



You have downloaded a document from  
**RE-BUŚ**  
repository of the University of Silesia in Katowice

**Title:** Model usługi świadczonej w chmurze obliczeniowej a status administratora danych osobowych

**Author:** Wojciech Panek

**Citation style:** Panek Wojciech. (2019). Model usługi świadczonej w chmurze obliczeniowej a status administratora danych osobowych. W: S. Tkacz, Z. Tobor (red.), "Prawo a nowe technologie" (S. 128-136). Katowice : Wydawnictwo Uniwersytetu Śląskiego.



Uznanie autorstwa - Na tych samych warunkach - Licencja ta pozwala na kopiowanie, zmienianie, rozprowadzanie, przedstawianie i wykonywanie utworu tak długo, jak tylko na utwory zależne będzie udzielana taka sama licencja.

# Model usługi świadczonej w chmurze obliczeniowej a status administratora danych osobowych

WOJCIECH PANEK  
*Uniwersytet Śląski w Katowicach*

## Cloud computing services model vs the status of personal data controller

**Abstract:** The article examines the influence of the cloud computing service model on the status of a personal data controller, with reference to the Court of Justice of the European Union sentences in C-131/12 and C-210/16 cases. First, the author shortly characterises cloud computing and the service models based on it. Then, he subordinates the roles of the controller and the processor to the particular models of cloud computing. Finally, the author points out that in cloud computing relations the customer is a personal data controller, whereas the cloud provider depending on the model may be a processor or, in case of IaaS and PaaS models, might use disclaimer mechanisms included in the Act on Rendering Electronic Services.

**Keywords:** GDPR, cloud computing, data controller, processor, cloud models

## 1. Wstęp

Chmura obliczeniowa stanowi stosunkowo nowe narzędzie IT. Ze względu na swoje zalety<sup>1</sup> cieszy się sporym zainteresowaniem. Szeroki wachlarz możliwości stworzenia dopasowanej usługi, o czym będzie mowa dalej, powoduje, że chmura wykorzystywana jest do różnych celów. Jednym z nich jest obrót informacjami, z których spora część stanowi dane osobowe. Ze względu na przetwarzanie danych osobowych w chmurze stała się ona przedmiotem

---

<sup>1</sup> Na przykład związane z kwestią bezpieczeństwa: EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY: *Cloud Computing Benefits, risks and recommendations for information security*, 2012, s. 9–11, <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view> [Data dostępu: 28.11.2018 r.].

zainteresowania doktryny ochrony danych osobowych<sup>2</sup>, w szczególności zagadnienia ustalenia podmiotu będącego administratorem danych osobowych<sup>3</sup>. Celem niniejszego artykułu jest odpowiedź na pytanie, czy model usługi świadczonej w chmurze obliczeniowej ma wpływ na status określonego podmiotu jako administratora danych osobowych, z uwzględnieniem uwag dotyczących administratora poczynionych w wyrokach Trybunału Sprawiedliwości Unii Europejskiej [dalej: TSUE] w sprawach *Google Spain*<sup>4</sup> oraz *Wirtschaftsakademie Schleswig-Holstein GmbH*<sup>5</sup>. W pierwszej z nich, znanej przede wszystkim w kontekście rozstrzygnięcia o prawie do bycia zapomnianym, TSUE uznał za administratora danych osobowych podmiot będący operatorem wyszukiwarki internetowej<sup>6</sup>. W sprawie *Wirtschaftsakademie* status administratora danych osobowych został przyznany administratorowi fanpage'a prowadzonego na portalu społecznościowym<sup>7</sup>. W obu sprawach TSUE, rozstrzygając przedstawione pytania prejudycjalne, zawarł wskazówki, które mogą pomóc w dystynkcji roli administratora danych osobowych i podmiotu przetwarzającego.

## 2. Modele usług w chmurze obliczeniowej

Każdy z nas świadomie bądź nie choć raz skorzystał lub nadal korzysta z chmury. Jednak mało kto zastanawiał się nad tym, czym właściwie jest chmura obliczeniowa. Aby ułatwić zrozumienie dalszych wywodów, należy rozpocząć od krótkiej charakterystyki chmury.

