) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz.U.2011.159.948 ze zm. (dalej: „**r.p.w.**");

(j) Ustawę z dnia z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, Dz.U. z 2015 r. poz. 1884 ze zm. (dalej: „**ustawa o działalności ubezpieczeniowej i reasekuracyjnej**" albo „**u.d.u.r.**");

(4) – oraz o Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: „**Rozporządzenie**" albo „**RODO**"), którego przepisy będą miały zastosowanie od dnia 25 maja 2018 r.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

# II. WNIOSKI I REKOMENDACJE

(1) Pod pojęciem chmury obliczeniowej należy rozumieć model przetwarzania umożliwiający dogodny, realizowany na żądanie dostęp do współdzielonej puli konfigurowalnych zasobów informatycznych (np. sieci, serwerów, pamięci, aplikacji i usługi), które mogą zostać natychmiastowo zaalokowane i udostępnione poprzez dostęp sieciowy z minimalnym wysiłkiem zarządzania oraz na minimalnym poziomie interwencji członków personelu usługodawcy chmurowego. Do podstawowych cech *cloud computingu* należą: samoobsługowość, dostęp przez sieć, współdzielenie wykorzystywanych zasobów, alokowanie zasobów, mierzalność usług, różnorodność modeli świadczenia usług.

(2) Można wyróżnić wiele sposobów podziału i wynikających z nich kategorii usług chmurowych. Kluczowe są jednak dwa z nich. Na podstawie pierwszego, dotyczącego rodzaju i dyslokacji udostępnianych zasobów, można wyróżnić **chmurę publiczną, chmurę prywatną, chmurę wspólnotową i chmurę hybrydową**. Na podstawie drugiego, dotyczącego modelu świadczenia usług, można wyróżnić usługi: ***Infrastructure as a Service* (IaaS)**, ***Platform as a Service* (PaaS)**, ***Software as a Service* (SaaS)**. Mówi się w tym kontekście także o *Everything as a Service* (XaaS).

(3) Nie istnieje żaden akt prawny regulujący całościowo zagadnienie chmury obliczeniowej. W świetle prawa stanowi ona rodzaj umowy o świadczenie usług uregulowanej w Kodeksie cywilnym, zazwyczaj wzbogaconej elementami licencyjnymi, podlegającymi regulacji prawa autorskiego (przy czym często przysparza trudności precyzyjne wskazanie, w jakim zakresie postanowienia umowy dotycząca *cloud computingu* mają charakter usługowy, a w jakim licencyjny). Ponadto odnośnie do chmury znajdują zastosowanie szczegółowe regulacje dotyczące pewnych obszarów gospodarki – takie jak np. prawo bankowe w zakresie przepisów o outsourcingu bankowym. W związku z nimi bywają wydawane akty tzw. *soft law* dotyczące bardzo szczegółowych zagadnień powiązanych (m.in.) z *cloud computingiem*.

(4) Nie istnieje także żaden akt prawny ustanawiający restrykcje dla administracji publicznej w zakresie stosowania przez nią chmury obliczeniowej. Nie robi tego w szczególności prawo zamówień publicznych. Z jego perspektywy zamówienie na usługi chmurowe jest standardowym zamówieniem publicznym. Przy czym jego kwalifikacja jako dostawy lub usługi w rozumieniu prawa zamówień



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

publicznych będzie zależeć od specyfiki przedmiotu takiego zamówienia. Co więcej, w razie oferowania usług chmurowych przez „pośrednika" (partnera) dostawcy chmury, co jest często spotykane na rynku, o ile relacja pomiędzy nim a zamawiającym będzie podlegać reżimowi prawa zamówień publicznych, o tyle relacja pomiędzy zamawiającym a właściwym dostawcą chmury co do zasady będzie z niego wyłączona (a więc p.z.p. nie będą podlegały umowy, porozumienia czy regulaminy dostawcy – chyba że stanowiłyby one integralną część umowy w sprawie zamówienia publicznego).

(5) Jest warte zaznaczenia, że z punktu widzenia prawa zamówień publicznych i wyrażonej w nim zasady uczciwej konkurencji (art. 7 ust. 1 p.z.p.), nie stanowi realnego ryzyka hipotetyczna możliwość nieautoryzowanego dostępu dostawcy usług chmurowych wykorzystywanych przez jednostkę administracji publicznej do danych dotyczących innego przetargu, w którym ten dostawca potencjalnie może brać udział (w celu uzyskania wiedzy o ofertach swoich konkurentów). W praktyce wystąpienie takiej sytuacji jest mało prawdopodobne i stanowiłoby rażące naruszenie umowy pomiędzy zamawiającym a dostawcą usług chmurowych.

(6) Niezależnie od powyższego, z wykorzystaniem rozwiązań chmurowych wiąże się szereg istotnych ryzyk. Do najważniejszych z nich należy zaliczyć kwestie dotyczące:

(a) danych osobowych – co wynika w dużej mierze ze znaczących zmian prawnych w tym obszarze – implikowanych wprowadzeniem przepisów RODO. Rozporządzenie to przewiduje w szczególności konieczność:

1. zawarcia między stronami umowy o powierzenie przetwarzania danych osobowych, która powinna wskazywać zwłaszcza: przedmiot i czas przetwarzania danych, ich rodzaj, charakter, a także cel przetwarzania,

2. zastosowania przez dostawcę chmury odpowiednich środków organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danym osobowym (czego obowiązek powinna uwzględniać umowa z dostawcą),

3. zaakceptowania przez administratora danych (usługobiorcę) wykorzystywania przez dostawcę podwykonawców oraz, jeśli mają oni świadczyć usługi, nałożenia na nich takich samych obowiązków w zakresie przetwarzania danych osobowych, jakie ciążą na dostawcy,



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

4. usunięcia lub zwrotu danych osobowych po zakończeniu świadczenia usług,
5. umożliwienia administratorowi (usługobiorcy) otrzymywania informacji od dostawcy o zakresie ochrony danych oraz przeprowadzania audytu,
6. spełnienia szczególnych warunków w sytuacji transferu danych osobowych za granicę, do kraju innego niż należący do EOG lub Konfederacji Szwajcarskiej;

(b) informacji niejawnych – ustawa o ochronie informacji niejawnych przewiduje specjalne warunki przetwarzania informacji niejawnych we wszelkiego rodzaju systemach teleinformatycznych. W ich wyniku przetwarzanie informacji niejawnych w chmurze publicznej może okazać się w praktyce niemożliwe. Natomiast nie musi to dotyczyć chmury prywatnej, nad której fizyczną infrastrukturą usługobiorca może mieć pełną kontrolę (analiza w stosunku do chmury wspólnotowej lub hybrydowej musiałaby być przeprowadzona odrębnie dla każdego przypadku, w zależności od jej właściwości). Wspomniane wyżej problemy w przetwarzaniu informacji niejawnych w chmurze publicznej dotyczą przede wszystkim:

1. braku kontroli usługobiorcy kontroli nad fizyczną infrastrukturą – którą zarządza dostawca chmury i która w większości przypadków jest bardzo rozproszona,
2. braku wiedzy usługobiorcy nt. architektury i mechanizmów działania chmury,
3. braku wpływu na modyfikowanie i rozwijanie oprogramowania budującego chmurę,
4. kwestii usuwania danych zawierających informacje niejawne – a precyzyjniej, braku wiedzy usługobiorcy o sposobie i terminach przeprowadzenia takiego usunięcia,
5. braku realnej możliwości przeprowadzenia przez usługobiorcę testów i audytów oprogramowania „budującego" chmurę.

(7) Podsumowując powyższą kwestię, jednostka administracji publicznej, chcąc przetwarzać dane osobowe w chmurze, musi zapewnić sobie usługodawcę spełniającego szereg wymagań wynikających z przepisów o ochronie danych osobowych. Natomiast w zakresie informacji niejawnych należy stwierdzić, że o



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

ile ich przetwarzanie w chmurze prywatnej, przy spełnieniu szczególnych obowiązków określonych w u.o.i.n., jest możliwe, o tyle co do zasady niemal niemożliwe będzie dopełnienie ich w celu przetwarzania informacji niejawnych w chmurze publicznej. Z tego powodu nie rekomendujemy takiego działania.

(8) W związku ze stosowaniem chmury pojawią się także inne ryzyka. Są to przede wszystkim zagrożenia wynikające z:

(a) modelu kontraktowania w obszarze usług chmurowych – gdzie stosowane są umowy adhezyjne (tzn. nienegocjowalne lub negocjowalne w niewielkim zakresie), referujące do zewnętrznych wzorców (regulaminów) umownych, których treść jest dosyć swobodnie modyfikowana przez dostawców chmurowych;

(b) poufności – podmioty publiczne powinny zapewnić sobie jak najszersze i rygorystyczne zasady ochrony informacji poufnych w kontraktach z dostawcą chmury;

(c) *vendor lock-in* – tj. uzależnienia od dostawcy, które może wynikać przede wszystkim z postanowień dotyczących wynagrodzenia oraz z braku planu rezygnacji z danych usług chmurowych (tzw. *exit planu*);

(d) integracji rozwiązania chmurowego z innymi chmurami lub oprogramowaniem – co może wiązać się z nieoczekiwanymi, dodatkowymi opłatami ze strony usługobiorcy.

(9) Jakkolwiek administracji publicznej nie obejmują żadne szczegółowe regulacje prawne odnoszące się do *cloud computingu*, za celowe należałoby uznać dokonanie przez nią „zapożyczenia" rozwiązań stosowanych (z mocy przepisów prawa) w sektorze finansowym odnośnie chmury – czy szerzej – outsourcingu IT. Dotyczy to, w naszej opinii, w szczególności posiadania własnej, rozbudowanej i szczegółowej dokumentacji zawierającej plany i procedury pozwalające uniknąć wystąpienia danych ryzyk związanych z usługami chmurowymi lub zaradzić ich skutkom sprawnie i przy jak najmniejszych stratach finansowych.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

# III. CHARAKTERYSTYKA OGÓLNA ROZWIĄZAŃ CHMUROWYCH

[Pojęcie i charakterystyka chmury]

(1) Chmura obliczeniowa stanowi metodę eksploatacji zasobów IT, przeciwstawianą tradycyjnym rozwiązaniom *on-premise* – tzn. opartym na własnej, fizycznej infrastrukturze IT. W powszechnym odbiorze chmura stanowi techniczną „nowinkę" – i chociaż rzeczywiście jest modelem znacznie młodszym niż *on-premise*, to nie jest rozwiązaniem całkowicie nowym. Pojęcie chmury obliczeniowej oraz przetwarzania danych w chmurze (*cloud computing*) ma ponad 20-letnią historię: zostało po raz pierwszy użyte przez S.E. Gillet i M. Kapora w 1996 roku[1]. Ponadto *cloud computing*, rozumiany jako zespół technologii teleinformatycznych oraz jednocześnie model przetwarzania danych w formie usług, jest oparty na funkcjonujących wcześniej rozwiązaniach technicznych, takich jak przetwarzanie sieciowe (*grid computing*), *utility computing*, wirtualizacja, *autonomic computing*, *service-orientated architecture* (SOA).

(2) Celem modelu chmurowego jest uproszczenie pozyskiwania i eksploatacji mocy obliczeniowej oraz niezbędnych usług teleinformatycznych – w sposób analogiczny do tego, w którym dostarczane są podstawowe media (jak woda, prąd, gaz, usługi telekomunikacyjne). Cel ten można określić mianem dążenia do „utowarowienia" zasobów IT[2].

(3) W kontekście pojęcia chmury obliczeniowej nie można mówić o jednolitej, ogólnie przyjętej definicji, w literaturze funkcjonuje ich bardzo wiele[3]. Jednakże szczególnym uznaniem i popularnością cieszy się propozycja definicji chmury przedstawiona przez Krajowy Instytut Norm i Technologii Stanów Zjednoczonych (*National Institute of Standards and Technology*, w skrócie: NIST), która określa chmurę obliczeniową jako model przetwarzania umożliwiający dogodny, realizowany na żądanie dostęp do współdzielonej puli konfigurowalnych zasobów informatycznych (np. sieci, serwerów, pamięci,

[1] S.E. Gillett, M. Kapor: *The Self-governing Internet: Coordination by Design, Coordination and Administration of the Internet, Workshop at Kennedy School of Government*, Harvard University September 8-10, 1996.

[2] Zob. N. G. Carr, *IT Doesn't Matter*, Harvard Business Review, 2003/05, s. 7-11.

[3] Przegląd przykładów definicji dostępny m.in. na stronie: http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2016/T2/t2_0725.pdf.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

aplikacji i usługi), które mogą zostać natychmiastowo zaalokowane i udostępnione poprzez dostęp sieciowy z minimalnym wysiłkiem zarządzania i na minimalnym poziomie interwencji reprezentantów usługodawcy[4].

(4) Na podstawie przytoczonej powyżej definicji możliwe jest określenie podstawowych cech oraz warunków funkcjonowania usług świadczonych w modelu chmurowym. Są to:

(a) samoobsługowość – dostępność usług na żądanie (*on demand*) użytkownika, przy czym użytkownicy zgłaszający zapotrzebowanie na takie usługi korzystają z nich samodzielnie i w sposób zautomatyzowany, bez konieczności wsparcia ze strony dostawcy rozwiązania;

(b) dostęp przez sieć – świadczenie usług przez Internet;

(c) współdzielenie wykorzystywanych zasobów – udostępnianie na bazie tej samej infrastruktury IT, niezależnie i jednocześnie, usług dla wielu niepowiązanych ze sobą użytkowników;

(d) elastyczne alokowanie i zwalnianie zasobów – możliwość modyfikowania *online* zakresu usług w zależności od potrzeb użytkowników i odpowiadająca jej zmienność zakresu zasobów infrastrukturalnych zaangażowanych w obsługę tych usług;

(e) mierzalność usług – możliwość monitorowania zakresu i intensywności świadczenia usług;

(f) różnorodność – wielość i różnorakość modeli świadczenia usług oraz rodzaju świadczonych usług.

(5) Stosowanie rozwiązań chmurowych wiąże się z powstaniem określonych skutków w sferze ekonomicznej oraz społecznej. Wśród nich, w pierwszym rzędzie, można wyróżnić wzrost konkurencyjności usług informatycznych dostępnych dla podmiotów publicznych oraz prywatnych. Należy także spostrzec dynamizację digitalizacji – tak sektora prywatnego, jak i administracji publicznej – rozumianą jako:

(a) usprawnienie ich działania;

(b) zwiększenie dostępności usług kierowanych do użytkownika końcowego (odpowiednio: usługobiorcy lub obywatela) dzięki zastosowaniu nowoczesnych technologii.

[Typologia oraz charakterystyka modelu chmurowego świadczenia usług]

[4] Definicja dostępna pod adresem: https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(6) Z uwagi na różnorodność funkcjonujących w obrocie gospodarczym rozwiązań chmurowych, istnieje wiele kryteriów ich podziału. Jednakże ze względu na ich znaczenie praktyczne, wskazania i charakterystyki wymagają dwa z tych kryteriów, zaproponowane przez NIST[5]: rodzaj i dyslokacja dostarczanych zasobów IT (*ang. deployment*) oraz model świadczonych usług.

