

12 punktów audytu umowy SaaS

Praktyczny przewodnik po kluczowych ryzykach kontraktów
Software-as-a-Service. Co sprawdzić przed podpisaniem — oczami
radcy prawnego specjalizującego się w prawie IT.

Wprowadzenie

Umowa SaaS to dziś jeden z najczęściej zawieranych kontraktów technologicznych. Jednocześnie — jeden z najczęściej podpisywanych bez realnego zrozumienia ryzyk. Standardowe wzorce dostawców („our standard terms”) z reguły faworyzują dostawcę i pozostawiają klientowi bardzo wąski margines roszczeń.

Ten materiał to wyciąg z 12 obszarów, które weryfikuję w każdej umowie SaaS — niezależnie od tego, czy wartość kontraktu to 5 tys. czy 5 mln złotych. Każdy punkt zawiera konkretne pytania, na które warto znać odpowiedź *przed* podpisaniem, oraz typowe „red flagi”, które powinny wzbudzić czujność.

JAK KORZYSTAĆ Z CHECKLISTY

Przejdź przez 12 punktów z umową w drugiej ręce. Zaznacz pozycje, które masz rozstrzygnięte. Te bez odpowiedzi to obszary do negocjacji albo do dalszej weryfikacji prawnej. Szczególną uwagę zwróć na sekcje oznaczone jako „Red flag”.

DLA KOGO TEN MATERIAŁ

Dla CTO, COO, dyrektorów IT i dyrektorów zakupów weryfikujących umowy SaaS przed podpisaniem. Dla zespołów prawnych potrzebujących szybkiego frameworka do pierwszej oceny ryzyk. Dla startupów wybierających kluczową infrastrukturę.

CZEGO TEN MATERIAŁ NIE ZASTĘPUJE

Indywidualnej analizy prawnej. Każda umowa funkcjonuje w konkretnym kontekście biznesowym, regulacyjnym i operacyjnym — checklist to punkt wyjścia, nie substytut doradztwa.

12 punktów audytu

01

Przedmiot usługi i zakres funkcjonalny

Czym dokładnie jest „usługa”? Wzorce SaaS często odsyłają do dynamicznej dokumentacji online, którą dostawca może jednostronnie modyfikować. Brak precyzyjnego opisu funkcjonalności to brak podstawy do roszczeń, gdy kluczowa funkcja zniknie po update.

- ☐ Czy zakres funkcjonalny jest opisany w załączniku — czy tylko przez link do strony WWW dostawcy?
- ☐ Czy dostawca może jednostronnie usuwać funkcje? Z jakim wyprzedzeniem?
- ☐ Czy wskazane są konkretne wersje, środowiska, integracje?

RED FLAG

Klauzula „We may modify the Services at any time at our sole discretion” bez okresu wypowiedzenia po stronie klienta.

02

SLA i konsekwencje niedostępności

„99,9% uptime” brzmi imponująco do momentu, gdy zobaczysz definicję „Dostępności” oraz katalog wyłączeń. Często okazuje się, że okno serwisowe, „force majeure” i działania osób trzecich pochłaniają większość ryzyka.

- ☐ Jak liczona jest dostępność (miesięcznie, kwartalnie, rocznie)?
- ☐ Co jest wyłączone z SLA (planned maintenance, beta, third-party)?
- ☐ Jaki jest service credit i czy jest jedynym środkiem (sole remedy)?
- ☐ Czy istnieje próg uprawniający do wypowiedzenia bez kary?

RED FLAG

Service credit jako „sole and exclusive remedy” + niski próg kar (np. 5% MRR) bez prawa do wypowiedzenia umowy.

03

Powierzenie przetwarzania danych (DPA)

Każda umowa SaaS, w której dostawca przetwarza dane osobowe klienta (czyli praktycznie każda), wymaga DPA spełniającej art. 28 RODO. Brak DPA = naruszenie po stronie administratora (Twojej firmy).

- ☐ Czy DPA jest załącznikiem do umowy i obejmuje wszystkie kategorie danych?
- ☐ Czy lista subprocesorów jest aktualna i zatwierdzona?
- ☐ Czy są klauzule SCC (Standard Contractual Clauses) dla transferów poza EOG?
- ☐ Jakie są obowiązki dostawcy przy wsparciu w odpowiedziach na żądania osób, których dane dotyczą?
- ☐ Jaki jest mechanizm notyfikacji o naruszeniu (24h, 48h, 72h)?