---

<sup>2</sup> Między innymi: M. BRZOZOWSKA: *Ochrona danych osobowych w sieci*. Wrocław 2012, rozdz. 8; X. KONARSKI: *Przetwarzanie danych osobowych w chmurze obliczeniowej*. „Dodatek do Monitora Prawniczego” 2013, nr 8, s. 39–44; E. MOLENDĄ-KROPIELNICKA: *Cloud Computing – zagadnienia prawne*. „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” 2013, nr 119, s. 116–128; B. FISCHER: *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych – wybrane zagadnienia*. „Dodatek do Monitora Prawniczego” 2014, nr 9, s. 1012. Legalis; M. SIWICKI: *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajemnicy telekomunikacyjnej w chmurach obliczeniowych*. „Prokuratura i Prawo” 2015, nr 5, s. 120–126; IDEM: *Ochrona danych osobowych w zatrudnieniu w chmurze obliczeniowej*. „Monitor Prawniczy” 2016, nr 12, s. 654–659; A. KRASUSKI: *Chmura obliczeniowa. Prawne aspekty zastosowania*. Warszawa 2018, rozdz. V i VII.

<sup>3</sup> Między innymi: M. BRZOZOWSKA: *Ochrona danych osobowych...*, s. 224–226; E. MOLENDĄ-KROPIELNICKA: *Cloud Computing...*, s. 119–125; B. FISCHER: *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych...*; A. KRASUSKI: *Chmura obliczeniowa...*, s. 375–436.

<sup>4</sup> Wyrok Trybunału (Wielka Izba) C-131/12 z dnia 13 maja 2014 r. LEX nr 1455816.

<sup>5</sup> Wyrok Trybunału (Wielka Izba) C-210/16 z dnia 5 czerwca 2018 r. LEX nr 2497978.

<sup>6</sup> Punkt 41 wyroku C-131/12.

<sup>7</sup> Punkt 44 wyroku C-210/16.

W obrocie można spotkać różne definicje tego narzędzia<sup>8</sup>. Na przykład można przytoczyć definicję legalną zawartą w dyrektywie 2016/1148<sup>9</sup>, która w art. 4 pkt 19 wskazuje, że „usługa przetwarzania w chmurze oznacza usługę cyfrową, umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania”. Już sama lektura zaprezentowanej definicji sugeruje, że została ona dokonana przez wskazanie cech chmury. Również doktryna wyjaśnia pojęcie chmury, wymieniając jej różne cechy<sup>10</sup>. Pierwszą cechą jest wirtualizacja, dzięki której nie zmieniając sprzętu zyskujemy pomnożone zasoby teleinformatyczne, a łącznikiem między sprzętem a zasobami jest właściwe oprogramowanie<sup>11</sup>. Dzięki stosownej aplikacji użytkownik korzystający ze swojego wysłużonego sprzętu zyskuje dostęp do najnowocześniejszych zasobów, ponosząc jedynie koszty związane z subskrypcją usługi. Jest to cecha, bez której chmura nie może funkcjonować<sup>12</sup>. Kolejna cecha jest konsekwencją wirtualizacji, która powoduje, że lokalizacja użytkownika jest irrelevantna dla korzystania przez niego z subskrybowanej usługi, zatem w każdym miejscu, o każdej porze, jak najszybciej to możliwe wykorzystuje on usługę<sup>13</sup>. Istotną cechą jest elastyczność usług świadczonych w chmurze, niejako będąca efektem jej skalowalności<sup>14</sup>. Od potrzeb użytkownika uzależniony jest wybór dostawcy, konfiguracja usługi, w tym także jej zmiana, która może nastąpić w trakcie korzystania z chmury<sup>15</sup>. Szczególnie ważną cechą, która dodatkowo wpływa na wzrost zainteresowania chmurą, jest możliwość dzielenia się zasobami. Dostawca usług może wykorzystać te same zasoby dla świadczenia usługi na rzecz różnych użytkowników<sup>16</sup>, jak również sami użytkownicy mogą dzielić się z innymi podmiotami swoimi zasobami w chmurze i jednocześnie korzystać z nich w niezakłócony sposób<sup>17</sup>.