(7) Według kryterium rodzaju i dyslokacji zasobów IT w ramach świadczenia usług chmurowych należy wyróżnić cztery następujące rodzaje usług chmurowych:

(a) chmurę prywatną (*private cloud*), charakteryzującą się tym, że:

1. jej zasoby są udostępniane do korzystania wyłącznie przez jedną organizację,

2. infrastruktura informatyczna może należeć, być zarządzana i utrzymywana przez jednostki wewnętrzne organizacji korzystającej z chmury prywatnej lub usługodawcę zewnętrznego,

3. zasoby informatyczne mogą znajdować sią w lokalizacji należącej do organizacji korzystającej z chmury prywatnej lub poza lokalizacjami tej organizacji;

(b) chmurę publiczną (*public cloud*), charakteryzującą się tym, że:

1. zasoby informatyczne w jej zakresie udostępniane są do korzystania przez nieokreśloną grupę odbiorców dysponujących dostępem do Internetu,

2. jej zasoby mogą należeć, być zarządzane i utrzymywane przez komercyjne podmioty zewnętrzne, organizacje rządowe lub akademickie;

(c) chmurę społecznościową/wspólnotową (*community cloud*), charakteryzującą się tym, że:

1. zasoby informatyczne udostępniane w jej ramach są udostępniane do wyłącznego użytku specyficznej, ściśle określonej grupy użytkowników, którzy mają zbliżone potrzeby oraz wymagania (np. dotyczące zapewnianych funkcjonalności, standardów bezpieczeństwa, etc.),

2. jej zasoby mogą należeć, być zarządzane i utrzymywane przez jedną z organizacji należących do danej społeczności lub przez usługodawcę zewnętrznego,

[5] P. Mell, T. Grance, *The NIST Definition of Cloud Computing,* dostępny pod adresem: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

3. zapewniane w jej ramach zasoby IT mogą znajdować się w lokalizacji członka lub kilku członków danej społeczności lub w lokalizacji zewnętrznego dostawcy;

(d) chmurę hybrydową (*hybrid cloud*), charakteryzującą się tym, że jej zasoby informatyczne stanowią kombinację dwóch lub większej liczby odrębnych rodzajów chmur opisanych powyżej [lit. chmurę prywatną (*private cloud*), charakteryzującą się tym, że:-chmurę społecznościową/wspólnotową (*community cloud*), charakteryzującą się tym, że:]. Chmury te są odrębnymi jednostkami, ale pozostają połączone ze sobą zgodnie z ustalonymi standardami lub technologią, co zapewnia ich kompatybilność, a także pozwala na przenoszenie danych i aplikacji pomiędzy nimi – zgodnie z intencją użytkownika[6].

(8) Według kryterium modelu świadczenia usług chmurowych należy wyróżnić następujące rodzaje świadczenia usług w chmurze:

(a) Infrastruktura jako usługa (*Infrastructure as a Service*/IaaS).

1. W ramach tego modelu użytkownik uzyskuje dostęp do mocy obliczeniowej, pamięci, sieci oraz innych podstawowych zasobów informatycznych, których wykorzystanie pozwala na uruchomienie potrzebnego oprogramowania (np. systemu operacyjnego lub aplikacji).

2. Użytkownik nie ma możliwości zarządzania udostępnionymi mu zasobami ani kontrolowania ich, ale może zarządzać systemem operacyjnym oraz instalowanymi przez siebie aplikacjami, a ponadto dysponuje ograniczoną kontrolą nad wybranymi komponentami sieciowymi (np. *host firewalls*).

3. Podstawowe usługi dostępne w ramach IaaS to m.in. udostępnianie maszyn wirtualnych, hosting serwerów, archiwizowanie danych.

(b) Platforma jako usługa (*Platform as a Service*/PaaS).

1. Użytkownik uzyskuje dostęp do zasobów infrastrukturalnych, dzięki którym może uruchomić lub rozwijać aplikacje przy wykorzystaniu języków oprogramowania, bibliotek, usług oraz narzędzi dostarczanych i utrzymywanych przez usługodawcę.

[6] Definicje powyższe pochodzą z opracowania pt. *Ekspertyza badawcza w przedmiocie wykorzystania usług przetwarzania w chmurze obliczeniowej (cloud computing) w sektorze administracji publicznej (z uwzględnieniem JST) w Polsce*, s. 72-73.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

2. Użytkownik nie ma kontroli nad zasobami chmury ani nie może nimi zarządzać (jak np. udostępnioną mu siecią, serwerami, systemami operacyjnymi lub pamięciami masowymi).

3. Kontrola użytkownika ograniczona jest do aplikacji przez niego rozwijanych. Dodatkowo użytkownik może mieć również możliwość konfiguracji parametrów środowiska, na którym aplikacje są uruchamiane.

4. Przykładowe zasoby IT udostępniane w ramach PaaS to m.in. bazy danych, narzędzia testowe oraz programistyczne, usługi katalogowe.

(c) Oprogramowanie jako usługa (*Software as a Service*/SaaS).

1. Użytkownik ma możliwość korzystania z aplikacji udostępnianych przez usługodawcę, zainstalowanych na infrastrukturze wykonawcy.

2. Użytkownik nie dysponuje, co do zasady, żadnymi mechanizmami kontroli ani zarządzania zasobami chmury, takimi jak np. sieć, serwery, systemy operacyjne, etc.

3. Do najpopularniejszych usług z grupy SaaS należą rozwiązania, z którymi użytkownik końcowy ma bezpośredni kontakt, takie jak systemy do obsługi poczty elektronicznej, systemy do zarządzania klientami (CRM), a także narzędzia analityczne[7].

(d) Inne rodzaje usług (Everything as a Service/XaaS), jak np. Business Process as a Service (BPaaS), Billing as a Service (BaaS) czy Analytics as a Service (AaaS).

(9) Poniżej, w formie graficznej, zostało zaprezentowane zestawienie zakresów kontroli nad komponentami infrastruktury informatycznej w poszczególnych modelach świadczenia usług chmurowych, wskazanych w pkt Infrastruktura jako usługa (*Infrastructure as a Service*/IaaS).-Oprogramowanie jako usługa (*Software as a Service*/SaaS). powyżej, w porównaniu z tradycyjnym modelem korzystania z usług IT, tj. modelem *on-premise*.

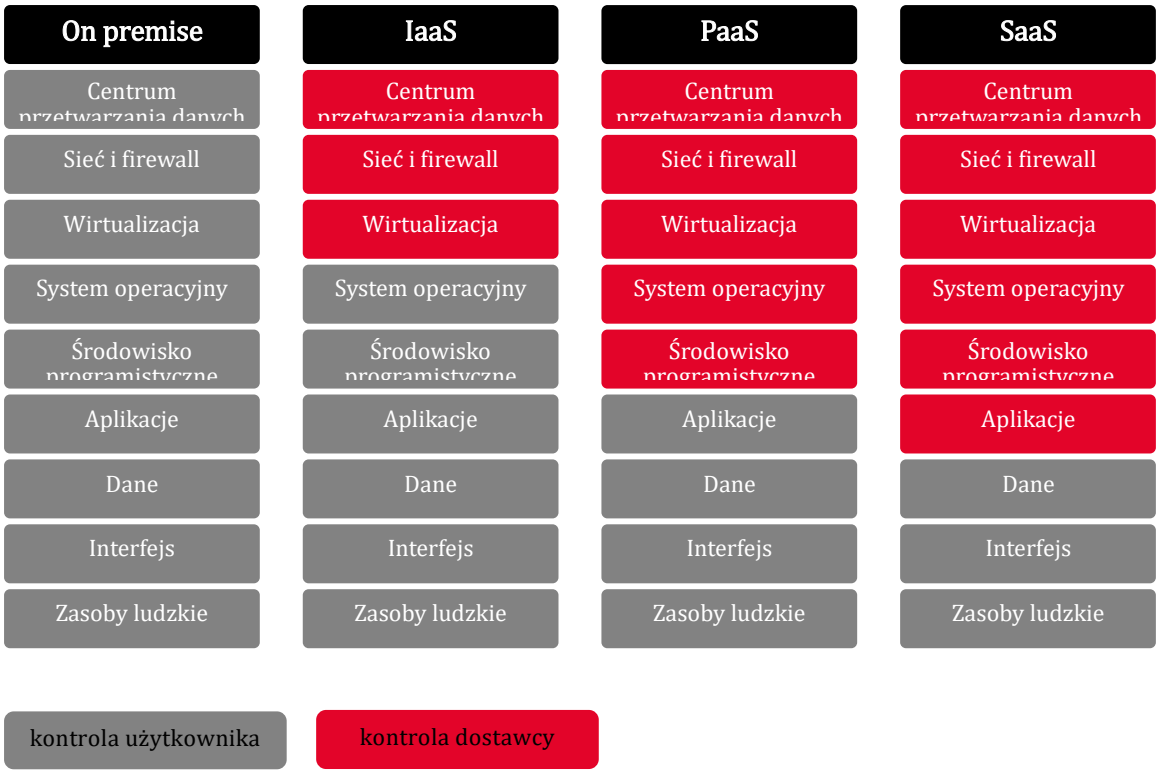
(10)

[7] *Ekspertyza badawcza w przedmiocie wykorzystania usług przetwarzania w chmurze obliczeniowej (cloud computing) w sektorze administracji publicznej (z uwzględnieniem JST) w Polsce*, s. 66.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893




Wykres na podstawie: *Ekspertyza badawcza w przedmiocie wykorzystania usług przetwarzania w chmurze obliczeniowej (cloud computing) w sektorze administracji publicznej (z uwzględnieniem JST) w Polsce*, s. 68.

(11) Powyższa grafika jasno wskazuje, że zakres kontroli podmiotu korzystającego z zasobów IT w przypadku korzystania z usług chmurowych jest niższy niż w przypadku opierania się na rozwiązaniach *on-premise*. Wynika to jednak z natury rozwiązań chmurowych. Współdzielenie zasobów oraz ich alokowanie, pozwalające osiągnąć chmurze optymalne działanie, wymaga możliwości elastycznego, sprawnego i automatycznego zarządzania mocą obliczeniową. Jednakże usługobiorca nie dysponuje nie tylko kontrolą nad zasobami informatycznymi chmury – w przeważającej liczbie przypadków (w zakresie chmury publicznej) usługobiorca nie ma także wiedzy, jak wygląda struktura zasobów IT, gdzie jest zlokalizowana, ani na jakich zasadach funkcjonuje.

(12) Symptomatyczna dla usług chmurowych jest ich „warstwowa" budowa: na jedną udostępnianą w określonym modelu usługę (np. SaaS) składają się usługi z zakresu Paas oraz IaaS, jak ma to miejsce w przypadku m.in. portali społecznościowych. Wówczas podmioty świadczące usługi stanowiące warstwę „niewidoczną" dla klienta końcowego funkcjonują jako poddostawcy względem dostawcy głównej usługi. Przykładu takiego modelu dostarcza aplikacja *Skydox*,



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

która zastała zbudowana na bazie PaaS stworzonej przez Engine Yard, która z kolei korzysta z IaaS dostarczonego przez Amazon. Należy podkreślić, że w sytuacji takiej „warstwowej" usługi chmurowej, umowa o jej świadczenie zawierana jest z dostawcą usługi głównej („widocznej" dla usługobiorcy), a jego poddostawcy nie są w żaden sposób kontraktowo związani z usługobiorcą. Z uwagi na to, korzystanie z tego modelu usług wymaga wzmożonej czujności, zwłaszcza na etapie zawierania kontraktu. Struktura danej usługi rzutuje m.in. na poziom zapewnianego przez nią bezpieczeństwa danych, co ma szczególne znaczenie w przypadku podmiotów administracji publicznej[8].

[Perspektywy związane z rozwojem usług chmurowych]

(13) W chwili obecnej daje się zaobserwować nadzwyczaj dynamiczną ekspansję rozwiązań chmurowych na światowych rynkach. Analitycy przewidują, że w bezpośrednim lub pośrednim związku z nią do 2020 r. zostanie na całym świecie wydane więcej niż bilion dolarów amerykańskich (1.000.000.000.000 $)[9]. Przy czym należy brać pod uwagę, że w związku z rozwojem techniki – przebiegającym niemalże w postępie geometrycznym – chmura może okazać się stadium rozwoju, etapem w drodze do osiągnięcia kolejnych zdobyczy cywilizacyjnych.

(14) Wspominana powyżej ekspansja rynkowa oraz nieustanny rozwój technologii przetwarzania w chmurze jednoznacznie przesądzają o ogromnym potencjale, możliwym do wykorzystania w przypadku zastosowania modelu chmurowego w miejsce tradycyjnego modelu *on-premise*, zarówno przez podmioty prywatne, jak i sektor publiczny.

(15) Chmura wiąże się także z szeregiem ryzyk. Ich rodzaj oraz rozmiar zależą jednak przede wszystkim od modelu usług chmurowych (z rozróżnieniem w szczególności na chmurę prywatną i chmurę publiczną). Wśród technicznych zagrożeń wymienia się uzależnienie świadczenia usług w chmurze od dostępu do Internetu oraz możliwość występowanie problemów z migracją danych.

(16) Istnieje także szereg ryzyk prawnych powiązanych z *cloudem*. Należą do nich w szczególności problemy z zakresu:

(a) poufności i bezpieczeństwa danych (zwłaszcza danych osobowych);

(b) zawierania umów z dostawcami usług i zmieniania ich treści (kontraktowania);

[8] Więcej na ten temat w: C. Millard, *Cloud Computing Law*, Oxford University Press, s. 13 i n.

[9] *Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending*, Gartner 2016.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(c) uzależnienia (całkowitego lub częściowego) od dostawcy usług (tzw. *vendor lock-in*);

(d) integracji z innymi zasobami IT usługobiorcy.

(17) Wskazane wyżej ryzyka zostaną szczegółowo omówione w dalszej części Opinii.

(18) Problematyczna dla usługobiorcy rozwiązań chmurowych jest konieczność sprostania wymogom rozproszonych i nie zawsze jasno ustosunkowanych do *cloud computingu* przepisów prawa – których przegląd również zostanie przedstawiony w dalszej części Opinii.

(19) Niezależnie od powyższego, kluczową i immanentną cechą usług chmurowych (oprócz prywatnej chmury tworzonej przez sam podmiot chcący z niej korzystać lub zbudowanej dla niego w sposób dedykowany przez zewnętrznego dostawcę), mogącą generować ryzyka i niedogodności dla usługobiorcy, jest standaryzacja. Ma ona dwa wymiary: techniczny oraz kontraktowy. W tym pierwszym, charakterystycznym zwłaszcza dla chmury publicznej, polega na możliwości korzystania z takiego pakietu i standardu usług, jaki oferuje dostawca dla szerokiego grona klientów, z brakiem możliwości lub niewielką możliwością dostosowania ich do indywidualnych potrzeb usługobiorcy. Należy jednak dostrzec zalety takiego modelu. Tylko dzięki daleko idącemu ujednoliceniu typu świadczonych usług możliwe jest sprawne alokowanie zasobów, tanie i szybkie usuwanie błędów, czy wreszcie – oferowanie rozwiązań w atrakcyjnych cenach. Drugim aspektem standaryzacji chmury jest powiązany z nią, wspomniany już wyżej model kontraktowania: oparty na umowach adhezyjnych (zawieranych przez przystąpienie), referujących do zewnętrznych regulaminów – w którym prawa i obowiązki stron są *de facto* narzucone przez dostawcę. Zagadnienie to zostanie szerzej poruszone w dalszej części Opinii. Przyczyn takiej postawy dostawców chmury można upatrywać co prawda niewątpliwie w ich silnej pozycji rynkowej, ale nie można ich do niej zawężać. Występują wśród nich także pewne racjonalne podstawy ekonomiczne: tylko wystandaryzowana polityka kontraktowania, bez stosowania odstępstw dla klientów, pozwala osiągnąć standaryzację usług w rozumieniu technicznym – i korzyści z niej wynikające.

(20)



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

# IV. CHMURA W SEKTORZE PUBLICZNYM NA ŚWIECIE

(1) Chmura obliczeniowa jako rozwiązanie stosunkowo nowe, jednak odnoszące ogromne sukcesy w sektorze prywatnym, została dostrzeżona także przez sektor publiczny, który pomimo ograniczonej elastyczności działania oraz co do zasady szerszego zakresu wymagań związanych m.in. z bezpieczeństwem danych, systematycznie implementuje *clouda* jako niosącą wiele korzyści alternatywę dla rozwiązań *on-premise*. Zainteresowanie to odzwierciedlają sporządzane przez organizacje międzynarodowe analizy i raporty dotyczące funkcjonowania rozwiązań chmurowych wśród instytucji administracji publicznej, stanowiące odpowiedź na rosnące zapotrzebowanie na produkty chmurowe wśród tego typu podmiotów. Spośród nich na wyróżnienie zasługują materiały opracowane przez European Union Agency for Network and Information Security (ENISA), takie jak m.in. *Cloud Computing Risk Assessment (2009)*[10], *Security and Resilience in Governmental Clouds (2011)*[11], *Good Practices for Governmental Clouds (2013)*[12] oraz *Security Framework for Governmental Clouds (2014)*[13].

