



# Software as a Service

Wymiar prawny

Model SaaS stał się kluczowy w dostarczaniu oprogramowania. Obecnie jest on zaliczany do głównego nurtu rozwiązań na rynku IT. Jednakże jakkolwiek prosty i korzystny się wydaje, jest wiele aspektów prawnych, na które warto zwrócić uwagę - od licencji i warunków umów po bezpieczeństwo danych i prywatność informacji.

### Płać jak chcesz

Problem zaczyna się zwykle już od umowy licencyjnej: Czy klient powinien płacić z góry czy z dołu? Jakie rodzaje licencji są stosowane? Odpowiedzi na te pytania mogą się różnić w zależności od kraju i praktyki prawnej. Na początku funkcjonowania SaaS, dostawcy mogli wybrać pomiędzy licencjonowaniem oprogramowania lub usługi. Druga opcja jest obecnie bardziej powszechna, może być powiązana z umowami typu Try and Buy i daje dostawcy większą elastyczność. Ponadto, licencjonowanie produktu jako usługi w USA dostarcza ogromnych korzyści dla klienta, gdyż usługi są tam zwolnione z opodatkowania.

Najważniejszy jest jednak wybór między subskrypcją a licencją na żądanie. Pierwsza opcja wymaga płatności miesięcznych, rocznych, itd., bez względu na potrzeby i wykorzystanie oprogramowania, podczas gdy druga oznacza płacenie na bieżąco za użycie. Warto zauważyć, że użytkownik płaci nie tylko za oprogramowanie, ale także za hosting, bezpieczeństwo danych i ich przechowywanie. Założenie, że umowa dotyczy bezpieczeństwa danych sprawia, że jakiegokolwiek jej naruszenie może spowodować pozwanie dostawcy. Ta sama sytuacja dotyczy złej jakości usługi lub przestoju serwerów, dlatego warunki umowy powinny być ustalane z należytą uwagą.

### Bezpieczne czy nie?

Klientów najbardziej martwi utrata danych lub naruszenie bezpieczeństwa. Dostawcy powinni zatem pamiętać, aby powziąć niezbędne działania w celu uniknięcia takiej sytuacji. Mogą również brać pod uwagę certyfikowanie poszczególnych usług w oparciu o świadectwo SAS 70, które określa profesjonalne standardy wykorzystywane do szacowania dokładności wykonania i bezpieczeństwa usługi. Taki wymiar kontroli jest szeroko uznawany w USA. W obrębie Unii Europejskiej zaleca się postępowanie oparte na dyrektywie 2002/58/EC, dotyczącej prywatności i łączności elektronicznej. Dyrektywa zakłada, iż dostawca publicznie dostępnych usług łączności elektronicznej „musi podjąć odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa swoich usług” (art. 4). Jest to kontynuacja poprzedniej dyrektywy - 95/46/EC – dotyczącej ochrony danych osobowych. Każde unijne i amerykańskie przedsiębiorstwo gromadzące dane osobowe może też wybrać program Safe Harbor, aby otrzymać unijny certyfikat zgodności z Dyrektywą o ochronie danych. Takie przedsiębiorstwa lub organizacje muszą jednak odnawiać certyfikat co 12 miesięcy. Należy pamiętać, iż wszystkie działania prawne podejmowane w przypadku naruszenia umowy lub innych problemów związanych z bezpieczeństwem, będą zależały od miejsca gdzie przedsiębiorstwo i centra danych się znajdują, gdzie znajduje się klient lub od tego, jakiego typu dane są używane, itd. Wobec tego wskazane jest konsultowanie się z kompetentnym doradcą odnośnie prawa, które powinno zostać zastosowane w danej sytuacji.

### Strzeż się cyberprzestępstw

Dostawca, podobnie jak klient, powinien pamiętać, że żaden system bezpieczeństwa nie jest w stu procentach niezawodny. Zaleca się zatem dostawcom ograniczanie swoich zobowiązań w zakresie zapewnienia bezpieczeństwa. W razie wystąpienia naruszenia, klient może pozwać dostawcę za wprowadzenie w błąd. Według Konwencji o cyberprzestępczości z Budapesztu, osoba prawna „może zostać pociągnięta do odpowiedzialności, gdy brak nadzoru lub kontroli ze strony osoby fizycznej [...] umożliwił popełnienie przestępstwa” (art. 12). 44 stany w USA nałożyły zarówno na dostawców, jak i klientów obowiązek zgłaszania osobom, których dane są posiadane przez firmę, każdego przypadku naruszenia bezpieczeństwa. Decyzja kto jest osobą odpowiedzialną zostaje podjęta przez umowę między dostawcą SaaS i klientem. W tym wypadku podobnie zaleca się ostrożne negocjacje.

### SLA

Kolejnym zagadnieniem jest SLA (ang. Service Level Agreement - umowa o poziomie jakości usług). Jest to kluczowa część umowy między dostawcą a klientem. Oczywiście dostawca może uniknąć wiązania się jakimikolwiek zobowiązaniami, jednak podpisanie SLA jest decyzją biznesową wymaganą do konkurencji na wysokim szczeblu. Jeśli raporty wykonania są dostępne dla klienta, z pewnością poczuje się on pewniej.

Jakie rodzaje SLA są zatem wymagane i wskazane? Minimum jest wsparcie i dostępność systemu (uptime), „pięć dziewiątek” (uptime wynoszący 99,999%) jest pożądanym poziomem niezawodności, oznaczającym zaledwie pięć minut przestoju rocznie. Jednak wiele czynników przyczynia się do niezawodności systemu, co powoduje trudności w szacowaniu możliwych poziomów dostępności i niezawodności. Zatem ponownie dostawca powinien pamiętać o podaniu rozsądnych wartości, aby uniknąć zerwania umowy przez klienta, jeśli czas przestoju się wydłuży. Zwykle rozwiązaniem są kredyty na przyszłe usługi zamiast zwrotu kosztów, chronią one przed zerwaniem umowy przez klienta.

### Wskazówki

- Zawsze negocjuj długoterminowe płatności z góry. Nieprzekonani klienci mogą płacić co kwartał, nie corocznie.
- Nigdy nie domagaj się doskonałego bezpieczeństwa i jakości usługi. Nawet główni dostawcy mogą doświadczać przestojów lub naruszenia umowy.
- Nigdy nie zgadzaj się na zwrot kosztów usług kontraktowanych przed rozwiązaniem umowy. Nie chcesz przecież, aby Twoja firma zbankrutowała przez naruszenie jednej umowy lub gwarancji.
- Nigdy nie lekceważ zagadnień prawnych dotyczących SaaS, każdy dostawca powinien uważnie prześledzić umowę.

Dokumenty wspomniane w artykule			
sygnatariusz	nazwa	tematyka dokumentu	strona
UE	Dyrektywa 2002/58/EC	Dyrektywa dotycząca prywatności i łączności elektronicznej	<a href="#">link</a>
UE	Dyrektywa 95/46/EC	Dyrektywa o ochronie jednostek z uwzględnieniem przetwarzania danych osobowych i ich swobodnego przepływu	<a href="#">link</a>
UE + Kanada, Japonia, USA, RPA	Konwencja o Cyberprzestępczości		<a href="#">link</a>
UE-USA	2000/520/EC	Zasada Safe harbor	<a href="#">link</a>

Jeżeli są Państwo zainteresowani szczegółowymi informacjami dotyczącymi rozwiązań SaaS, zapraszamy do kontaktu z naszym konsultantem na [www.veraxsystems.com](http://www.veraxsystems.com).