<sup>8</sup> Między innymi: A. KRASUSKI: *Chmura obliczeniowa...*, s. 48–55; E. MOLENDĄ-KROPIELNICKĄ: *Cloud Computing...*, s. 110–112; M. SIWICKI: *Ochrona praw autorskich...*, s. 111–112.

<sup>9</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dz.Urz. UE L 2016.194.1.

<sup>10</sup> Tak: A. KRASUSKI: *Chmura obliczeniowa...*, s. 58–61; M. SIWICKI: *Ochrona praw autorskich...*, s. 112–113; IDEM: *Prawo właściwe dla zobowiązań pozaumownych z naruszeń prawa autorskiego w chmurze obliczeniowej*. „Monitor Prawniczy” 2016, nr 22, s. 1209–1210.

<sup>11</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 59.

<sup>12</sup> Ibidem, s. 61.

<sup>13</sup> E. MOLENDĄ-KROPIELNICKĄ: *Cloud Computing...*, s. 112.

<sup>14</sup> Skalowalność w rozumieniu zaprezentowanym przez M. Siwickiego. M. SIWICKI: *Prawo właściwe dla zobowiązań pozaumownych...*, s. 1210.

<sup>15</sup> M. SIWICKI: *Ochrona praw autorskich...*, s. 113.

<sup>16</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 59.

<sup>17</sup> Ł. PIROŻEK: *Prawne aspekty świadczenia usług w modelu SaaS przez przedsiębiorcę telekomunikacyjnego*. „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2015, nr 6 (4), s. 74.

Dla tematu niniejszego artykułu podstawowe znaczenie ma przedstawienie poszczególnych modeli usług, z których można skorzystać w chmurze obliczeniowej. W swoim raporcie European Network and Information Security Agency [dalej: ENISA] wskazuje na trzy modele: Infrastructure as a Service – IaaS, Platform as a Service – PaaS, oraz Software as a Service – SaaS<sup>18</sup>.

Pierwszy z nich – IaaS – określany jest następująco – infrastruktura jako usługa. W ramach tego modelu dostawca zapewnia zasoby sprzętowe, np.: moc obliczeniową, natomiast użytkownik korzysta z tego środowiska za pośrednictwem Internetu, dostosowując infrastrukturę do własnych potrzeb przez instalację lub stworzenie odpowiedniego systemu operacyjnego, a następnie potrzebnych aplikacji. W efekcie to na nim spoczywają obowiązki związane m.in. z kwestią bezpieczeństwa zarówno systemu operacyjnego, jak i samych aplikacji<sup>19</sup>. Przykładem modelu usługi IaaS jest Microsoft Azure<sup>20</sup>. Kolejny model – PaaS, czyli platforma jako usługa – polega na udostępnieniu przez dostawcę odpowiedniego środowiska: sprzętu wraz z systemem operacyjnym<sup>21</sup>. Działanie użytkownika ogranicza się do stworzenia lub instalacji potrzebnej mu aplikacji oraz zarządzania nią. Wpływa to na zmianę kwestii odpowiedzialności za poszczególne elementy, za zabezpieczenia poniżej poziomu aplikacji<sup>22</sup>. Przykładem takiej usługi jest Google App Engine<sup>23</sup>. Usługa SaaS dostarcza użytkownikowi gotowy program. W tym modelu użytkownik korzysta z gotowej aplikacji oferowanej przez dostawcę, który odpowiada za wszystkie kwestie, począwszy od poziomu aplikacji<sup>24</sup>. Użytkownik zyskuje gotową aplikację, z której może korzystać, w tym oferować ją swoim klientom oraz wprowadzać pewne modyfikacje, ale tylko w takim zakresie, w jakim umożliwił to dostawca<sup>25</sup>, np. Gmail czy Piacasa albo YouTube<sup>26</sup>.

Poza wymienionymi modelami zaproponowanymi przez ENISA wyróżnia się także inne modele, jak np. Communication lub Data as a Service<sup>27</sup>, jednak będą one sprowadzać się do któregoś z wyżej wymienionych modeli podstawowych.

---

<sup>18</sup> EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY: *Cloud Computing Benefits, risks and recommendations for information security...*, s. 5.

<sup>19</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 62–67.