(2) Poniżej krótko zaprezentowano stan implementacji rozwiązań chmurowych w krajach wyselekcjonowanych z uwagi na wysoki poziom rozwoju technologii informacyjnej w sektorze publicznym, który reprezentują, w tym także w zakresie stosowanych rozwiązań *cloudowych*. Wybrano dwa kraje należące do Unii Europejskiej, przynależące do grupy **Digital 5**, oraz Stany Zjednoczone, które reprezentują diametralnie odmienny system prawny niż prawo stosowane w państwach członkowskich Unii Europejskiej, jednak w wielu obszarach są inicjatorami nowoczesnych rozwiązań cyfrowych, pozostają równorzędnym partnerem w międzynarodowej współpracy w zakresie informatyzacji administracji publicznej (np. uczestniczą w pracach grupy roboczej, zrzeszającej poza Stanami Zjednoczonymi także Kanadę, Australię,

[10] Materiał dostępny w wersji elektronicznej na stronie: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[11] Materiał dostępny w wersji elektronicznej na stronie: https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds

[12] Materiał dostępny w wersji elektronicznej na stronie: httpshttps://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds

[13] Materiał dostępny w wersji elektronicznej na stronie: https://www.enisa.europa.eu/publications/security-framework-for-govenmental-clouds



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

Danię, Izrael, Meksyk, Japonię, Nową Zelandię oraz Wielką Brytanię, dotyczących tzw. *International Identity*).

[Estonia]

(3) Estonia to jeden z niekwestionowanych liderów w zakresie implementacji nowoczesnych technologii w administracji publicznej na świecie. Powszechnie wskazuje się, że pod względem bezpośrednich korzyści dla obywateli estońskich system tzw. e-administracji jest obecnie prawdopodobnie najnowocześniejszym i najbardziej kompleksowo obsługującym obywateli rozwiązaniem w Unii Europejskiej[14].

(4) Szeroki wachlarz zróżnicowanych e-usług oferowanych przez system stworzony w ramach inicjatywy **e-Estonia** umożliwia realizację podstawowych praw i obowiązków obywatelskich, przedsiębiorczości oraz zdrowia. Wśród nich wskazać można rozwiązania takie jak e-Voting, e-Tax, e-Business Register, e-Prescription, Electronic Health Record, e-Police, e-Court czy e-Cabinet.

(5) Powyższe wyliczenie ma jedynie przykładowy charakter[15]. Program e-Estonia, oprócz rozwiązań dostępnych przez wyszukiwarkę internetową, obejmuje również szereg aplikacji mobilnych, mających na celu dalsze rozpowszechnienie korzystania z usług dostarczanych drogą elektroniczną wśród obywateli.

(6) Program estoński został skonstruowany za pomocą komplementarnych, umożliwiających płynną integrację modułów. Dzięki tym cechom całość może być poddawana nieustannym aktualizacjom w celu elastycznego dostosowywania usług do wyłaniających się na bieżąco potrzeb społeczeństwa informacyjnego.

(7) Jednym z podstawowych elementów estońskiego systemu e-administracji jest uruchomione w 2001 r. rozwiązanie **X-Road**. Narzędzie to łączy usługi oraz bazy danych w sektorze publicznym i prywatnym, umożliwiając ich integrację oraz interakcję w celu świadczenia usług dostępnych w ramach portalu e-Estonia, będąc odpowiednikiem rozwiązania brytyjskiego pod nazwą *Government Secure Intranet* (GSI).

(8) Pierwotnie rozwiązanie X-Road miało służyć głównie jako środowisko umożliwiające przeszukiwanie dostępnych baz danych. Obecnie stanowi ono

[14] Więcej informacji dostępne na oficjalnej stronie portalu: https://e-estonia.com w tym dane statystyczne dostępne na stronie: https://e-estonia.com/facts/ oraz w ramach raportu EU eGovernment 2016 dostępnego na stronie: https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016-shows-online-public-services-improved-unevenly

[15] Pełna informacja dotycząca oferowanych w ramach e-Estonia serwisów dostępna jest na stronie: https://e-estonia.com/components/



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

kluczowy element decentralizujący główne estońskie bazy danych, umożliwiający dostęp do nich przez wszystkie podmioty administracji publicznej. Dzięki możliwości szybkiej multiplikacji baz danych, przesyłania ogromnych zestawów danych oraz bieżącego dodawania nowych informacji, X-Road stanowi narzędzie niezbędne do tworzenia nowych rozwiązań. Obecnie każda z e-usług dostępnych na portalu e-Estonia korzysta z rozwiązania X-Road, które, oprócz wyżej opisanych walorów funkcjonalnych, jest rozwiązaniem zapewniającym bezpieczeństwo danych poprzez szyfrowanie danych archiwizowanych, a także poprzez każdorazowe uwierzytelnianie i rejestrowanie danych wchodzących do systemu.

(9) Obecnie szacuje się, że ponad 50% mieszkańców Estonii korzysta z X-Road poprzez portal eesti.ee. Wielokrotnie podkreślano, że to właśnie umiejętność sprawnej archiwizacji oraz segregacji dużych zasobów kluczowych dla Estonii danych przesądziła o sukcesie projektu digitalizacji administracji publicznej w ramach programu e-Estonia. Zostało to dostrzeżone przez inne kraje takie jak np. Finlandia, gdzie również podjęto próby zastosowania systemu X-Road w celu wymiany plików pomiędzy podmiotami administracji publicznej[16].

[Stany Zjednoczone]

(10) Stany Zjednoczone należą do grona krajów, które dość wcześnie zaczęły budować fundamenty społeczeństwa informacyjnego i obecnie, pomimo tego, że nie należą do grupy Digital 5, mogą pochwalić się szeregiem rozwiązań dorównujących tym stosowanym w Europie i Azji. Od czasu zaanonsowania przez prezydenta Baracka Obamę strategii ***Cloud First*** w lutym 2011 roku, podmioty administracji publicznej zaczęły dostrzegać walory rozwiązań chmurowych i postrzegać je jako alternatywę dla stosowanych wcześniej rozwiązań *on-premise.* Co ciekawe, Stany Zjednoczone są postrzegane jako swoisty fenomen z racji na to, że zainteresowanie rozwiązaniami chmurowymi, zgłaszane przez podmioty administracji publicznej, jest często oceniane jako większe niż to ze strony sektora prywatnego[17].

(11) Jednym z rozwiązań, które miały kluczowy wpływ na rozbudzenie zainteresowania i zbudowanie zaufania podmiotów publicznych do *clouda*, jest uruchomiona przez rząd federalny platforma zakupowa Apps.gov. Ma ona na

[16] McKinsey, *Digital by default: A guide to transforming government.*

[17] http://fortune.com/2016/09/02/us-government-embraces-cloud/



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

celu ułatwienie procesu zamawiania usług chmurowych, przy jednoczesnym obniżeniu kosztów pozyskiwania tych usług przez agencje federalne, a także skróceniu czasu trwania procedury zamówieniowej[18].

(12) Platforma zakupowa zrzesza dostawców usług chmurowych zatwierdzonych wcześniej przez General Services Administration (GSA). Na stronie portalu Apps.gov znajduje się regularnie aktualizowany katalog usług, które są dostępne dla agencji federalnych. Głównymi celami, przyświecającymi wdrożeniu platformy zakupowej w Stanach Zjednoczonych, było zwiększenie wydajności operacyjnej oraz optymalizacja korzystania z rozwiązań IT przez jednostki administracji publicznej.

(13) Jednym ze stosowanych w Stanach Zjednoczonych systemów oceny oraz autoryzacji usług chmurowym pod kątem bezpieczeństwa ich stosowania przez administrację publiczną jest **FedRAMP** (*Federal Risk and Authorization Management Program*). Do nadrzędnych celów tego programu zalicza się m.in.:

(a) zwiększenie zaufania do usług chmurowych, w tym w szczególności zbudowanie przekonania o wystarczającym poziomie bezpieczeństwa zapewnianego przez zweryfikowane usługi bezpieczeństwa;

(b) przyspieszenie zastosowania rekomendowanych bezpiecznych rozwiązań chmurowych;

(c) zbudowanie przejrzystego, jednolitego modelu weryfikacji usług chmurowych w zakresie bezpieczeństwa;

(d) zapewnienie stosowania przyjętych zasad oraz standardów w zakresie bezpieczeństwa usług chmurowych[19].

(14) Usługi chmurowe, które z sukcesem przeszły przez weryfikację prowadzoną w ramach systemu FedRAMP uznawane są za gwarantujące należyty poziom zabezpieczeń wymaganych w przypadku stosowania ich przez jednostki administracji publicznej, zatem znajduje on zastosowanie w ramach weryfikacji usług chmurowych na potrzeby włączenia ich do katalogu usług oferowanych na platformie Apps.gov. Platforma ta stale się rozwija, co stanowi odzwierciedlenie rosnącego zainteresowania usługami chmurowymi wśród podmiotów administracji publicznej w Stanach Zjednoczonych.

[Wielka Brytania]

[18] Dostęp do platformy pod adresem: https://apps.gov/

[19] Więcej informacji na oficjalne stronie programu FedRAMP pod adresem: https://www.fedramp.gov/about-us/about/



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(15) Wielka Brytania, obok Estonii, należy do najbardziej rozwiniętych technologicznie krajów Europy. Wszelkie inicjatywy dotyczące społeczeństwa informacyjnego, w tym strony internetowe poszczególnych ministerstw oraz oferowane przez administrację publiczną e-usługi, dostępne są na platformie **Gov.uk**.

(16) Począwszy od roku 2014 celem Wlk. Brytanii była jak najszybsza digitalizacja najbardziej popularnych usług świadczonych przez administrację publiczną. Obok usług koncentrujących się na obsłudze obywateli, Wlk. Brytania podjęła intensywne działania na rzecz optymalizacji funkcjonowania administracji publicznej jako takiej, w tym zarządzania infrastrukturą IT. Jednym z przejawów zmiany w podejściu do technologii cyfrowej były działania podjęte przez rząd, obejmujące wprowadzenie inicjatyw takich jak:

(a) ***Government as a platform*** – rozwiązanie mające na celu ułatwienie tworzenia rozwiązań informatycznych przez administrację publiczną[20]; oraz

(b) ***Cloud First*** - wytyczna przyjęta przez rząd w 2013 roku, nakierowana na zmotywowanie podmiotów administracji publicznej do korzystania z rozwiązań chmurowych, w tym przede wszystkim z chmury publicznej[21].

(17) Jednym z najbardziej przełomowych i skutecznych rozwiązań brytyjskich, dotyczących optymalizacji funkcjonowania administracji publicznej w zakresie nowoczesnych technologii oraz zmniejszenia nakładów na infrastrukturę IT, jest **Digital Marketplace**. To portal służący do realizacji zamówień na usługi, w tym usługi chmurowe, przez jednostki administracji publicznej oraz wybrane jednostki spoza administracji. Zamówienia te realizowane są na podstawie zawartych z usługodawcami umów ramowych na usługi, w tym m.in. usługi chmurowe w ramach modelu G-Cloud. Rozwiązanie to zostało zaprezentowane w marcu 2011 roku w opublikowanym przez rząd brytyjski dokumencie kierunkowym pt. *Government Cloud Strategy*[22], a następnie z sukcesem udostępnione uprawnionym użytkownikom w lutym 2012 roku.

[20] Więcej informacji na stronie: https://www.gov.uk/government/policies/government-as-a-platform

[21] Więcej informacji dostępne na stronie: https://www.gov.uk/guidance/government-cloud-first-policy

[22] Pełna wersja dokumentu dostępna pod adresem: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

# V. RYZYKA PRAWNE ZWIĄZANE Z USŁUGAMI CHMUROWYMI

[Model kontraktowania]

(1) Kontrakty na usługi chmurowe mają specyficzny charakter – są zazwyczaj sformułowane dość lakonicznie, w zakresie większości zagadnień istotnych dla usług odsyłając do regulaminów przygotowywanych jednostronnie przez dostawcę chmury (które w trakcie obowiązywania umowy mogą na dodatek podlegać – i w praktyce często podlegają – zmianom). Co więcej, silna pozycja rynkowa dostawców oraz charakter usług chmurowych powodują, że treść zobowiązań z kontraktów chmurowych często przedstawia się łagodnie dla dostawcy – i niemal zawsze podlega negocjacjom w niewielkim zakresie.

(2) Jak było wspomniane wyżej, standaryzacja postanowień kontraktowych (tj. oferowanie przez dostawcę jednolitych warunków wszystkim jego klientom) oraz oparcie ich na regulaminach jest charakterystyczną cechą dla umów w zakresie *cloud computingu* – determinowaną cechami samych usług. Gdyby zobowiązania dostawcy różniły się wobec różnych klientów, nie mógłby świadczyć wobec nich usług w jednakowy, zautomatyzowany sposób. Negatywnym skutkiem takiego stanu rzeczy jest niewielki zakres, w jakim klient realnie może wynegocjować ustępstwa lub szczególne warunki świadczenia usług ze strony dostawcy. Nie jest odosobnionym przypadkiem, że jedyną decyzją, jaką klient może podjąć w stosunku do umowy dotyczącej *cloud computingu* jest jej zawarcie lub nie. Taki rodzaj kontraktów określa się mianem adhezyjnych – tzn. zawieranych przez przystąpienie. Z kolei opieranie przeważającej części rzeczywistej treści umów na regulaminach jest podyktowane „ekonomią" kontraktową – założeniem chmury jest jej ciągłe rozwijanie i modyfikowanie przez dostawcę (na co usługobiorca nie ma wpływu) – w związku z tym, ewoluować może w pewnych wypadkach treść zobowiązań łączących dostawców z ich klientami. Częste aneksowanie umów z wieloma rozproszonymi klientami generowałoby znaczne trudności i koszty – tymczasem w większości krajów prawo ustanawia łatwiejszy tryb dokonywania zmian w regulaminach.

(3) Polski ustawodawca przewidział określone rygory związane z zawieraniem umów z podmiotami narzucającymi przygotowane przez siebie warunki



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

w regulaminach (wzorach umów). Art. 384 § 1 k.c. stanowi, że ustalony przez jedną ze stron wzorzec umowy wiąże drugą stronę, jeśli został jej doręczony przed zawarciem umowy. Natomiast jeśli umowa odwołuje się do wzorca w formie elektronicznej, to zgodnie z art. 384 § 4 k.c., wzorzec ten powinien zostać udostępniony drugiej stronie przed zawarciem umowy w taki sposób, aby mogła go ona przechowywać i odtwarzać w zwykłym toku czynności (to kryterium spełnia np., wysłanie pliku w formacie .pdf). Celem wskazanych przepisów jest umożliwienie podmiotowi przystępującemu do zawarcia umowy adhezyjnej, referującej do wzorca umownego, dokładne zapoznanie się z tym wzorcem. W tym miejscu należy dodać, że art. 385 § 1 k.c. przewiduje, że w razie sprzeczności treści umowy z wzorcem umowy strony są związane umową. Ponadto sam regulamin (wzorzec umowny), dotyczący usług chmurowych, powinien spełniać warunki przewidziane w ustawie o świadczeniu usług drogą elektroniczną, które zostały opisane w punktach Art. 8 ust. 1 u.ś.u.d.e. nakłada na usługodawcę obowiązek określenia regulaminu świadczenia usług drogą elektroniczną (pkt 1) oraz obowiązek jego nieodpłatnego udostępnienia usługobiorcy przed zawarciem umowy o świadczenie usług (pkt 2). Przepis ten ponadto wskazuje, że udostępnienie regulaminu powinno nastąpić w sposób umożliwiający pozyskanie, odtwarzanie i utrwalanie jego treści za pomocą systemu teleinformatycznego, którym posługuje się usługobiorca. Art. 8 ust. 2 u.ś.u.d.e. przewiduje, że usługobiorca nie jest związany postanowieniami regulaminu, które nie zostały mu udostępnione w sposób opisany powyżej. oraz Art. 8 ust. 3 u.ś.u.d.e. wymienia elementy, które musi zawsze zawierać regulamin świadczenia usług drogą elektroniczną (używając zwrotu „w szczególności", co oznacza, że w przedmiotowym przepisie mamy do czynienia z katalogiem otwartym). Elementy te to określenie: rodzaju i zakresu usług świadczonych drogą elektroniczną, warunki ich świadczenia (w tym niezbędne wymagania techniczne i zakaz dostarczania przez usługobiorcę treści o charakterze bezprawnym), warunki zawierania i rozwiązywania umowy o świadczenie usług drogą elektroniczną oraz tryb postępowania reklamacyjnego. poniżej.