RED FLAG

Brak DPA / DPA jednostronnie modyfikowalna / transfer do USA bez SCC i bez DPF certification.

04

Bezpieczeństwo informacji i certyfikacje

Deklaracje typu „we take security seriously” nie mają żadnej wartości prawnej. Liczą się konkretne zobowiązania: certyfikacje, audyty, mechanizmy szyfrowania, polityki backup i prawo do audytu po stronie klienta.

- ☐ Czy dostawca posiada ISO 27001, SOC 2 Type II, ewentualnie inne właściwe certyfikaty?
- ☐ Czy klient ma prawo do audytu (lub raportów z audytów niezależnych)?
- ☐ Czy zdefiniowano standardy szyfrowania w spoczynku i w tranzycie?
- ☐ Czy określono RTO / RPO (Recovery Time / Recovery Point Objective)?
- ☐ Jak klasyfikowane są incydenty i jakie są terminy zgłoszeń?

05

Prawa do danych i exit data

Najczęściej pomijany, a najgroźniejszy w praktyce obszar. Po zakończeniu umowy klient musi mieć realną możliwość odzyskania swoich danych — w użytecznym formacie, w rozsądnym terminie, bez dodatkowych opłat.

- ☐ Kto jest właścicielem danych? (zawsze powinien być klient)
- ☐ Jaki jest format eksportu (CSV, JSON, full DB dump)?
- ☐ Ile czasu po zakończeniu umowy dane są dostępne do pobrania?
- ☐ Czy są opłaty za eksport / migrację / wsparcie przy migracji?
- ☐ Kiedy i jak dostawca usuwa dane oraz jak to dokumentuje?

RED FLAG

„Upon termination, Customer Data will be deleted within 30 days" bez zagwarantowanego eksportu w czytelnym formacie.

06

Limitacja odpowiedzialności i caps

Standardowa klauzula ogranicza odpowiedzialność do równowartości 12-miesięcznych opłat. Gdy SaaS przetwarza dane wrażliwe albo jest krytyczny dla operacji, taki cap to fikcja zabezpieczenia.

- ☐ Jaki jest ogólny limit (12-miesięczny? niższy?)
- ☐ Czy są wyłączenia z capa (data breach, IP infringement, gross negligence)?
- ☐ Czy wzajemność limitów jest zachowana?
- ☐ Czy są wyłączone szkody pośrednie / utracone korzyści — i czy to wzajemne?

RED FLAG

Cap niższy niż 12 miesięcy + brak super-cap dla naruszeń ochrony danych + jednostronne wyłączenie szkód pośrednich (tylko po stronie dostawcy).

07

Indemnification — gwarancja IP

Korzystając z SaaS, korzystasz z czyjegoś kodu. Jeśli dostawca naruszy prawa autorskie lub patenty, roszczenia mogą trafić również do Ciebie. Klauzula indemnification powinna chronić klienta przed takim ryzykiem.

- ☐ Czy dostawca zobowiązuje się do obrony klienta przed roszczeniami osób trzecich z tytułu naruszenia IP?
- ☐ Czy obejmuje to również koszty postępowania i ugody?
- ☐ Jakie są wyjątki (modyfikacje przez klienta, użycie niezgodne z dokumentacją)?
- ☐ Czy istnieje obowiązek dostarczenia alternatywnego rozwiązania w razie sporu?

08

Cennik, indeksacja i odnowienia

Auto-renewal + jednostronna podwyżka + krótkie okno wypowiedzenia to klasyczna pułapka SaaS. Roczna umowa zamienia się w wieloletni kontrakt z rosnącą ceną.

- ☐ Czy umowa odnawia się automatycznie? Z jakim wyprzedzeniem trzeba ją wypowiedzieć?
- ☐ Jaka jest formuła indeksacji (CPI, sztywny %, dyskrejacja dostawcy)?
- ☐ Czy podwyżka wymaga akceptacji, czy „milczącego przyjęcia”?
- ☐ Czy są price locki na pierwsze X lat?

RED FLAG

Auto-renewal + 90-dniowe wypowiedzenie + „at our then-current rates” bez ograniczenia wzrostu.