<sup>20</sup> E. MOLENDĄ-KROPIELNICKA: *Cloud Computing...*, s. 114.

<sup>21</sup> *Ibidem*, s. 113–114.

<sup>22</sup> J. KUDŁA, A. STASZAK: *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*. „Prokuratura i Prawo” 2017, nr 7–8, s. 40; A. KRASUSKI: *Chmura obliczeniowa...*, s. 68–70.

<sup>23</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 70.

<sup>24</sup> X. KONARSKI: *Przetwarzanie danych osobowych...*, s. 40.

<sup>25</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 72–73.

<sup>26</sup> E. MOLENDĄ-KROPIELNICKA: *Cloud Computing...*, s. 113.

<sup>27</sup> Ł. PIROŻEK: *Prawne aspekty świadczenia usług w modelu SaaS...*, s. 74.

Warto także zwrócić uwagę na podział na chmurę publiczną i prywatną. Kryterium tego rozróżnienia jest zasięg świadczonych usług<sup>28</sup> lub model wdrożenia<sup>29</sup>. Pozostawiając kwestię nomenklatury, istotą tego podziału jest ustalenie, do kogo skierowane są usługi. W przypadku chmury publicznej jej usługi w zasadzie są dostępne dla wszystkich<sup>30</sup>. Chmura prywatna oferuje usługi dla pewnego, określonego kręgu użytkowników.

### 3. Przetwarzanie danych osobowych w chmurze obliczeniowej

Stosunek prawny występujący między dostawcą usługi a użytkownikiem wywołuje wiele skutków prawnych. Jeśli usługa związana jest z przetwarzaniem danych osobowych, to pojawia się konieczność ustalenia, który z podmiotów: dostawca czy użytkownik, odgrywa rolę administratora danych osobowych.

Dla omawianego zagadnienia istotne są pojęcia administratora danych oraz podmiotu przetwarzającego. Definicję administratora danych osobowych zawiera art. 4 pkt 7 rozporządzenia 2016/679 w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych [dalej: RODO]<sup>31</sup>, według którego jest to „osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych”. Definicja ta nie różni się od pojęcia administratora danych zawartego w dyrektywie 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: dyrektywa 95/46]<sup>32</sup>. Artykuł 4 pkt 8 RODO definiuje podmiot przetwarzający jako „osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora”. Podobną definicję zawierał art. 2 pkt e dyrektywy 95/46.

Konieczność ustalenia podmiotów odgrywających rolę administratora i podmiotu przetwarzającego wynika z relacji zachodzących między nimi. To na administratorze spoczywa odpowiedzialność za przetwarzanie danych osobowych, także wtedy, gdy przetwarzanie odbywa się w jego imieniu<sup>33</sup>. Biorąc pod uwagę sankcje przewidziane w rozdziale VIII RODO, zarówno dostawca, jak i użytkownik będą dążyli do ograniczenia ponoszonej odpowiedzialności.

<sup>28</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 75.

<sup>29</sup> X. KONARSKI: *Przetwarzanie danych osobowych...*, s. 39.

<sup>30</sup> Ibidem.

<sup>31</sup> Dz.Urz. UE L 2016.119.1.

<sup>32</sup> Dz.Urz. UE L 1995.281.31.

<sup>33</sup> Motyw 74 RODO.



Doktryna dość zgodnie przyjmuje, że w przypadku przetwarzania danych osobowych w chmurze to użytkownik jest administratorem danych osobowych, a dostawca usługi – podmiotem przetwarzającym<sup>34</sup>. Ponadto, jak wskazuje Andrzej Krasuski, „statusu współadministratora danych nie można przypisać dostawcy usług w chmurze [...], gdyż realizuje cele przetwarzania, dla których zleciłodawca, będący administratorem danych, pozyskał podstawę przetwarzania danych [...]”<sup>35</sup>. Przyjrzyjmy się zatem, czy model świadczonej usługi modyfikuje przydzielone role.