(4) Kodeks cywilny przewiduje także szczególny tryb związany ze zmianą regulaminu w trakcie realizacji umowy o charakterze ciągłym (jaką jest umowa dotycząca usług w chmurze). Zgodnie z art. $384^1$ k.c., wzorzec wydany w czasie trwania stosunku umownego o charakterze ciągłym wiąże drugą stronę, jeżeli zostały zachowane wymagania określone w art. 384 k.c., a strona nie wypowiedziała umowy w najbliższym terminie wypowiedzenia. Z regulacji tej wynika, że jeśli dostawca będzie chciał zmienić regulamin w trakcie świadczenia usług, powinien przedstawić go odpowiednio (doręczając w sposób wynikający



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

z art. 384 k.c., opisany powyżej) usługobiorcy. W świetle polskiego prawa usługobiorca nie może być związany postanowieniami regulaminu, które nie zostały mu przedstawione. Natomiast w przypadku właściwego dostarczenia nowego wzorca, usługobiorca staje przed wyborem: zaakceptowania regulaminu – wówczas nowy regulamin jest wiążący (natomiast wśród doktryny prawniczej sporne jest, czy od chwili doręczenia[23] wzorca, czy od bezskutecznego upływu okresu wypowiedzenia[24] – zdaniem autorów Opinii, słuszne jest drugie ze wskazanych stanowisk), albo jego niezaakceptowania – co wymaga jednak rezygnacji z usług i wypowiedzenia umowy w najbliższym terminie wypowiedzenia. Przy czym, jeśli umowa nie określa terminów wypowiedzenia, usługobiorca nieakceptujący regulaminu powinien go wypowiedzieć niezwłocznie – tj. w czasie niezbędnym do namysłu, *biorąc pod uwagę obszerność wzorca oraz zakres i wagę dokonywanych zmian*[25].

[Poufność]

(5) Dla podmiotów z kręgu administracji publicznej, zamierzających korzystać z usług chmurowych, zapewnienie sobie jak najwyższego standardu ochrony informacji poufnych w ramach umowy jest daleko ważniejsze niż dla podmiotów z rynku prywatnego. Te ostatnie, w przypadku „niedoborów" w ramach kontraktowej regulacji poufności, mogą liczyć na ochronę udzielaną przez przepisy ustawy o zwalczaniu nieuczciwej konkurencji – w szczególności jej art. 11 ust. 1 – statuujący czyn nieuczciwej konkurencji, jakim jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej (według art. 11 ust. 4 u.z.n.k. przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności). Jednakże przepisy ustawy o zwalczaniu nieuczciwej konkurencji, w tym jej art. 11, stosuje się wyłącznie do przedsiębiorców w rozumieniu art. 2 u.z.n.k. – tj. osób fizycznych, osób prawnych oraz jednostek organizacyjnych niemających osobowości prawnej, które prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową, uczestniczą w działalności

[23] Tak K. Zagrobelny [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, Warszawa 2016, s. 705.

[24] Tak Sąd Najwyższy w wyroku z dnia 18 grudnia 2002 r., IV CKN 1616/00, LEX.

[25] A. Olejniczak [w:] A. Kidyba (red.), *Kodeks cywilny. Komentarz. Tom III. Zobowiązania - część ogólna*, pkt 7 komentarza do art. $384^1$ k.c., LEX.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

gospodarczej. Większość jednostek administracji rządowej nie można uznać za przedsiębiorców we wskazanym wyżej znaczeniu[26]. Równocześnie zastrzegamy, że w Opinii nie dokonujemy oceny wpływu ustawy o dostępie do informacji publicznej na poufność informacji należących do jednostek administracji publicznej.

(6) Z uwagi na powyższe szczególnego znaczenia nabiera porozumienie o zachowaniu poufności (ang. *Non-Disclosure Agreement*, w skrócie: NDA) – które należy zawrzeć w ramach umowy o świadczenie usług chmurowych. Jego brak lub niepełność może prowadzić do znaczących strat. Jest to zagadnienie tym istotniejsze, że udostępniając swoje poufne informacje do chmury, usługobiorca nie będzie miał nad nią kontroli, ani najpewniej nawet wiedzy o jej strukturze, zasadach działania, zasadach dostępu do niej i lokalizacji jej infrastruktury.

(7) Kluczowe dla NDA jest przede wszystkim określenie jego przedmiotu – czyli zdefiniowanie informacji poufnych. Z punktu widzenia usługobiorcy, powinno to być jak najszersze pojęcie – obejmujące, w miarę możliwości, wszelkie dane *uploadowane* do chmury. Usługobiorca powinien zobowiązać się do zachowania takich danych w poufności, tj. nieudostępniania ich podmiotom trzecim (z uwzględnieniem pewnych wyjątków, takich jak zatrudnione u usługobiorcy osoby) oraz do niewykorzystywania ich w innym celu niż do realizacji umowy. Usługobiorca powinien też dążyć do zapewnienia przez usługodawcę, że jego informacje poufne nie będą powielane w szerszym zakresie, niż jest to konieczne dla realizacji umowy, oraz że będą zabezpieczone technicznie przed dostępem niepowołanych osób.

(8) Dla zabezpieczenia interesów usługobiorcy koniecznie jest także uregulowanie skutków wygaśnięcia umowy o świadczenie usług chmurowych (z jakichkolwiek przyczyn) wobec informacji poufnych. Usługobiorca dąży do zobowiązania się przez usługodawcę, że jego dane zostaną niezwłocznie i w całości usunięte z zasobów usługobiorcy.

(9) W miarę możliwości usługobiorca powinien również negocjować kwestię limitu odpowiedzialności w kontekście poufności – z uwagi na rozmiar szkód, jakie mogą powstać dla niego w związku z naruszeniem zobowiązania do poufności przez usługobiorcę. Optymalnie byłoby w ogóle wyłączenie szkód spowodowanych naruszeniem NDA spod limitu. W przypadku braku takiej możliwości, należałoby dążyć do ustanowienia w tym obszarze jak najwyższego poziomu ograniczenia.

[26] Za przedsiębiorców można uznać za to z pewnością niektóre podmioty publiczne: m.in. spółki skarbu państwa, czy chociażby jednostki samorządu terytorialnego. Zob. np. wyrok Sądu Najwyższego z dnia 9.8.2012 r., V CSK 366/11, Legalis.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(10) Ostatnią istotną kwestią, dotyczącą poufności, jest czas jej obowiązywania. Usługobiorca powinien go zapewnić przez okres trwania umowy oraz odpowiednio długi czas po jej wygaśnięciu. Ten drugi aspekt wymaga szczególnej uwagi – z powodu prawnego charakteru NDA jako umowy ciągłej. Umowy ciągłe wygasają z upływem terminu, na jaki zastały zawarte, a jeśli zostały zawarte na czas nieoznaczony (bezterminowo), to zgodnie z art. $365^1$ k.c., wygasają po dokonaniu wypowiedzenia. Przy czym, co wynika ze wspomnianego wyżej przepisu, jeśli strony nie ustaliły okresu wypowiedzenia, umowa wygaśnie niezwłocznie po wypowiedzeniu. Prowadzi to do wniosku, że proste sformułowanie postanowienia typu „dostawca jest zobowiązany do zachowania poufności także po wygaśnięciu umowy" nie zabezpiecza usługobiorcy – dostawca będzie mógł doprowadzić do wygaśnięcia zobowiązania do poufności poprzez złożenie oświadczenia o wypowiedzeniu. Koniecznie jest zatem albo wskazanie terminu po wygaśnięciu umowy, w którym będzie obowiązywać NDA (wówczas nie będzie możliwe wcześniejsze jego wypowiedzenie), albo zawarcie NDA na czas nieoznaczony – ale ze wskazaniem odpowiednio długich terminów wypowiedzenia zabezpieczających przed nagłą możliwością zwolnienia się z odpowiedzialności za informacje poufne.

[Dane osobowe]

(11) Jako że dnia 27 kwietnia 2016 r. opublikowano Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[27], które osiągnie pełną skuteczność dnia 25 maja 2018, uchylając jednocześnie Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dalej zwaną „Dyrektywą"), na potrzeby niniejszej Opinii analizowany będzie stan prawny obowiązujący na podstawie RODO, natomiast wszelkie odwołania do Dyrektywy czy też polskiej Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922; dalej

[27] Pełny tekst aktu prawnego dostępny na stronie: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

zwanej „UODO") będą miały na celu jedynie pokazanie najistotniejszych z punktu widzenia dostawcy usług chmurowych różnic wprowadzonych przez prawodawcę unijnego w nowym akcie.

(12) Należy podkreślić, że zmiany, wprowadzone przez Rozporządzenie w zakresie ochrony praw podmiotów danych osobowych, mają charakter przełomowy i fundamentalny. Z racji na mający miejsce w czasie ostatnich 20 lat bezprecedensowy rozwój technologii informatycznej powstała potrzeba stworzenia nowego systemu ochrony danych osobowych osób fizycznych, których prawa nie były do tej pory należycie respektowane z racji na brak odpowiednich instrumentów prawnych gwarantujących ich skuteczną ochronę na podstawie dotychczasowych regulacji. Jako że zakres zmian jest niezwykle szeroki, wprowadzono dwuletni okres dostosowawczy przed osiągnięciem jego pełnej skuteczności, aby jednostki organizacyjne przetwarzające dane osobowe miały odpowiednią ilość czasu na zaplanowanie działań, a następnie wdrożenie koniecznych zmian w ich funkcjonowaniu.

(13) Zgodnie z treścią RODO, od 25 maja 2018 r. podmioty przetwarzające dane osobowe osób przebywających w Unii Europejskiej (dalej zwanej „UE") w związku z (i) oferowaniem towarów lub usług w UE, albo (ii) monitorowaniem ich zachowania, są zobowiązane do stosowania się do przepisów Rozporządzenia (Art. 3 ust. 1 oraz 2 RODO). Warto w tym miejscu zaznaczyć, że prawodawca wprost wskazał (Art. 3 ust. 1), że obowiązkami związanymi z przetwarzaniem danych osobowych objęci są zarówno administratorzy danych, jak i podmioty przetwarzające te dane w imieniu ich administratorów, co stanowi długo oczekiwane i wielokrotnie postulowane rozszerzenie kręgu pomiotów ponoszących indywidualną odpowiedzialność za ochronę danych osobowych[28].

(14) Punktem wyjścia dla niniejszej analizy powinno być stwierdzenie, że usługodawca świadczący usługi chmurowe, któremu usługobiorca powierza dane do przetwarzania, w tym dane osobowe osób przebywając w UE, pełni w świetle zarówno UODO, jak i RODO rolę podmiotu przetwarzającego dane. Zakres jego obowiązków związanych, związanych z ochroną danych i powierzonych mu do przetwarzania przez administratora, które zostały na niego nałożone w ramach Rozporządzenia, jest diametralnie szerszy, co zostanie opisane szczegółowo w dalszej części Opinii.

---

28 Dla porównania, w świetle Dyrektywy oraz UODO podmiotem, który ponosi znaczącą część odpowiedzialności za naruszenia związane z ochroną danych osobowych, jest administrator tych danych, podczas gdy odpowiedzialność podmiotów przetwarzających dane osobowe, powierzone im przez administratora, jest bardzo ograniczona. Prawodawca słusznie dostrzegł konieczność wprowadzenia równowagi w zakresie zakresu obowiązków obu grup podmiotów, co motywowane było koniecznością zdecydowanego podniesienia poziomu ochrony danych osobowych osób fizycznych, obecnie masowo przetwarzanych z zastosowaniem nowoczesnych technologii, niezależnie od charakteru działalności danego podmiotu.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(15) Co do zasady, RODO nie wprowadza nowych instytucji dotyczących konkretnie rozwiązań chmurowych. Jednak z racji na rozszerzenie zakresu podmiotów objętych wprost tym aktem prawnym, dostawcy usług chmurowych zmuszeni są do wypełniania szeregu obowiązków, które do tej pory dotyczyły głównie administratorów. Co więcej, nieprzestrzeganie ich obłożone zostało sankcjami, w tym w szczególności dotkliwą karą finansową, której wysokość sięgać może do 20 milionów euro lub 4% całkowitego, globalnego obrotu osiągniętego przez organizację w poprzednim roku obrotowym. Ma to na celu zmotywowanie podmiotów do zmiany podejścia do kwestii dotyczących ochrony danych osobowych, które dotychczas były często rażąco lekceważone, doprowadzając do niekontrolowanego przetwarzania oraz licznych wycieków tych danych ze szkodą dla osób fizycznych będących ich podmiotami.

(16) Obowiązki podmiotów przetwarzających dane osobowe na rzecz ich administratorów zostały zbiorczo uregulowane w Art. 28 RODO, jednak nie ogranicza to zastosowania innych jego przepisów, które dotyczą zarówno administratorów, jak i podmiotów przetwarzających dane w jego imieniu (m.in. kwestii dotyczących transferów danych osobowych do państw trzecich lub organizacji międzynarodowych, uregulowanych w Rozdziale V RODO). Poniżej przedstawione zostanie podsumowanie najważniejszych zagadnień dotyczących wymagań w stosunku do podmiotów przetwarzających dane na rzecz administratorów, w tym dostawców usług chmurowych.

(17) Zgodnie z treścią RODO, podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania **odpowiednich środków organizacyjnych i technicznych**. Celem wprowadzenia tego wymogu jest zapewnienie bezpieczeństwa danych osobowych oraz realizacja praw podmiotów tych danych. Takim środkiem może być np. pseudonimizacja lub szyfrowanie, jednak jest to jeden z przykładów środków wskazanych jako możliwe lub rekomendowane do zastosowania przez podmioty przetwarzające dane osobowe, a nie wymóg sformułowany wprost w rozporządzeniu.

(18) W związku z korzystaniem przez dostawców usług chmurowych z usług **podwykonawców**, co stało się obecnie nagminną praktyką, chociażby z racji uwarunkowań konstrukcyjnych tych rozwiązań (tzw. warstwowość), Rozporządzenie wprowadza zakaz korzystania z usług osób trzecich, które miałyby przetwarzać dane osobowe powierzone dostawcom przez administratorów bez ich uprzedniej pisemnej zgody (zgoda ogólna lub szczegółowa). W przypadku zgody ogólnej, dostawca jest uprawniony do podpowierzania danych osobowych do przetwarzania podmiotom zewnętrznym, które zostały przez administratora zaakceptowane. Mogą one



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

być wskazane np. w postaci listy podwykonawców, zawartej w treści umowy o świadczenie usług chmurowych, zawartej między administratorem danych a dostawcą usług chmurowych, przy czym w takim przypadku dostawca jest dodatkowo zobowiązany do informowania z wyprzedzeniem o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia podwykonawców figurujących na tej liście, co umożliwi administratorowi wyrażenie sprzeciwu wobec takich zmian. Z kolei zgoda szczegółowa dotyczy jednostkowego przypadku zakontraktowania podwykonawcy przez dostawcę.

(19) Kolejną kwestią, związaną z korzystaniem z usług osób trzecich przez dostawców usług chmurowych, jest **obowiązek nałożenia na tychże podwykonawców tych samych obowiązków w zakresie ochrony danych**, jakie obejmują dostawcę na podstawie zawartej przez niego z administratorem umowy. Dotychczas administrator danych kontrolował obszar ochrony danych osobowych jedynie w zakresie stosunku prawnego istniejące między nim a bezpośrednim dostawcą, co w przypadku udzielenie zgody na podpowierzenie danych osobowych do przetwarzania osobom trzecim przekładało się na możliwość wystąpienia wysokiego ryzyka zagrożeń dla bezpieczeństwa tych danych z racji na niekompatybilność standardów administratora z działaniami podejmowanymi przez osoby trzecie, zakontraktowane przez dostawcę usług jako podwykonawcy.

(20) Rozporządzenie podtrzymuje wyprowadzony w Dyrektywie obowiązek zawierania przez administratorów **umów powierzenia przetwarzania danych z podmiotami przetwarzającymi**, jednocześnie rozbudowując oraz konkretyzując wymogi, jakie musi ona spełniać. Wśród najważniejszych wskazać należy określenie przedmiotu i czasu przetwarzania danych osobowych, ich rodzaju oraz charakteru, a także celu ich przetwarzania. Umowa taka powinna również określać możliwie szczegółowo obowiązki i prawa administratora oraz dostawcy, w tym m.in.:

(a) obowiązek przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora;

(b) wymóg złożenia oświadczeń o zachowaniu danych w tajemnicy przez osoby upoważnione do przetwarzania przez dostawcę;

(c) obowiązek zastosowania środków zapewniających bezpieczeństwo (o ile nie zostały opisane szerzej w innej umowie lub części umowy z dostawcą);

(d) obowiązek udzielania pomocy w wywiązywaniu się przez administratora z obowiązków wobec podmiotów danych osobowych,



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(e) obowiązek udzielania pomocy w wywiązywaniu się przez administratora z obowiązków związanych z przeprowadzaniem **oceny skutków przetwarzania danych** (DPIA) oraz obowiązków opisanych w art. 32 – 36 (np. obowiązki notyfikacyjne).