09

Wypowiedzenie i mechanizmy exitu

Symetria praw do wypowiedzenia to rzadkość. Dostawca z reguły rezerwuje sobie szerokie podstawy (naruszenie polityki, zaleganie z płatnością) przy bardzo ograniczonych prawach klienta.

- ☐ Jakie są podstawy wypowiedzenia po obu stronach?
- ☐ Czy jest okres na uzdrowienie naruszenia (cure period)?
- ☐ Czy klient może wypowiedzieć przy istotnej zmianie usługi / DPA / cen?
- ☐ Co dzieje się z opłatami z góry przy wypowiedzeniu z winy dostawcy?

10

Prawo właściwe i jurysdykcja

Wzorce międzynarodowych dostawców z reguły wskazują na prawo Delaware/Kalifornii i arbitraż w USA. Dla polskiej spółki to często praktyczne wyłączenie roszczeń.

- ☐ Jakie prawo jest właściwe?
- ☐ Gdzie i jak rozstrzygane są spory (sąd, arbitraż, mediacja)?
- ☐ Czy klauzula jurysdykcyjna jest skuteczna wobec polskich konsumentów / B2B?
- ☐ Czy nie wyłączono przepisów semi-imperatywnych prawa polskiego?

11

Zgodność z AI Act i wykorzystanie danych do trenowania

Coraz więcej SaaSów rezerwuje sobie prawo do wykorzystywania danych klienta do trenowania modeli AI. To kluczowy obszar w 2026 roku — szczególnie wobec AI Act i obowiązków transparentności.

- ☐ Czy dane klienta są używane do trenowania modeli? Czy istnieje opt-out?
- ☐ Czy są moduły AI w usłudze? Jaką rolę pełni dostawca w rozumieniu AI Act?
- ☐ Czy klient otrzymuje dokumentację techniczną wymaganą dla systemów wysokiego ryzyka?
- ☐ Jak wygląda klasyfikacja systemu (zakazany / wysokiego ryzyka / GPAI)?

12

Zmiany regulaminu i polityk

Ostatni — i często najgroźniejszy — punkt. Klauzule typu „We may update these Terms at any time” sprawiają, że umowa, którą podpisałeś, w praktyce nie istnieje. Liczy się to, co dostawca napisze w portalu w przyszłym tygodniu.

- ☐ Czy regulamin / polityki mogą być jednostronnie zmieniane?
- ☐ Z jakim wyprzedzeniem klient jest informowany o zmianach?
- ☐ Czy istotne zmiany dają prawo do wypowiedzenia bez kary?
- ☐ Co się dzieje przy braku akceptacji zmian (terminacja czy automatyczne przyjęcie)?

RED FLAG

„Continued use of the Services constitutes acceptance of the updated Terms” — bez prawa do wypowiedzenia.

Co dalej

Te 12 punktów to framework — nie wyrok. Każda umowa SaaS funkcjonuje w innym kontekście biznesowym, regulacyjnym i negocjacyjnym. Niektóre klauzule, które w jednej sytuacji są red flagiem, w innej będą rynkowym standardem.

Jeśli masz przed sobą konkretną umowę i potrzebujesz oceny ryzyk, negocjacji z dostawcą albo opracowania własnego wzorca — chętnie pomogę.

Konsultacja w sprawie Twojej umowy

Pierwsza konsultacja jest bezpłatna. W 30 minut jesteśmy w stanie wskazać kluczowe ryzyka konkretnego kontraktu i zaproponować priorytety negocjacyjne.

E-MAIL

dbudzis@bskp.legal

TELEFON

+48 516 220 143

WWW

bskp.legal

Zastrzeżenie: Niniejszy materiał ma charakter wyłącznie edukacyjny i informacyjny. Nie stanowi opinii prawnej, porady prawnej ani świadczenia pomocy prawnej w rozumieniu ustawy o radcach prawnych. Zastosowanie konkretnych klauzul i ich ocena zależy od okoliczności konkretnej sprawy. Przed podjęciem decyzji biznesowych w oparciu o powyższe treści zalecamy konsultację z radcą prawnym lub adwokatem.

© 2026 Kancelaria Radcy Prawnego Damian Budzis. Wszelkie prawa zastrzeżone. Materiał można udostępniać w oryginalnej formie, bez wprowadzania zmian.