Jak już wskazano, model IaaS polega na udostępnieniu przez dostawcę infrastruktury. W zasadzie na tym jego rola się kończy. Reszta pozostaje w gestii użytkownika. To on podejmuje decyzje w sprawie właściwego systemu operacyjnego, wprowadza określoną aplikację. W przypadku danych osobowych to on ustala „cel i sposoby przetwarzania danych osobowych”<sup>36</sup>. W zasadzie nie ulega wątpliwości, że użytkownika należy uznać za administratora. Może zdarzyć się tak, że dostawca będzie miał wpływ na określenie sposobów przetwarzania, np. regulując kwestie bezpieczeństwa na poziomie posiadanej infrastruktury. Nie będzie to jednak wpływ rozpatrywany w kategorii „zasadniczych elementów”, które rozstrzygają o statusie administratora<sup>37</sup>. W przypadku tego modelu możliwe jest inne rozwiązanie. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług elektronicznych<sup>38</sup> przewiduje mechanizmy wyłączające odpowiedzialność usługodawcy. Są nimi: prosty przekaz, *caching* i *hosting*<sup>39</sup>. Dla omawianego tematu szczególnie przydatne są pierwszy i ostatni z nich. Prosty przekaz polega na tym, że dostawca tylko transmituje dane, nie dokonując modyfikacji ich treści, a odpowiedzialność jest wyłączona, jeśli jednocześnie nie jest inicjatorem przekazu danych, nie wybiera odbiorcy przekazu danych oraz nie wybiera i nie modyfikuje informacji zawartych w przekazie<sup>40</sup>. *Hosting* związany jest z usługą przechowywania danych na udostępnionych zasobach systemu teleinformatycznego, przy czym nieponoszenie odpowiedzialności będzie miało miejsce, jeśli usługodawca nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocz-

<sup>34</sup> Tak m.in.: M. BRZOZOWSKA: *Ochrona danych osobowych...*, s. 224–226; X. KONARSKI: *Przetwarzanie danych osobowych...*, s. 40–41; M. SIWICKI: *Ochrona danych osobowych...*, s. 656; B. FISCHER: *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych...*; A. KRASUSKI: *Chmura obliczeniowa...*, s. 375–436.

<sup>35</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 394.

<sup>36</sup> Artykuł 4 pkt 7 RODO.

<sup>37</sup> X. KONARSKI: *Przetwarzanie danych osobowych...*, s. 40.

<sup>38</sup> Dz.U. 2017.1219 j.t.

<sup>39</sup> J. BARTA, P. FAJGIELSKI, R. MARKIEWICZ: *Ochrona danych osobowych. Komentarz*. Warszawa 2015, s. 214–215.

<sup>40</sup> Artykuł 12 ust. 1 ustawy o świadczeniu usług drogą elektroniczną.

nie uniemożliwi dostęp do tych danych<sup>41</sup>. W przypadku usługi IaaS możliwe jest wystąpienie obu tych mechanizmów, co wynika z istoty tego modelu. Wszystko zależy jednak od konkretnego przypadku. Co prawda w pkt. 34 wyroku w sprawie Google Spain TSUE stwierdza, że „sprzeczne zarówno z wyraźnym brzmieniem tego przepisu, lecz również z jego celem – polegającym na zapewnieniu, poprzez przyjęcie szerokiej definicji pojęcia »administratora«, skutecznej i pełnej ochrony osobom, których dotyczą dane – byłoby wyłączenie z zakresu jego stosowania operatora wyszukiwarki internetowej ze względu na to, iż nie sprawuje on kontroli nad danymi osobowymi opublikowanymi na stronach internetowych osób trzecich”, jednak nie sposób stwierdzić, że owa uwaga odnosi się także do dostawcy usługi IaaS. Takie stanowisko TSUE wynika z funkcji wyszukiwarki internetowej, które zostały opisane m.in. w pkt. 41 wyroku, a polegają „na zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie ich udostępnianiu internautom w sposób uporządkowany zgodnie z określonymi preferencjami [...]”. Model IaaS znacznie różni się od działalności przeglądarki. Dostawca nie ingeruje w treści gromadzone przez użytkownika, nie przegląda ich. Brak takiego obowiązku wynika także z art. 15 ustawy o świadczeniu usług drogą elektroniczną, który stanowi, że dostawca „nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych [...]”. Jak słusznie zauważają Janusz Barta, Paweł Fajgielski i Ryszard Markiewicz, „obowiązek taki byłby zresztą ze względów technicznych trudny do wykonania (jeśli w ogóle możliwy), a co ważniejsze oznaczałby naruszenie gwarantowanej w art. 49 Konstytucji RP wolności i tajemnicy komunikowania się”<sup>42</sup>. Mając na względzie powyższe uwagi, należy stwierdzić, że w przypadku modelu IaaS dostawca chmury może być uznany za przetwarzającego dane, ale możliwe jest także skorzystanie z wyłączenia odpowiedzialności i uznanie go za dokonującego prostego przekazu czy hostingu<sup>43</sup>.