(21) Idąc dalej, zgodnie z treścią RODO dostawca usług chmurowych zobowiązany jest do **usunięcia lub zwrotu danych osobowych po zakończeniu świadczenia usług** (zgodnie z decyzją administratora), chyba że prawo UE lub państwa członkowskiego nakazują ich przechowywanie. Daje to administratorom gwarancję, że powierzone dostawcom w celu realizacji umowy o świadczenie usług chmurowych dane nie będą po zakończeniu okresu jej trwania przechowywane przez niego bez wiedzy oraz kontroli administratora.

(22) Kolejnym wymogiem wobec dostawców, który bez wątpienia wychodzi naprzeciw sygnalizowanym w czasie prac nad treścią Rozporządzenia potrzebom rynku, jest **obowiązek dostarczenia administratorowi informacji niezbędnych do wypełniania przez niego obowiązków** w zakresie ochrony danych oraz **umożliwienie przeprowadzanie przez administratora audytu** w zakresie przestrzegania zasad przetwarzania danych osobowych przez dostawcę.

(23) Kwestią budzącą wiele kontrowersji i niejasności zarówno w świetle Dyrektywy, jak i RODO, a jednocześnie niezwykle istotną dla oceny ryzyk związanych z umowami o świadczenie usług metodą chmurową, jest **międzynarodowy transfer danych osobowych.** W świetle postanowień Dyrektywy i UODO, jak i RODO, przekazywanie danych osobowych do państwa trzeciego (tj. państwa nienależącego do Europejskiego Obszaru Gospodarczego) co do zasady jest możliwe tylko wtedy, gdy państwo to zapewnia „odpowiedni stopień ochrony danych osobowych".

(24) W przypadku przetwarzania danych poza EOG, Rozporządzenie nakazuje stosowanie mechanizmów w nim opisanych, w tym m.in.:

(a) przekazywanie danych do państw trzecich, w stosunku do których Komisja Europejska wydała decyzję o gwarantowaniu odpowiedniego stopnia ochrony danych (tu kwalifikują się kraje takie jak np. Szwajcaria, Kanada, Izrael oraz Stany Zjednoczone z racji na uzgodnienie zasad przekazywania danych w ramach tzw. Tarczy Prywatności – *Privacy Shield*);

(b) wprowadzenie w organizacji wiążących reguł korporacyjnych, które będą zgodne z prawnie obowiązującymi zasadami ochrony danych osobowych; oraz



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(c) zastosowanie opublikowanych przez Komisję Europejską standardowych klauzul umownych.

(25) Powyższe wyliczenie nie ma charakteru wyczerpującego. W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony (Art. 45) lub braku odpowiednich zabezpieczeń określonych w Art. 46, w tym wiążących reguł korporacyjnych, przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie pod warunkami wskazanymi enumeratywnie w treści Rozporządzenia (Art. 49), kwalifikującymi się jako „wyjątki w szczególnych sytuacjach".

(26) Podsumowując, wskazane powyżej najistotniejsze kwestie dotyczące przetwarzania danych osobowych przez dostawców usług chmurowych mają na celu **podniesienie standardów ochrony danych osobowych** wśród pomiotów, którym administratorzy powierzyli do przetwarzania dane osobowe. Zmiany, jakie wprowadziło RODO w tym zakresie, ocenić należy jako pożądane z punktu widzenia usługobiorców, jako że w świetle nowych przepisów są oni w stanie w dużo szerszym zakresie kontrolować czynności przetwarzania powierzanych przez nich do chmury danych oraz egzekwować od dostawców przestrzeganie wyznaczonych w umowach standardów zgodnych z treścią Rozporządzenia. Jako że zgodnie z treścią RODO umowa powierzenia przetwarzania powinna określać zarówno zakres obowiązków administratora, jak i podmiotu przetwarzającego dane w jego imieniu, **usługobiorca ma możliwość dokładnego wytyczenia granicy odpowiedzialności za przetwarzanie danych osobowych między nim a usługodawcą *clouda***, co może znacząco obniżyć ponoszone przez administratora ryzyko, związane z potencjalnych naruszeniem bezpieczeństwa tych danych, i tym samym skutkować wyłączeniem lub ograniczeniem zakresu sankcji z nim związanych.

[Vendor lock-in]

(27) Istotnym ryzykiem prawnym wynikającym z usług chmurowych jest niebezpieczeństwo *vendor lock-in*, tj. sytuacji, w której klient jest uzależniony od usług dostawcy do tego stopnia, że jego zmiana wiąże się ze znaczącymi kosztami lub niedogodnościami. Może ona wynikać w szczególności z dwóch źródeł: postanowień umowy dotyczących wynagrodzenia dostawcy oraz z kwestii *exit planu*.

(28) Ryzyko znaczących strat w razie wypowiedzenia umowy dotyczącej chmury, spowodowanych postanowieniami o wynagrodzeniu, przyjmuje wiele obliczy.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

Jako przykład można wskazać taką treść kontraktu, z której wynika obowiązek znaczącej płatności za długi okres rozliczeniowy z góry – i rezygnacja z usług w jego trakcie nie będzie wiązać się z odzyskaniem „nadpłaconej" części. Jednak krytycznym ryzykiem, pojawiającym się w klauzulach umów i regulaminów dotyczących usług w chmurze, jest uprawnienie dostawcy do przerwania świadczenia usług (w całości lub niektórych z nich) w razie nieotrzymania pełnej umówionej płatności w ustalonym terminie. To zmusza usługobiorcę do regularnych wpłat wynagrodzenia nawet w przypadku intencji rezygnacji z usług – przynajmniej do momentu pełnej gotowości do przeniesienia danych do innej chmury lub do oprogramowania w ramach rozwiązania *on-premise*.

(29) Kwestią jeszcze silniej uzależniającą usługobiorcę od dostawcy jest brak *exit planu*, czyli z góry opracowanego planu sprawnej rezygnacji z dotychczasowych usług („wyjścia" z chmury) i przejścia do nowego dostawcy chmury lub do systemu zbudowanego w modelu *on-premise*. Należy przy tym zaznaczyć, że wynegocjowanie realnie przydatnych zobowiązań dostawcy w zakresie *exit planu* jest rynkowo bardzo trudne – przy czym oczywiście, jeśli jest możliwe, usługobiorca powinien o nie zabiegać. Przede wszystkim jednak usługobiorca powinien mieć opracowany *exit plan* rozumiany jako wewnętrzny materiał, przygotowujący go na sytuację konieczności zmiany dostawcy, który pozwoli przejść do innego dostawcy usług lub w ogóle zrezygnować z chmury sprawnie, bez uszczerbku dla przechowywanych w *cloudzie* danych oraz przy poniesieniu jak najmniejszych kosztów. Konieczność przygotowania planu wyjścia dla jednostek administracji publicznej jest tym większa, że zawierają one kontrakty na czas oznaczony, często nieprzekraczający 12 miesięcy – co powoduje częste zawieranie kolejnych umów i potencjalną możliwość częstych migracji pomiędzy różnymi chmurami.

(30)

[Integracja]

(31) Dla większości usługobiorców określone usługi chmurowe obsługują pewien wycinek ich działalności – podczas gdy inne obszary są obsługiwane przez inne systemy informatyczne lub rozwiązania chmurowe. Dla sprawnego działania organizacji konieczne jest wówczas zintegrowanie tych rozwiązań, aby swobodnie można było przekazywać pomiędzy nimi dane.

(32) Dokonanie takiej integracji wiąże się jednak z istotnym ryzykiem prawnym. Część dostawców zastrzega obowiązek płatności dodatkowej opłaty licencyjnej za podłączenie do ich rozwiązania, choćby pośrednie, innego systemu informatycznego lub chmury, – z uwagi na to, że udzielona przez nich licencja



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

dotyczy tylko ściśle zdefiniowanych użytkowników nazwanych i nie obejmuje komunikacji z innym rozwiązaniem informatycznym[29]. Zintegrowanie takiej chmury z innym systemem może rodzić znaczące roszczenia finansowe dostawcy.

[29] Zob. artykuł dostępny pod adresem: http://www.pcworld.com/article/3171001/cloud-computing/sap-license-fees-are-due-even-for-indirect-users-court-says.html.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

# VI. PRZEGLĄD USTAWODAWSTWA DOTYCZĄCEGO CHMURY

[Wprowadzenie]

(1) W polskim porządku prawnym nie występuje żadna ustawa regulująca kompleksowo, w całości lub w jakiejkolwiek części zagadnienia związane z korzystaniem usług świadczonych w oparciu o chmurę obliczeniową. Wiąże się to z koniecznością oceny tych kwestii przez pryzmat wielu rozproszonych przepisów o różnorakim charakterze.

(2) Przystępując do przeglądu ustawodawstwa dotyczącego chmury obliczeniowej, należy brać pod uwagę zarówno akty prawne, które dotyczą pewnych ogólnych faktów i zjawisk o zakresie szerszym niż chmura (ale w których się ona mieści), jak i te dotyczące bezpośrednio *cloud computingu* – choćby nawet nieposługujące się bezpośrednio tym pojęciem. Do pierwszego wskazanego wyżej typu ustawodawstwa należy przede wszystkim Kodeks cywilny oraz prawo autorskie (oprogramowanie budujące chmurę zazwyczaj będzie stanowić utwory w rozumieniu art. 1 ust. 1 pr.aut.). Z uwagi na fakt, że korzystanie z chmury jest możliwe tylko za pośrednictwem Internetu, należy do nich również ustawa o świadczeniu usług drogą elektroniczną. Za to zarówno do pierwszej, jak i drugiej ze wskazanych grup, należą akty prawne o charakterze branżowym, regulujące poszczególne sektory gospodarcze (np. prawo bankowe), które, ze względu na szczególny status informacji powierzanych podmiotom w nich działającym, zostały obciążone przez ustawodawcę szczególnymi obowiązkami dotyczącymi przetwarzania takich informacji w *cloudzie*.

(3) Ponadto, na wzmożoną uwagę w kontekście chmury zasługuje także tematyka danych osobowych, z uwagi na to, że typowym jest, zwłaszcza dla usługobiorców chmurowych o znacznym potencjale gospodarczym lub stanowiących jednostki administracji publicznej, że dane osobowe są przetwarzane za pomocą chmury obliczeniowej. W takiej sytuacji przepisy prawne narzucają konkretne obowiązki dotyczące korzystania z chmury.

(4) Z punktu widzenia jednostek administracji publicznej wymaga omówienia także możliwość przetwarzania w chmurze informacji niejawnych



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

w rozumieniu ustawy o ochronie informacji niejawnych i związane z tym wymagania.

[Prawo cywilne]

(5) Relacja dostawcy chmury i jego klienta stanowi stosunek cywilnoprawny. Z tego powodu to Kodeks cywilny stoi w pierwszym rzędzie aktów prawnych regulujących zagadnienia dotyczące *cloud computingu*.

(6) Kodeks cywilny nie rozpoznaje relacji prawnej dotyczącej świadczenia usług w modelu *cloud computingu* w zamian za wynagrodzenie wśród umów zobowiązaniowych przewidzianych w Tytule XI Księgi Trzeciej Kodeksu cywilnego (art. 535 i n. k.c.) – określanych w języku prawniczym umowami nazwanymi. Nie oznacza to jednak, że ustawodawca nie uregulował w ogóle tej umowy (i szeregu innych niewystępujących we wspomnianym wyżej katalogu). Abstrahując od ogólnych przepisów dotyczących wszelkich stosunków cywilnoprawnych, w Kodeksie cywilnym został przewidziany przepis dotyczący umów o świadczenie usług, które nie są uregulowane innymi przepisami: art. 750 k.c. Nakazuje on stosować odpowiednio do takich umów przepisy o zleceniu (art. 734 i n. k.c.). Umowy takie określa się mianem umów podobnych do zlecenia)[30]. Regulacja art. 750 k.c. jest bardzo lakoniczna, zatem jej interpretowanie budzi problemy. Otóż wskazane w niej „odpowiednie stosowanie" oznacza, że *zależnie od treści konkretnej umowy (charakteru zleconej usługi) niektóre przepisy o zleceniu będą stosowane wprost, inne z pewnymi modyfikacjami, a jeszcze inne w ogóle nie znajdą zastosowania*[31].

(7) Szczegółowa analiza tego, które przepisy o zleceniu powinny zostać zastosowane wprost dla kontraktów chmurowych, które odpowiednio, a które w ogóle – i jakie ma to konsekwencje prawne – wykracza poza ramy Opinii. W tym miejscu należy wskazać jedynie kluczowe aspekty powiązane ze stosowaniem przepisów o zleceniu do umów o świadczenie usług chmurowych.

(8) Nadzwyczaj istotnym zagadnieniem w przedmiocie umowy chmurowej – jako umowy podobnej do zlecenia – jest charakter odpowiedzialności dostawcy usług chmurowych: odpowiedzialności za staranne działanie. Polega ona na tym, że dostawca nie odpowiada bezpośrednio za rezultat założony w umowie,

[30] W doktrynie prawniczej przyjmuje się taką kwalifikację jednogłośnie. Zob. E. Molenda-Kropielnicka, *Cloud computing – zagadnienia prawne*, Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej, 2013/119, s. 143.

[31] P. Machnikowski [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, Warszawa 2016, s. 1413.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

ale za dołożenie wszelkich starań z zachowaniem staranności na poziomie określonym w Kodeksie cywilnym[32] (wobec podmiotów profesjonalnych art. 355 k.c. przewiduje obowiązek zachowania należytej staranności: tj. staranności ogólnie wymaganej w stosunkach danego rodzaju [§ 1] przy uwzględnieniu zawodowego charakteru tej działalności [§ 2]).

(9) Art. 738 w zw. z art. 750 k.c. przewiduje, że w umowie podobnej do zlecenia możliwe jest powierzenie części zakresu realizowanych usług podwykonawcy, jeśli wynika to z umowy, zwyczaju, albo gdy przyjmujący zlecenie (usługodawca) jest do tego zmuszony przez okoliczności. Prowadzi to do wniosku, że jeśli w świadczenie usług chmurowych mają być zaangażowani poddostawcy, umowa powinna przewidywać taką możliwość.

(10) Kluczowe dla umowy o świadczenie usług chmurowych – jako umowy podobnej do zlecenia – jest kwestia czasu jej trwania. Strony powinny określić go w umowie, natomiast jeśli tego nie zrobią, będzie to umowa na czas nieoznaczony. Niezależnie od tego, zgodnie z art. 746 w zw. z art. 750 k.c. zarówno usługobiorca, jak i usługodawca są uprawnieni do wypowiedzenia umowy w każdym czasie, z trzema zastrzeżeniami:

(a) w przypadku wypowiedzenia przez usługobiorcę (zleceniodawcę), powinien on zwrócić usługodawcy wydatki, a jeśli umowa była odpłatna – również zapłacić wynagrodzenie za dotychczas świadczone usługi;

(b) w razie wypowiedzenia umowy (jeśli była odpłatna) przez którąkolwiek ze stron bez ważnego powodu, strona ta będzie zobowiązana do naprawienia szkody, jeśli w wyniku wypowiedzenia doznała jej druga strona;

(c) art. 746 § 3 k.c. przewiduje, że nie można zrzec się z góry uprawnienia do wypowiedzenia z ważnych powodów. Wobec tego, interpretując z przeciwieństwa (*a contrario*), możliwe jest zrzeczenie się (przez obie strony lub jedną z nich) z góry prawa do wypowiedzenia z powodów innych niż ważne.

(11) Pojęcie „ważnego powodu" nie ma ustawowej definicji. Stanowi ono otwarty katalog przyczyn. W jego zakres wchodzić mogą zarówno przyczyny o charakterze obiektywnym, jak i subiektywnym[33]. W przypadku złożenia

[32] Por. K. Kopaczyńska-Pieczniak [w:] A. Kidyba (red.), *Kodeks cywilny. Komentarz. Tom III. Zobowiązania - część szczególna*, pkt 9 komentarza do art. 734 k.c., LEX.

[33] P. Machnikowski [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, Warszawa 2016, s. 1408.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

oświadczenia o wypowiedzeniu umowa wygasa ze skutkiem natychmiastowym, chyba że strony przewidziały w umowie termin wypowiedzenia[34].

(12) Niezależnie od powyższych rozważań należy mieć na względzie, że umowy o świadczenie usług objęte zakresem regulacji art. 750 k.c. stanowią, z prawnego punktu widzenia, nad wyraz elastyczne narzędzie. Z tego powodu, korzystając z prawa swobody umów, strony powinny uregulować bezpośrednio w takiej umowie jak najwięcej istotnych dla nich kwestii oraz zabezpieczyć dostrzegane ryzyka biznesowe.

[Świadczenie usług drogą elektroniczną]

(13) Ustawa o świadczeniu usług drogą elektroniczną określa (m.in.) obowiązki usługodawcy z tytułu świadczenia usług drogą elektroniczną i zasady wyłączania odpowiedzialności usługodawcy z tego tytułu (art. 1 pkt 1 i 2 u.ś.u.d.e.). Zgodnie z art. 2 pkt 4 u.ś.u.d.e. świadczenie usług drogą elektroniczną oznacza wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Wskazana definicja obejmuje usługi chmurowe, co powoduje objęcie ich świadczenia zakresem ustawy o świadczeniu usług drogą elektroniczną.

(14) Ustawa o świadczeniu usług drogą elektroniczną przewiduje szereg obowiązków informacyjnych oraz zasady dystrybuowania informacji handlowej. Jednakże, z perspektywy przedmiotu opinii, najistotniejszymi kwestiami dotyczącymi chmury, poruszonymi w tym akcie prawnym są: regulamin świadczenia usług drogą elektroniczną oraz ograniczenia odpowiedzialności usługodawcy.

(15) Art. 8 ust. 1 u.ś.u.d.e. nakłada na usługodawcę obowiązek określenia regulaminu świadczenia usług drogą elektroniczną (pkt 1) oraz obowiązek jego nieodpłatnego udostępnienia usługobiorcy przed zawarciem umowy o świadczenie usług (pkt 2). Przepis ten ponadto wskazuje, że udostępnienie regulaminu powinno nastąpić w sposób umożliwiający pozyskanie,

[34] Por. K. Kopaczyńska-Pieczniak [w:] A. Kidyba (red.), *Kodeks cywilny. Komentarz. Tom III. Zobowiązania - część szczególna*, pkt 4 komentarza do art. 746 k.c., LEX.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

odtwarzanie i utrwalanie jego treści za pomocą systemu teleinformatycznego, którym posługuje się usługobiorca. Art. 8 ust. 2 u.ś.u.d.e. przewiduje, że usługobiorca nie jest związany postanowieniami regulaminu, które nie zostały mu udostępnione w sposób opisany powyżej.

(16) Art. 8 ust. 3 u.ś.u.d.e. wymienia elementy, które musi zawsze zawierać regulamin świadczenia usług drogą elektroniczną (używając zwrotu „w szczególności", co oznacza, że w przedmiotowym przepisie mamy do czynienia z katalogiem otwartym). Elementy te to określenie: rodzaju i zakresu usług świadczonych drogą elektroniczną, warunki ich świadczenia (w tym niezbędne wymagania techniczne i zakaz dostarczania przez usługobiorcę treści o charakterze bezprawnym), warunki zawierania i rozwiązywania umowy o świadczenie usług drogą elektroniczną oraz tryb postępowania reklamacyjnego.

(17) Bardzo istotną regulację (chociaż bardziej z punktu widzenia usługodawcy niż usługobiorcy) zawierają przepisy art. 12-15 u.ś.u.d.e. Mowa w nich o wyłączeniu odpowiedzialności usługodawcy za treść danych, w stosunku do których, w zakresie usług świadczonych drogą elektroniczną, świadczy usługi polegające na prostym przesyle (*mere conduit*), automatycznym przejściowym i pośrednim przechowywaniu danych (*caching*) oraz *hostingu* – pod warunkiem spełnienia warunków szczegółowo opisanych w tych przepisach.

[Prawo autorskie]

(18) Szczegółowa charakterystyka problemów dotyczących *cloud computingu* na tle prawa autorskiego dalece wykracza poza ramy Opinii. Dla jej celów konieczne jest jedynie dokonanie oceny, czy w ramach umowy o świadczenie usług chmurowych (zwłaszcza w modelu SaaS) powinna zostać zawarta umowa licencyjna w rozumieniu art. 41 ust. 2 pr.aut. – jako że usługi świadczone w modelu chmurowym są realizowane dzięki oprogramowaniu komputerowemu „budującemu" chmurę, którym dysponuje dostawca usług, a oprogramowanie to w zdecydowanej części będzie stanowić utwory w rozumieniu art. 1 ust. 1 pr.aut

(19) Korzystanie z oprogramowania komputerowego zainstalowanego na infrastrukturze fizycznej zawsze wymaga jego zwielokrotniania w całości lub w części – co zgodnie z art. 74 ust. 4 pr.aut. jest objęte zakresem autorskich praw majątkowych podmiotu uprawnionego do takiego oprogramowania. W takiej sytuacji oczywiste jest, że podmiot inny niż uprawniony prawnoautorsko może korzystać z takiego oprogramowania wyłącznie na podstawie licencji udzielonej przez uprawnionego lub na podstawie szczególnego przepisu prawa



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

autorskiego (mowa tutaj przede wszystkim o art. 75 pr.aut. dotyczącym tzw. legalnego dysponenta).

(20) Powyższego toku rozumowania nie można łatwo przełożyć na sytuację korzystania z rozwiązań chmurowych. Wprawdzie na jego skutek dochodzi do zwielokrotniania oprogramowania – ale odbywa się to poza kontrolą i poza infrastrukturą usługobiorcy, a jedynie na jego żądanie. Wobec tego można spierać się, czy w takim układzie:

(a) dochodzi do dokonania czynności mieszczących się w obrębie monopolu prawnoautorskiego i jest konieczne zawarcie licencji między usługobiorcą a usługodawcą; czy

(b) dochodzi do dokonania czynności mieszczących się w obrębie monopolu prawnoautorskiego, ale usługobiorca może korzystać z oprogramowania za pośrednictwem chmury bez konieczności zawierania licencji, na podstawie art. 75 pr.aut., jako legalny dysponent; czy

(c) nie dochodzi do dokonania czynności mieszczących się w obrębie autorskich praw majątkowych i nie jest konieczne udzielenie usługobiorcy jakiejkolwiek licencji, ani korzystanie z prawnoautorskich uprawnień ustawowych.

(21) Jednoznaczne wskazanie, które z przedstawionych wyżej alternatywnych stanowisk jest poprawne, będzie o tyle trudne, że nauka prawna nie jest zgodna w tym względzie[35], brakuje też orzecznictwa sądów. W naszej opinii, oceny konieczności zawierania umowy licencyjnej należałoby każdorazowo dokonywać mając na uwadze specyfikę określonej usługi chmurowej. Niezależnie od tego, z punktu widzenia usługobiorcy, najbezpieczniej jest dostosować się do najbardziej rygorystycznego stanowiska – i zawrzeć licencję.

(22) Należy w tym miejscu wskazać także, że często świadczenie usług w chmurze, zwłaszcza w modelu SaaS, odbywa się przy użyciu zainstalowanej w infrastrukturze usługobiorcy wtyczki czy aplikacji – wówczas, przynajmniej w jej zakresie, udzielenie licencji jest konieczne.

[Informacje niejawne]

(23) Podmioty publiczne, decydując o korzystaniu z rozwiązań chmurowych, powinny przeanalizować, czy będą za ich pomocą przetwarzać informacje niejawne. Jeśli tak, powinny uwzględnić dotyczące ich wymagania ustawowe.

[35] Zob. E. Molenda-Kropielnicka, *Cloud computing – zagadnienia prawne*, Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej, 2013/119, s. 131-132.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(24) Zasady ochrony informacji niejawnych, tj. informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu wyrażenia – określa ustawa o ochronie informacji niejawnych (art. 1 ust. 1 u.o.i.n.). Celem tejże ustawy jest zabezpieczenie kluczowych informacji z punktu widzenia interesu państwa przed niepożądanych dostępem. Przepisy ustawy o ochronie informacji niejawnych mają zastosowanie do podmiotów publicznych wymienionych w art. 1 ust. 2 u.o.i.n. Dotyczą one m.in. ochrony informacji niejawnych w systemach teleinformatycznych (art. 1 ust. 1 pkt 7 u.o.i.n.).

(25) Przetwarzanie informacji niejawnych w systemach teleinformatycznych wymaga dokonania w stosunku do tych systemów akredytacji (art. 48 ust. 1 u.o.i.n.), tj. dopuszczenia systemu teleinformatycznego do przetwarzania informacji niejawnych (art. 2 pkt 10 u.o.i.n.). Akredytacji udziela się na czas określony, nie dłuższy niż 5 lat (art. 48 ust. 2 u.o.i.n.), przy czym udzielenie jej wymaga uprzedniego sporządzenia kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego oraz jej zatwierdzenia przez odpowiedni organ (ABW/SKW – w przypadku systemu przeznaczonego dla informacji o klauzuli „poufne" lub wyższej – albo kierownika jednostki organizacyjnej – w przypadku systemu informacji opatrzonych klauzulą „zastrzeżone"). Na dokumentację powyższą składają się, zgodnie z art. 2 pkt 7-9 u.o.i.n.:

(a) dokument szczególnych wymagań bezpieczeństwa – tj. systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;

(b) dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, tj. opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych, przetwarzanych w systemie teleinformatycznym, oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp.

(26) Zawartość oraz ramy czasowe opracowania i korygowania wskazanych powyżej dokumentów specyfikuje szczegółowo ustawa oraz rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. Zgodnie z nimi:

(a) dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania systemu, uzupełnia na etapie wdrażania, a modyfikuje na etapie eksploatacji – przed dokonaniem zmian



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

w systemie teleinformatycznym (co oznacza, że bez uprzedniej zmiany dokumentu system nie powinien być zmieniany). Powinien on zawierać m.in. wyniki szacowania ryzyka dla bezpieczeństwa informacji niejawnych, sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na nie (art. 49 ust. 1 i 2 u.o.i.n.), a także wymagania eksploatacyjne dla wymiany informacji i połączeń z innymi systemami teleinformatycznymi, informacje o lokalizacji systemu teleinformatycznego, zastosowanych zabezpieczeniach, o bezpieczeństwie fizycznym (w tym granicach i lokalizacjach ochronnych oraz środkach ich ochrony), informacje o ochronie elektromagnetycznej, stosowanych narzędziach lub urządzeniach kryptograficznych, utrzymaniu systemu (w tym dokonywaniu przeglądów diagnostycznych i napraw), zapobieganiu incydentom bezpieczeństwa (w tym ochronie przed oprogramowaniem złośliwym), zasadach wprowadzania poprawek lub uaktualnień oprogramowania, kontroli dostępu, audycie wewnętrznym, zmianach w systemie teleinformatycznym: w tym dotyczących aktualizacji dokumentacji i bezpieczeństwa systemu teleinformatycznego oraz warunkach ponownej akredytacji systemu teleinformatycznego i wycofaniu z eksploatacji (§ 25 r.p.w.);

(b) dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego opracowuje się na etapie wdrażania systemu i modyfikuje na etapie eksploatacji – przed dokonaniem zmian w systemie teleinformatycznym (art. 49 ust. 3 u.o.i.n.). Obejmuje on szczegółowy wykaz procedur bezpieczeństwa, m.in. odnośnie do: bezpieczeństwa urządzeń i oprogramowania, zarządzania konfiguracją sprzętowo-programową (w tym zasad serwisowania lub modernizacji oraz wycofywania z użycia elementów systemu teleinformatycznego), monitorowania i audytu systemu teleinformatycznego, reagowania na incydenty bezpieczeństwa (§ 26 r.p.w.).

(27) W przypadku dokonywania akredytacji przez ABW/SKW, służby te powinny, oprócz zapoznania się z dokumentacją bezpieczeństwa systemu teleinformatycznego, przeprowadzić audyt bezpieczeństwa systemu teleinformatycznego (art. 48 ust. 6 u.o.i.n.), tj. weryfikację poprawności realizacji wymagań i procedur określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego (art. 2 pkt 12 u.o.i.n.).



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(28) Oprócz spełnienia powyższych wymagań, dla przetwarzania informacji niejawnych w systemie teleinformatycznym konieczne jest spełnienie także szeregu innych warunków określonych w r.p.w., dotyczących samego systemu, jak i zarządzania nim, w zakres których wchodzi m.in.: objęcie systemu procesem zarządzania ryzykiem, wprowadzenie wielopoziomowej ochrony systemu, wykonywanie okresowych testów bezpieczeństwa, minimalizacja funkcjonalności (tj. instalowanie i korzystanie w systemie wyłącznie z funkcji i usług niezbędnych do prawidłowej realizacji zadań, do których system został stworzony - § 5 r.p.w.), ustalenie zasad tworzenia i przechowywania kopii zapasowych, ustalenie procedur monitorowania stanu technicznego systemu teleinformatycznego (§ 9 r.p.w.). Koniecznie jest także zapewnienie poufności informacji przekazywanych w formie transmisji poza strefami ochronnymi, przez stosowanie certyfikowanych urządzeń lub narzędzi kryptograficznych (§ 10 r.p.w.). Rozporządzenie wymaga także tworzenia i przechowywania rejestrów zdarzeń służących analizie incydentów bezpieczeństwa (§ 11 r.p.w.), wyposażenia samego systemu w mechanizmy lub procedury zapobiegające incydentom bezpieczeństwa (§ 12 r.p.w.) oraz wdrożenia do systemu zabezpieczeń uniemożliwiających przekazywanie niepożądanych informacji w przypadku organizowania połączenia międzysystemowego (§ 15 r.p.w.).

(29) Ustawa o ochronie informacji niejawnych reguluje nie tylko wdrażanie i proces eksploatacji systemu, w którym będą przetwarzane informacje niejawne. Przewiduje ona także szczególne zasady dotyczące modyfikowania takiego systemu lub rezygnowania z jego używania. Mianowicie: podstawą dokonywania wszelkich zmian systemu jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie (art. 49 ust. 5 u.o.i.n.) – tzn., że takie szacowanie zawsze musi poprzedzać zmianę w systemie, zaś sama zmiana powinna być powiązana z szacowaniem ryzyka. Jeśli natomiast system teleinformatyczny jest wycofywany, usuwa się z niego informacje niejawne, w szczególności poprzez przeniesienie ich do innego systemu teleinformatycznego, zarchiwizowanie lub zniszczenie informatycznych nośników danych (§ 18 ust. 6 pkt 4 u.o.i.n.).

(30) Opisane powyżej unormowania dotyczące przetwarzania informacji niejawnych są bardzo rozbudowane i dostosowanie do nich chmury w większości przypadków będzie nastręczać trudności. O ile względnie łatwo można sobie wyobrazić wdrożenie chmury prywatnej, odpowiadającej wymaganiom ustawy o ochronie informacji niejawnych (zwłaszcza gdyby jej infrastruktura znajdowała się pod kontrolą wdrażającego ją podmiotu), o tyle znacznie trudniej pogodzić je z chmurą publiczną.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(31) Możliwość przetwarzania informacji niejawnych przy użyciu rozwiązań informatycznych opartych o chmurę publiczną będzie napotykać problemy dotyczące przede wszystkim:

(a) kontroli nad infrastrukturą – którą zarządza dostawca chmury i która w większości wypadków jest bardzo rozproszona. Usługobiorca nie ma faktycznej możliwości wglądu w jej funkcjonowanie. Przeważnie nie będzie wiedział nie tylko, gdzie się ona znajduje, ale nawet jaki jest rozmiar zasobów go obsługujących (z uwagi na alokowanie mocy obliczeniowej). Usługobiorca nie ma też żadnego wglądu ani wpływu na procedury związane z dostępem do lokalizacji infrastruktury ani na ich fizyczne zabezpieczenie;

(b) architektury i mechanizmów działania chmury – usługobiorca nie uzyska informacji (ani tym bardziej wpływu) na stosowane przez dostawcę usług zabezpieczenia informatyczne, techniki szyfrowania, mechanizmy rozpoznawania oraz usuwania błędów czy incydentów bezpieczeństwa;

(c) modyfikowania i rozwijania oprogramowania budującego chmurę – w ramach rozwiązań *cloud computingowych* usługobiorca otrzymuje pewne możliwości korzystania z funkcjonalności oprogramowania, natomiast nie ma dostępu do niego samego, z uwagi na co nie ma wpływu i wiedzy dotyczących czasu, zakresu i rodzaju wprowadzanych modyfikacji oprogramowania. Jest to niebezpieczeństwo o tyle istotne, że, zgodnie z ustawą o ochronie informacji niejawnych, wszelkim modyfikacjom systemu przetwarzającego informacje niejawne powinien towarzyszyć proces szacowania ryzyka;

(d) usuwania danych – usługobiorca może żądać usunięcia informacji umieszczonych przez niego w chmurze – ale co do zasady nie będzie znał sposobu ani terminów, w jakich dane takie będą usunięte, ani czy faktycznie nie pozostanie po nich żadna kopia;

(e) testów i audytów – ich przeprowadzenie będzie możliwe w bardzo ograniczonym zakresie – tj. funkcjonalności udostępnionych przez usługobiorcę poprzez udostępniony przez niego interfejs. Nie będzie możliwe audytowanie czy testowanie oprogramowania dostawcy, które stoi za chmurą.