W modelu PaaS oferowana usługa przechodzi na inną płaszczyznę działania<sup>44</sup>. Dostawca zapewnia środowisko pracy, w którym użytkownik może tworzyć albo instalować gotowe aplikacje. W takim ujęciu aktualne pozostają uwagi dotyczące modelu IaaS, zatem uznanie dostawcy za podmiot przetwarzający albo dokonujący hostingu.

Zupełnie inaczej jawi się kwestia modelu SaaS. Użytkownik otrzymuje od dostawcy gotową aplikację, z której korzystanie może polegać na przetwarzaniu danych osobowych. Pozornie może się wydawać, że role dostawcy i użytkownika zostają zmienione. Wiąże się to przede wszystkim z rolą dostawcy w tym

<sup>41</sup> Artykuł 14 ust. 1 ustawy o świadczeniu usług drogą elektroniczną.

<sup>42</sup> J. BARTA, P. FAJGIELSKI, R. MARKIEWICZ: *Ochrona danych osobowych...*, s. 215.

<sup>43</sup> M. BRZOZOWSKA: *Ochrona danych osobowych...*, s. 226.

<sup>44</sup> M. SIWICKI: *Ochrona praw autorskich...*, s. 113.



modelu. To on zapewnia zarówno wszystkie płaszczyzny poniżej aplikacji, jak i samą aplikację, decydując o mechanizmach bezpieczeństwa, a przede wszystkim o danych, które będą przetwarzane w razie korzystania z tej aplikacji, powodując, że rola użytkownika jest w zasadzie marginalna i sprowadza się „tylko” do wyboru dostawcy i jego usługi, z niewielkim wpływem na aplikację i jej mechanizmy<sup>45</sup>. Jednak w dalszym ciągu dostawca pozostaje podmiotem przetwarzającym. Dobrze obrazuje to wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009 r., I OSK 227/09<sup>46</sup>, w którym ten rozstrzygnął kwestię uznania za administratora danych osobowych banku, który oferował imiennie przedpłacone karty płatnicze. Jak słusznie wskazuje Damian Karwala w głosie do wyroku I OSK 227/09, „bank, oferując określony produkt, zdefiniował tym samym (niejako »z góry«) ogólne warunki przetwarzania danych osobowych, w szczególności sposób i środki ich przetwarzania, a także – w pewnym zakresie – również cel ich przetwarzania, który związany jest ściśle z tego rodzaju produktem [...]. W tego rodzaju relacjach status administratora danych przyznawany powinien być podmiotowi korzystającemu z tego rodzaju produktów [...], podmiot oferujący na rynku określony produkt określa jedynie ogólne warunki przetwarzania danych osobowych. Klient natomiast, korzystający z tego produktu (np. posiadacz kart przedpłaconych), decyduje o szczegółach tego korzystania [...]. Co do zasady zatem podmiot tworzący określony produkt (np. program motywacyjny lub marketingowy), w tym również określający warunki przetwarzania danych osobowych w jego ramach, powinien być kwalifikowany jako tzw. *processor* danych [...]”<sup>47</sup>. Podobnie będzie w przypadku modelu SaaS, gdzie to użytkownik będzie w konkretnej sytuacji korzystał z aplikacji, mając bezpośredni wpływ na przetwarzanie danych osobowych, spełniając tym samym przesłanki uznania go za administratora danych osobowych. Co prawda, w powołanej sprawie bank został uznany za administratora danych osobowych, jednak jak wskazuje autor glosy: „Na status banku jako administratora danych w tej konkretnej sprawie wpływ mają inne okoliczności, związane ze specyfiką produktów bankowych [...]”<sup>48</sup>. W innym kontekście podobne stanowisko wyraził TSUE w sprawie *Wirtschaftsakademie*. W pkt. 36 wyroku TSUE wskazuje, że „utworzenie fanpage’a na Facebooku wiąże się z podjęciem przez jego administratora działań, polegających na ustaleniu parametrów zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakre-