(32) Podsumowując, kształt regulacji dotyczących przetwarzania informacji niejawnych w systemach teleinformatycznych poważnie utrudnia wykorzystywanie do tego celu chmury obliczeniowej. Oferowane na rynku rozwiązania w zakresie chmury publicznej dają możliwość zastosowania



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

omówionych powyżej wymagań w bardzo niewielkim stopniu. Znacznie łatwiej natomiast byłoby o ich spełnienie przy budowie chmury prywatnej.

[Regulacje branżowe]

(33) Istnieje szereg ustaw dotyczących poszczególnych sektorów gospodarki – w obszarze tzw. działalności regulowanej – w których zostały unormowane zagadnienia obejmujące swym zakresem *cloud computing*. Ponadto, w związku z działalnością w tych sektorach organów nadzorczych (takich jak Komisja Nadzoru Finansowego: KNF), problematyka chmury została zaadresowana także w aktach tzw. *soft law*. O ile wskazane poniżej regulacje nie obowiązują organów administracji publicznej, o tyle ich przybliżenie może okazać się pomocne – dla uwypuklenia problemów zauważonych w stosowaniu rozwiązań chmurowych i przyjętych w związku z nimi środkami zaradczymi.

(34) Szczególną regulację dotyczącą chmury zawiera prawo bankowe. W jego art. 6a-6d została uregulowana instytucja outsourcingu bankowego – tzn. powierzenia, w drodze zawarcia odpowiedniej umowy, podmiotowi trzeciemu wykonywania niektórych czynności niezbędnych do prawidłowego funkcjonowania banku[36]. Przetwarzanie w ramach usług chmurowych danych banku dotyczących prowadzenia czynności bankowych w praktyce zawsze będzie stanowić odmianę outsourcingu bankowego. W związku z powyższym, do relacji pomiędzy bankiem a dostawcą usług chmurowych należy zastosować zasady przewidziane w art. 6a-6d p.b. – przy czym art. 6a w zasadzie definiuje outsourcing bankowy, a dalsze przepisy wskazują dotyczące go reguły – w sferze odpowiedzialności, warunków proceduralnych ustanowienia go oraz podoutsourcingu.

(a) Co do zasady zawarcie umowy outsourcingu bankowego nie wymaga zgody organu nadzorczego (KNF) ani powiadamiania go o takiej umowie. Podobnie z wykorzystywaniem przez *insourcera* (jakim będzie dostawca chmury) poddostawców (podoutsourcing) – przy czym taką możliwość musi przewidywać umowa outsourcingu (art. 6a ust. 7 p.b.). Wyjątki od tej reguły ustanawia art. 6d p.b., przewidując konieczność uzyskania

[36] H. Gronkiewicz-Waltz (red.), Prawo bankowe, komentarz do art. 6a, Legalis 2015.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

zezwolenia KNF (decyzja administracyjna) na zawarcie umowy outsourcingu lub korzystanie z podoutsourcingu, jeśli *insourcer* albo podinsourcer nie mają siedziby albo stałego miejsca zamieszkania w państwie członkowskim Unii Europejskiej, albo faktycznym miejscem wykonywania powierzonych im czynności będzie terytorium państwa nienależącego do Unii Europejskiej (tzw. outsourcing i podoutsourcing pozaunijny). Przy czym, zgodnie z art. 6a p.b., sama umowa outsourcingu powinna być zawarta w formie pisemnej.

(b) Art. 6b prawa bankowego dokonuje podwójnego wyłączenia możliwości ograniczenia odpowiedzialności: *insourcera* wobec banku oraz banku wobec klienta (zarówno konsumenta, jak i przedsiębiorcy) – za szkody wyrządzone klientowi wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej. Przepis ten ma imperatywny charakter – nie można go wyłączyć ani umową pomiędzy bankiem i *insourcerem*, ani między bankiem a klientem (zatem przeciwne postanowienia umów, zgodnie z art. 58 § 1 i § 3 k.c., będą nieważne).

(c) Art. 6c p.b. ustanawia warunki i procedury, które powinny być spełnione dla możliwości stosowania outsourcingu bankowego – w tym chmury. Nakazuje on m.in. posiadanie przez bank i *insourcera* „planów działania zapewniających ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową", a bankowi prowadzenie ewidencji dokumentów (m.in. umowy outsourcingowej, planów działania, dokumentów dotyczących statusu *insourcera*, etc.), do której wglądu może żądać KNF. Przepis ten przewiduje także konieczność notyfikowania KNF i zawierania szczególnego rodzaju umów outsourcingowych: outsourcingu awaryjnego.

(d) Art. 6c ust. 7 p.b. nadaje ponadto KNF kompetencję do nakazania bankowi (w drodze decyzji administracyjnej) podjęcia działań zmierzających do zmiany lub rozwiązania umowy outsourcingowej, jeżeli jej wykonanie zagraża ostrożnemu i stabilnemu zarządzaniu bankiem lub gdy *insourcer* utracił wymagane uprawnienia niezbędne do wykonywania tej umowy.

(35) Kwestie dotyczące outsourcingu bankowego, w tym w formie *cloud computingu*, reguluje również Rekomendacja D, wydana na podstawie art. 137 ust. 1 pkt 5 p.b. przez KNF. Jest to akt *soft law* określający wytyczne organu nadzorczego względem banków w obszarze zarządzania technologią. To znaczy, że nie stanowi obowiązującego prawa – ale spełnienie jej zaleceń może decydować o pomyślnym wyniku kontroli KNF. Rekomendacja D składa się z 22



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

szczegółowych rekomendacji, odnoszących się m.in. do konieczności posiadania przez bank sformalizowanych procedur i zasad współpracy, ochrony środowiska teleinformatycznego przed szkodliwym oprogramowaniem, systemu zarządzania bezpieczeństwem środowiska teleinformatycznego oraz do kwestii przeprowadzania audytów. Co warte odnotowania, Rekomendacja D wprost odnosi się do chmury (jako metody przetwarzania danych banków poza własną infrastrukturą). Mianowicie: w wypadku przetwarzania w niej danych o wysokim stopniu poufności lub istotności, Rekomendacja zaleca (pkt 10.6): wprowadzić adekwatne mechanizmy kontrolne zapewniające poufność danych (np. poprzez ich szyfrowanie); zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę; posiadać informacje o tym, w jakich lokalizacjach geograficznych dane te są przetwarzane oraz jakie przepisy prawa obowiązują tam w przedmiotowym zakresie, a także zapewnić zgodność świadczonych usług w zakresie przetwarzania danych z przepisami prawa obowiązującymi w Polsce; zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia – wraz ze wszystkimi kopiami – przez dostawcę usług); przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia obowiązku przedstawiania przez dostawcę certyfikatów w zakresie zgodności z uznanymi międzynarodowymi normami dotyczącymi bezpieczeństwa informacji (szczególnie w przypadku przetwarzania danych poza granicami Europejskiego Obszaru Gospodarczego).

(36) Prawo bankowe reguluje także odrębnie możliwość udostępnienia *insourcerowi* informacji objętych, na podstawie art. 104 ust. 1 p.b., tajemnicą bankową. Dopuszczalność taką przewiduje art. 104 ust. 2 pkt 2 lit. a)-b) p.b. – przy spełnieniu przesłanek w nim opisanych. Przepis ten uzależnia dopuszczalność ujawnienia danych objętych tajemnicą bankową *insourcerowi* od niezbędności tego ujawnienia do należytego wykonania czynności oraz od stałego lub okresowego charakteru powierzenia. Przy czym przez okresowy charakter powierzenia należy w naszej ocenie rozumieć, że powierzenie czynności nie może być doraźne, a powinno nosić cechy stabilności i trwałości w okresie czasu[37]. Warunki te będą co do zasady spełnione dla usług realizowanych w modelu chmurowym. Niezależnie od powyższego, art. 104 ust. 5 p.b. pozwala *insourcerowi* wykorzystać udostępnione mu informacje wyłącznie w celu zawarcia i wykonania umowy outsourcingowej.

[37] Por. Rekomendowane kierunki interpretacyjne przepisów ustawy Prawo bankowe dotyczące outsourcingu, Pismo NBP z dnia 21 grudnia 2004 r. NB-BPN-I-022-070/04.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

(37) Kolejnym przykładem ustawodawstwa dotyczącego *cloud computingu*, nieodnoszącego się do niego wprost – ale do szerszego pojęcia outsourcingu – jest ustawa o działalności ubezpieczeniowej i reasekuracyjnej. Jej art. 3 ust. 1 pkt 27 definiuje outsourcing jako umowę między zakładem ubezpieczeń albo zakładem reasekuracji a dostawcą usług, na podstawie której dostawca usług wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń lub zakład reasekuracji, a także umowę, na podstawie której dostawca usług powierza wykonanie takiego procesu, usługi lub działania innym podmiotom, za pośrednictwem których wykonuje on dany proces, usługę lub działanie. Uważa się, że pojęcie to obejmuje również outsourcing IT, którego odmianą jest posługiwanie się usługami chmurowymi.

(38) Szczegółowa regulacja outsourcingu ubezpieczeniowego została przewidziana w przepisach art. 73 i n. oraz art. 46 u.d.u.r. Wymagają one, w pierwszym rzędzie, zawarcia umowy outsourcingowej w formie pisemnej.

(a) Podobnie jak w przypadku outsourcingu bankowego, nie jest koniecznie uzyskiwanie jakiegokolwiek zezwolenia na zawarcie umowy outsourcingu ubezpieczeniowego – w tym w obszarze IT. Dopuszczalne jest również stosowane podoutsourcingu.

(b) Outsourcing ubezpieczeniowy jest dopuszczalny, o ile dostawca usług będzie współpracował z organem nadzoru w zakresie powierzonych czynności lub funkcji; outsourcer oraz organy kontroli i nadzoru będą posiadać dostęp do danych związanych z powierzonymi czynnościami lub funkcjami; organ nadzoru będzie miał możliwość przeprowadzania kontroli działalności i stanu majątkowego dostawcy usług w zakresie powierzonych czynności lub funkcji (art. 74 u.d.u.r.).

(c) Art. 75 u.d.u.r. przewiduje dodatkowe warunki dopuszczalności zawarcia umowy outsourcingu, które mają dotyczyć funkcji należących do systemu zarządzania oraz podstawowych lub ważnych czynności (dotyczące m.in. niedopuszczalności przekazania zarządzania zakładem, pogorszenia jakości systemu zarządzania czy zwiększenia ryzyka operacyjnego; art. 75 ust. 1 u.d.u.r.), oraz nakazuje zawiadomić organ nadzoru o tego rodzaju outsourcingu co najmniej na 30 dni przed jego wdrożeniem, jak również o istotnej zmianie w outsourcingu tych funkcji lub czynności (art. 75 ust. 2 u.d.u.r.; przy czym KNF może zakazać zawarcia takiej umowy lub jej zmiany, w drodze decyzji administracyjnej – jeśli naruszałyby przepisy ustawowe o outsourcingu: art. 363 ust. 1 u.d.u.r.). Outsourcing IT, polegający na korzystaniu z rozwiązań chmurowych, nie dotyczy funkcji należących do systemu zarządzania –



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

ale może obsługiwać procesy kwalifikujące się jako podstawowe lub ważne czynności. Wówczas wdrożenie chmury wymagać będzie spełnienia wspomnianych wyżej specjalnych warunków.

(d) Jeśli umowa outsourcingu, dotycząca funkcji należących do systemu zarządzania albo podstawowych lub ważnych czynności, narusza regulacje ustawowe o outsourcingu, KNF jest uprawniona nakazać ubezpieczycielowi, w drodze decyzji administracyjnej, rozwiązanie umowy – i to nie stosując przewidzianych w umowie outsourcingu ograniczeń w zakresie możliwości i terminów jej rozwiązywania lub wypowiadania (art. 363 ust. 2 i 3 u.d.u.r.).

(e) Zgodnie z art. 76 u.d.u.r. nie można wyłączyć ani ograniczyć odpowiedzialności outsourcera (zakładu ubezpieczeniowego) za szkody wyrządzone ubezpieczającym, ubezpieczonym lub uprawnionym z umów ubezpieczenia, a także cedentom[38] wskutek niewykonania lub nienależytego wykonania outsourcingu.

(f) Art. 77 u.d.u.r. nakazuje outsourcerom prowadzić ewidencję umów outsourcingowych.

(g) Zgodnie z art. 46 ust. 1 pkt 4 u.d.u.r., zakład ubezpieczeń i zakład reasekuracji sporządzają na piśmie zasady dotyczące outsourcingu, w przypadku gdy zakład ubezpieczeń lub zakład reasekuracji stosuje lub zamierza go stosować, obejmujące m.in.: czynności ubezpieczeniowe lub reasekuracyjne, które zakład zamierza powierzać w drodze outsourcingu ze wskazaniem, które z tych czynności zakład uznaje za podstawowe lub ważne; kryteria wyboru podmiotu, któremu zakład zamierza powierzać wykonywanie czynności ubezpieczeniowych lub reasekuracyjnych; sposób realizacji warunków dopuszczalności outsourcingu (wspominanych wyżej, wynikających z art. 74 i art. 75 u.d.u.r.) czy zasady zarządzania ryzykiem związanym z powierzeniem, w drodze outsourcingu.

(39) W ramach outsourcingu, w tym w ramach rozwiązań chmurowych, dopuszczalne jest przetwarzanie danych stanowiących tajemnicę ubezpieczeniową – na podstawie art. 35 ust. 2 pkt 26 u.d.u.r.

(40) Analogicznie jak w sektorze bankowym, w obszarze ubezpieczeń KNF również wydała akt *soft law* dotyczący zarządzania zasobami IT: Wytyczne dotyczące zarzadzania obszarami technologii informacyjnej. Należy odnotować, że zawierają one odniesienia wprost do pojęcia chmury. W szczególności

[38] Cedent oznacza, zgodnie z art. 3 ust. 1 pkt 3 u.d.u.r.: zakład ubezpieczeń lub zakład reasekuracji, który w związku z wykonywaną działalnością ubezpieczeniową lub reasekuracyjną ceduje ryzyko na zakład reasekuracji lub zakład ubezpieczeń wykonujący działalność reasekuracyjną.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

zawierają, w pkt 10.6, identyczne zalecenia dotyczące przetwarzania w chmurze szczególnie ważnych informacji, jak Rekomendacja D – które zostały szczegółowo opisane w pkt Kwestie dotyczące outsourcingu bankowego, w tym w formie *cloud computingu*, reguluje również Rekomendacja D, wydana na podstawie art. 137 ust. 1 pkt 5 p.b. przez KNF. Jest to akt *soft law* określający wytyczne organu nadzorczego względem banków w obszarze zarządzania technologią. To znaczy, że nie stanowi obowiązującego prawa – ale spełnienie jej zaleceń może decydować o pomyślnym wyniku kontroli KNF. Rekomendacja D składa się z 22 szczegółowych rekomendacji, odnoszących się m.in. do konieczności posiadania przez bank sformalizowanych procedur i zasad współpracy, ochrony środowiska teleinformatycznego przed szkodliwym oprogramowaniem, systemu zarządzania bezpieczeństwem środowiska teleinformatycznego oraz do kwestii przeprowadzania audytów. Co warte odnotowania, Rekomendacja D wprost odnosi się do chmury (jako metody przetwarzania danych banków poza własną infrastrukturą). Mianowicie: w wypadku przetwarzania w niej danych o wysokim stopniu poufności lub istotności, Rekomendacja zaleca (pkt 10.6): wprowadzić adekwatne mechanizmy kontrolne zapewniające poufność danych (np. poprzez ich szyfrowanie); zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę; posiadać informacje o tym, w jakich lokalizacjach geograficznych dane te są przetwarzane oraz jakie przepisy prawa obowiązują tam w przedmiotowym zakresie, a także zapewnić zgodność świadczonych usług w zakresie przetwarzania danych z przepisami prawa obowiązującymi w Polsce; zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia – wraz ze wszystkimi kopiami – przez dostawcę usług); przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia obowiązku przedstawiania przez dostawcę certyfikatów w zakresie zgodności z uznanymi międzynarodowymi normami dotyczącymi bezpieczeństwa informacji (szczególnie w przypadku przetwarzania danych poza granicami Europejskiego Obszaru Gospodarczego). powyżej.

**II.**



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

# VII. CHMURA A PRAWO ZAMÓWIEŃ PUBLICZNYCH

[Usługi chmurowe w świetle prawa zamówień publicznych]

(1) Ustawa p.z.p., podobnie jak ma to miejsce w przypadku aktów prawnych, o których była mowa już wcześniej, nie zawiera szczególnych regulacji dedykowanych rozwiązaniom chmurowym. **Zamówienie na usługi chmurowe należy więc traktować jako standardowe zamówienie publiczne, do którego zastosowanie znajdują właściwe przepisy ustawy p.z.p.**

(2) Należy podkreślić, iż umowa o usługi chmurowe nie traci swojego cywilnoprawnego charakteru przez to, że jest zawierana w reżimie zamówień publicznych (tj. w wyniku postępowania o udzielenie zamówienia publicznego, przeprowadzonego przez zamawiającego publicznego w ramach jednego z trybów uregulowanych w ustawie p.z.p.). W świetle definicji legalnej zamówienia publicznego wyrażonej w art. 2 pkt 13 p.z.p., umowa o zamówienie publiczne cechuje się bowiem tym, że:
   (a) ma charakter odpłatny;
   (b) zawierana jest między zamawiającym a wykonawcą;
   (c) jej przedmiotem są usługi, dostawy lub roboty budowlane.

(3) Choć nie wynika to wprost z przytoczonej powyżej definicji legalnej, umowy w sprawie zamówienia publicznego mają charakter umów cywilnoprawnych, konsensualnych, dwustronnie zobowiązujących (zarówno zamawiający jak i wykonawca są względem siebie jednocześnie dłużnikiem i wierzycielem), wzajemnych (umowy te oparte są na ekwiwalentności świadczeń) oraz przedmiotowo i podmiotowo kwalifikowanych. Treść art. 139 ust. 1 p.z.p., który do umów w sprawie zamówienia publicznego nakazuje stosować przepisy k.c., zdaje się także wskazywać, iż umowy w sprawie zamówienia publicznego nie stanowią pozakodeksowego typu umowy nazwanej, charakterystycznego wyłącznie dla zamówień publicznych. Umowy te mogą bowiem przybierać różną postać (sprzedaż, usługi, dostawa, umowa o dzieło, umowa o roboty budowlane, najem, *etc.*), w zależności od charakteru głównego przedmiotu świadczenia wykonawcy. Konkretyzacja typu umowy następuje zaś



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

każdorazowo w ramach danego postępowania o udzielenie zamówienia publicznego.

(4) Zakwalifikowanie umowy chmurowej w modelu SaaS jako cywilnoprawnej umowy o świadczenie usług nie przesądza jednak automatycznie, że przedmiotowe zamówienie publiczne zostanie zakwalifikowane w taki sam sposób na gruncie ustawy p.z.p. (tj. jako zamówienie na usługi). Ustawa p.z.p. wprowadza bowiem odrębne od typologii umów przyjętej w k.c. definicje legalne pojęć „usługi", „dostawy" i „roboty budowlane". Podział zamówień publicznych przyjęty w ustawie p.z.p. znajduje zastosowanie głównie na gruncie postępowania o udzielenie zamówienia publicznego (chodzi tu o zróżnicowanie wymagań proceduralnych odnośnie do poszczególnych typów zamówień), zaś w zakresie materialnym (kontraktowym) należy posługiwać się kodeksową oraz pozakodeksową typologią umów cywilnoprawnych.

(5) Zgodnie z art. 2 pkt 2 p.z.p., pod pojęciem „dostawy" należy rozumieć nabywanie rzeczy oraz innych dóbr, w szczególności na podstawie umowy sprzedaży, dostawy, najmu, dzierżawy oraz leasingu z opcją lub bez opcji zakupu, które może obejmować dodatkowo rozmieszczenie lub instalację. Choć w porównaniu z poprzednią wersją cytowanej definicji (sprzed nowelizacji p.z.p. z 22 czerwca 2016 r.), ustawodawca polski z jej obecnej treści usunął nabycie "praw", zastępując je ogólnym pojęciem „innych dóbr", należy sądzić, iż zakres pojęcia „dostaw" nie uległ zmianie i w dalszym ciągu obejmuje ono także nabywanie praw. Przez prawa należy z kolei rozumieć majątkowe prawa podmiotowe, stanowiące przedmiot stosunków cywilnoprawnych, których respektowania podmiot ma prawo żądać. Będą to zatem nabywane na podstawie czynności prawnych uprawnienia do swobodnego podejmowania decyzji w granicach wyznaczonych treścią stosunku prawnego (np. autorskie prawa majątkowe)[39]. Z kolei art. 2 pkt 10 p.z.p. definiuje „usługi" jako wszelkie świadczenia, których przedmiotem nie są roboty budowlane lub dostawy**. Odpowiadając na pytanie, jak w świetle ustawy p.z.p. należy kwalifikować zamówienie publiczne na usługi chmurowe (w modelu SaaS) – tj. jako dostawę lub usługę – w pierwszej kolejności trzeba zatem rozstrzygnąć, czy zamówienie to może zostać uznane za dostawę.**

(6) **Zakwalifikowanie zamówienia na usługi chmurowe (SaaS) jako dostawy** może mieć miejsce w przypadku, gdy w ramach świadczenia tych usług zamawiający nabywa prawo do korzystania z oprogramowania. Taki stan rzeczy może zaś zachodzić w szczególności, gdy umowa SaaS zakładałaby

[39] P. Granecki, *Prawo zamówień publicznych. Komentarz*, uwagi do art. 2, LEX 2016.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

udzielenie licencji. W przypadku zaś, gdy umowa SaaS obejmowałaby wyłącznie przetwarzanie lub przechowanie danych przez wykonawcę, z wyłączeniem elementu korzystania z oprogramowania przez zamawiającego (a zatem umowa taka nie mogłaby zostać uznana za dostawę), **przedmiotowe zamówienie publiczne powinno zostać zakwalifikowane jako usługa**. Możliwy jest także wariant mieszany, w którym umowa SaaS obejmowałaby zarówno elementy korzystania z oprogramowania, jak i przetwarzanie oraz przechowywanie danych. W takim wypadku (tj. gdy dane zamówienie będzie obejmowało jednocześnie dostawy oraz usługi), zgodnie z art. 5c ust. 1 p.z.p., do udzielenia tego zamówienia stosować należy przepisy dotyczące rodzaju zamówienia, który odpowiada jego głównemu przedmiotowi. **Z powyższego wynika zatem, że kwalifikacja danego zamówienia publicznego, którego przedmiotem jest SaaS, jako dostawy lub usługi w rozumieniu ustawy p.z.p., zależy od konkretnego przypadku (specyfiki danej usługi SaaS)**.

(7) Praktyka pokazuje, że dostawcy usług chmurowych dzielą się na dwie grupy. Pierwsi oferują usługi *cloud computingu* w oparciu o umowę licencyjną. W większości przypadków są to dostawcy oprogramowania w modelu tradycyjnym, którzy zaczynają oferować je także w modelu SaaS. Z kolei druga grupa to dostawcy, którzy w większości dotychczas nie oferowali tradycyjnego oprogramowania i od razu rozpoczynają od modelu SaaS. Dostawcy ci najczęściej świadczą usługi chmurowe w oparciu o umowy o charakterze regulaminu świadczenia usługi drogą elektroniczną[40]. **Niezależnie od przyjętego modelu (licencja vs regulamin) istotną kwestią jest właściwe ukształtowanie treści umowy o zamówienie publiczne na usługi chmurowe przez zamawiającego. W zakresie przez nią nieuregulowanym zamawiający może być bowiem związany warunkami licencyjnymi/regulaminowymi, oferowanymi przez dostawcę usług chmurowych, które niejednokrotnie mogą przewidywać rozwiązania niekorzystne z punktu widzenia interesu zamawiającego**. Wyjściem z takiej sytuacji jest określenie przez zamawiającego w umowie o zamówienie publiczne niezbędnego minimum wymagań, które są kluczowe z jego perspektywy i które będzie musiał spełnić dostawca. W pozostałym zakresie mogłyby natomiast obowiązywać warunki licencyjne/regulaminowe dostawcy.

(8) Oddzielną kwestią jest natomiast to, czy dostawca usług chmurowych staje się formalnie stroną umowy o zamówienie publiczne? Częstą praktyką obserwowaną na rynku jest bowiem oferowanie usług chmurowych

[40] http://ipwsieci.pl/wpis,152,Cloud_computing__8211_i_proste_i_trudne_Cz_1.html



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

niebezpośrednio przez dostawców, lecz przez ich „pośredników" (partnerów biznesowych dostawców), którzy składają oferty w postępowaniach o udzielenie zamówienia publicznego niejako w imieniu dostawców. W takich przypadkach stronami umowy o zamówienie publiczne co do zasady stają się wyłącznie zamawiający oraz wykonawca – „pośrednik", a nie dostawca oprogramowania. **Praktyczną konsekwencją takiego stanu rzeczy jest to, że przepisy ustawy p.z.p. co do zasady będą stosowały się tylko do umowy o zamówienie publiczne, z wyłączeniem umów, porozumień lub regulaminów zawieranych dodatkowo przez zamawiającego z dostawcą usług chmurowych**. Wyjątek stanowi sytuacja, w której dokumenty te stanowiłyby integralną część umowy w sprawie zamówienia publicznego (np. jako załącznik).

(9) Z powyższego wynika także, że zamawiający zawierający umowę o zamówienie publiczne na usługi chmurowe z „pośrednikiem" ma ograniczony wpływ na kształt warunków licencyjnych/regulaminowych oferowanych przez dostawcę. W praktyce najczęściej jest on po prostu zmuszony zaakceptować warunki dostawcy. Sytuacji takiej można przeciwdziałać na dwa sposoby:

(a) wynegocjowanie bezpośrednio z dostawcą ogólnego porozumienia regulującego warunki licencyjne/regulaminowe dla nabywanego oprogramowania. W przypadku zawarcia takiego porozumienia, przy kolejnych zakupach „pośrednicy" byliby zobowiązani dostarczać usługi chmurowe na warunkach uzgodnionych w takim porozumieniu. Porozumienie mogłoby regulować wszystkie warunki licencyjne/regulaminowe w sposób kompleksowy lub koncentrować się jedynie na wybranych zagadnieniach – kluczowych z punktu widzenia zamawiającego. W tym drugim wypadku, w zakresie nieuregulowanym w porozumieniu, stosowane byłyby ogólne warunki licencyjne/regulaminowe dostawcy;

(b) określenie warunków licencyjnych/regulaminowych nabywanych usług chmurowych we wzorze umowy oddzielnie dla każdego zakupu (postępowania o udzielenie zamówienia publicznego). W takim wypadku ciężar wynegocjowania z dostawcą konkretnych warunków, wymaganych przez zamawiającego dla danego oprogramowania, zostałby przerzucony na „pośrednika". Zamawiający mógłby więc domagać się ich spełnienia wyłącznie od „pośrednika", z którym została zawarta umowa w sprawie zamówienia publicznego, a nie od dostawcy.

(10) Zawieranie umów na usługi chmurowe w reżimie zamówień publicznych ma jeszcze jedną specyficzną cechę. W świetle art. 142 p.z.p. generalną zasadą jest



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

bowiem zawieranie umów o zamówienie publiczne na czas oznaczony, nieprzekraczający 4 lat. Wyjątek stanowią umowy, których przedmiotem są dostawy licencji na oprogramowanie komputerowe, które, zgodnie z art. 143 ust. 1 pkt 5 p.z.p., mogą być zawierane na czas nieoznaczony. Jeśli zamawiający zdecydowałby się na zakup usług chmurowych na podstawie innej niż licencja, chcąc zapewnić ciągłość korzystania z usług chmurowych, musiałby on następnie zawierać kolejne umowy chmurowe, przeprowadzając w tym celu kolejne postępowania o udzielenie zamówienia publicznego. **Przy takim scenariuszu zamawiający powinien więc założyć odpowiedni margines czasowy na zorganizowanie nowego postępowania i zawarcie nowej umowy SaaS oraz odpowiednio uregulować w pierwotnej umowie kwestie dotyczące migracji danych – na wypadek zmiany dotychczasowego dostawcy usług chmurowych.**

(11) Z punktu widzenia p.z.p. istotną kwestią jest także należyte oszacowanie wartości zamówienia. W tym celu zamawiający powinien określić dokładną liczbę licencji/subskrypcji oprogramowania SaaS, które zamierza nabyć od wybranego wykonawcy.

[Pozycja dostawcy usług chmurowych w innych przetargach]

(12) Sytuacja, w której wykonawca świadczący usługi SaaS dla danego zamawiającego uczestniczyłby następnie w innych postępowaniach o udzielenie zamówienia publicznego, prowadzonych przez tego samego zamawiającego (przy których wykorzystywane byłoby dostarczane oprogramowanie SaaS, np. w celu weryfikacji ofert innych wykonawców), na pierwszy rzut oka może powodować pewne wątpliwości z punktu widzenia zasady uczciwej konkurencji (art. 7 ust. 1 p.z.p.). Teoretycznie można by bowiem twierdzić, że wykonawca dysponujący danymi zamawiającego przechowywanymi w chmurze, uczestnicząc w nowym postępowaniu, znalazłby w uprzywilejowanej sytuacji względem pozostałych wykonawców – np. mógłby w sposób nieuprawniony uzyskać dostęp do ofert innych wykonawców, co pozwoliłoby mu złożyć ofertę na korzystniejszych warunkach.

(13) **W naszej opinii takie stanowisko nie powinno jednak zasługiwać na uznanie.** Sam potencjalny dostęp dostawcy usług SaaS do danych zamawiającego przechowywanych w chmurze nie oznacza automatycznie, że dostawca z takiego dostępu skorzysta. Co więcej, w zdecydowanej większości przypadków działanie takie byłoby sprzeczne z warunkami na jakich świadczone są usługi SaaS, które, co do zasady, powinny zabraniać dostawcy



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893

wykorzystywania danych swoich klientów do własnych celów operacyjnych. Działanie takie należałoby więc uznać za nielegalne. **Zważywszy więc na to, że wystąpienie opisywanej sytuacji jest w praktyce mało prawdopodobne, sama hipotetyczna możliwość jej zaistnienia nie powinna powodować ryzyka w świetle przepisów p.z.p.** Wskazuje na to także praktyka rynkowa.

(14) Kwestia pozycji dostawcy w innych przetargach wiąże się także z zagadnieniem całkowitego lub częściowego uzależnienia zamawiającego od świadczonych przez niego usług SaaS (tzw. *vendor lock-in*). Zgodnie z wcześniejszymi uwagami, zamawiający powinien podjąć odpowiednie działania (w szczególności odpowiednio ukształtować treść umowy SaaS; uregulować kwestię migracji danych w przypadku zmiany dostawcy, opracować *exit plan, etc.*) w celu zapobieżenia sytuacji, w której byłby on *de facto* skazany na wybór dotychczasowego dostawcy SaaS w niekonkurencyjnym trybie z wolnej ręki. Taki scenariusz byłby bowiem ryzykowny zarówno z punktu widzenia przepisów ustawy p.z.p., jak i ustawy o odpowiedzialności za naruszenie dyscypliny finansów publicznych.



Maruta Wachta sp.j.

ul. Wspólna 62, 00-684 Warszawa
tel: +48 22 212 80 000, fax: +48 22 32 32 321, NIP: 676 01 11 300, REGON: 350653113, KRS: 0000083893