<sup>45</sup> Opinia 05/2012 Grupy Roboczej art. 29, przyjęta 1 lipca 2012 r., WP196, s. 8, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf) [Data dostępu: 28.11.2018 r.]; E. MOLENDĄ-KROPIELNICKA: *Cloud Computing...*, s. 125.

<sup>46</sup> LEX nr 579124.

<sup>47</sup> D. KARWALA: Glosa do wyroku NSA z dnia 1 grudnia 2009 r., I OSK 227/09, oraz do wyroku WSA z dnia 5 grudnia 2008 r., II SA/Wa 1242/08. LEX/el 2013.

<sup>48</sup> *Ibidem*.

sie zarządzania lub promocji jego działalności, co wpływa na przetwarzanie danych osobowych na potrzeby statystyk sporządzonych na podstawie liczby odwiedzających fanpage'a. Ów administrator może za pomocą filtrów udostępnionych przez Facebook zdefiniować kryteria, na podstawie których statystyki te muszą być sporządzane, a nawet określić kategorie osób, których dane osobowe będą wykorzystywane przez Facebook. W konsekwencji administrator fanpage'a prowadzonego na Facebooku przyczynia się do przetwarzania danych osobowych osób odwiedzających jego stronę". Konkludując, także w przypadku modelu SaaS co do zasady to dostawca usługi jest podmiotem przetwarzającym, natomiast użytkownik odgrywa rolę administratora danych osobowych.

Poza wymienionymi podziałami ról, stanowiącymi regułę, możliwa jest jednak także sytuacja, w której dostawca będzie administratorem danych osobowych. Będzie to miało miejsce wtedy, gdy w przypadku świadczenia któregoś z modeli usług – wydaje się, że w grę wchodzi tylko model SaaS – dostawca będzie wykorzystywał dane do własnych celów<sup>49</sup>. Będzie to jednak skutek zmiany celu, który powoduje zmianę jego roli<sup>50</sup>. Przykładem takiego działania jest wykorzystywanie plików cookies przez Facebooka, opisane w motywach 33 i 34 wyroku w sprawie *Wirtschaftsakademie*.

#### 4. Podsumowanie

Podsumowując, model usługi świadczonej w chmurze obliczeniowej przez dostawcę wpływa na jego status. W przypadku modeli IaaS i PaaS, poza sytuacją uznania go za podmiot przetwarzający, możliwe jest zastosowanie mechanizmów wyłączających odpowiedzialność, które zostały przewidziane przez ustawę o świadczeniu usług drogą elektroniczną. Ze względu na istotę usługi świadczonej w ramach modelu SaaS dostawca występuje w roli podmiotu przetwarzającego. Jednak powyższe uwagi dotyczą przede wszystkim modelowych rozwiązań. Komplikacja może wynikać m.in. z sytuacji, gdy sam dostawca będzie jednocześnie użytkownikiem, zwłaszcza w modelu SaaS, gdy dla stworzenia swojej usługi korzysta z modeli IaaS czy PaaS, oferowanych przez innych dostawców<sup>51</sup>. Może to spowodować utrudnienie ustalenia podziału ról administratora i podmiotu przetwarzającego<sup>52</sup>. Dla uniknięcia takiej sytuacji właściwym rozwiązaniem będzie doprecyzowanie ról i ponoszonej odpowiedzialności w ramach zawieranej umowy<sup>53</sup>.

<sup>49</sup> Opinia 05/2012, s. 8.

<sup>50</sup> A. KRASUSKI: *Chmura obliczeniowa...*, s. 394.

<sup>51</sup> *Ibidem*, s. 379.

<sup>52</sup> X. KONARSKI: *Przetwarzanie danych osobowych...*, s. 40.

<sup>53</sup> M. BRZOWSKA: *Ochrona danych osobowych...*, s. 224–225.