ZAŁĄCZNIK NR 4

POLITYKA DOPUSZCZALNEGO UŻYCIA (AUP)

do Umowy Ramowej o świadczenie usług hostingowych i usług powiązanych (MSA)
z dnia 20.02.2026

Wersja: 1.0
Data obowiązywania: od 20.02.2026
Usługodawca: SEO PARTNER Sp. z o.o. z siedzibą: 81-451 Gdynia, Aleja Zwycięstwa 96/98, IVC, C.518; NIP: 5882415466, REGON: 36356436500000, KRS: 0000598311

§1. Cel i zakres AUP

1. Niniejsza Polityka Dopuszczalnego Użycia („AUP") określa zasady korzystania z Usług świadczonych przez Usługodawcę, w tym hostingu współdzielonego, VPS z administracją, usług domenowych oraz usług pocztowych.
2. AUP ma na celu:
    1. ochronę bezpieczeństwa infrastruktury Usługodawcy i podmiotów trzecich,
    2. zapewnienie zgodności korzystania z Usług z prawem,
    3. ograniczenie nadużyć wpływających na dostępność i jakość usług innych klientów.
3. AUP stanowi integralną część Umowy. Naruszenie AUP stanowi istotne naruszenie Umowy i uprawnia Usługodawcę do zastosowania środków wskazanych w §10 AUP oraz MSA.
4. AUP stosuje się odpowiednio do działań Klienta, jego pracowników, współpracowników, administratorów, użytkowników końcowych oraz wszelkich podmiotów działających z wykorzystaniem zasobów Klienta.

§2. Zasada legalności i odpowiedzialność Klienta

1. Klient zobowiązuje się korzystać z Usług zgodnie z:
    1. powszechnie obowiązującym prawem,
    2. prawami osób trzecich,
    3. dobrymi obyczajami i zasadami współżycia społecznego,
    4. postanowieniami MSA, załączników i Zamówień.
2. Klient ponosi wyłączną odpowiedzialność za:
    1. treści przechowywane, publikowane, transmitowane lub udostępniane w ramach Usług,
    2. sposób wykorzystania Usług,
    3. skutki działań osób, którym udostępnił dostęp do Usług.
3. Klient ma obowiązek wdrożyć środki organizacyjne i techniczne zapobiegające nadużyciom, w szczególności politykę haseł, MFA (gdy dostępne), aktualizacje oprogramowania, monitoring logów i separację uprawnień.

§3. Działania bezwzględnie zakazane

Zakazane jest w szczególności:

1. wykorzystywanie Usług do popełniania przestępstw, wykroczeń lub deliktów cywilnych;
2. rozsyłanie spamu, mail bombingu, wiadomości phishingowych, scamowych, spoofingu lub innej niezamówionej komunikacji masowej;

3. hostowanie, dystrybucja lub uruchamianie złośliwego oprogramowania (malware), ransomware, spyware, botnetów, trojanów, exploitów, cryptojackingu itp.;
4. podejmowanie prób nieautoryzowanego dostępu do systemów, usług lub danych (w tym brute force, credential stuffing, privilege escalation, sniffing, skanowanie portów bez uprawnienia);
5. prowadzenie ataków DDoS/DoS, refleksyjnych, amplifikacyjnych albo świadczenie usług ułatwiających takie ataki;
6. hostowanie treści naruszających prawa własności intelektualnej, dobra osobiste, tajemnicę przedsiębiorstwa, prawo do wizerunku lub prywatności;
7. publikowanie lub udostępnianie treści zabronionych prawem, w tym treści terrorystycznych, nawołujących do przemocy, nienawiści, dyskryminacji, pornografii dziecięcej oraz innych treści bezprawnych;
8. prowadzenie działań, które mogą skutkować wpisaniem adresów IP, domen lub infrastruktury Usługodawcy na listy blokujące (RBL), w szczególności przez nadużycia pocztowe;
9. odsprzedaż, udostępnianie lub dalsze podnajmowanie Usług osobom trzecim bez wyraźnej zgody Usługodawcy;
10. obchodzenie ograniczeń technicznych, limitów bezpieczeństwa lub mechanizmów ochronnych wdrożonych przez Usługodawcę lub dostawcę bazowego.

§4. Zasady korzystania z poczty elektronicznej

1. Klient zobowiązuje się wykorzystywać usługi pocztowe zgodnie z przeznaczeniem i z poszanowaniem zasad uczciwej komunikacji elektronicznej.
2. Klient zapewnia legalną podstawę przetwarzania danych odbiorców i legalność wysyłki każdej komunikacji.
3. Zakazane jest w szczególności:
    1. wysyłanie niezamówionych informacji handlowych,
    2. fałszowanie nagłówków wiadomości,
    3. ukrywanie tożsamości nadawcy,
    4. wysyłka z naruszeniem zasad SPF, DKIM, DMARC lub równoważnych standardów bezpieczeństwa, jeśli są wymagane.
4. Usługodawca może stosować automatyczne i ręczne mechanizmy antyspamowe i antymalware, w tym:
    1. filtrowanie, kwarantannę, odrzucanie lub ograniczanie wiadomości,
    2. czasową lub trwałą blokadę konta pocztowego, domeny lub adresu IP.
5. Usługodawca nie gwarantuje skuteczności 100% filtracji wiadomości niechcianych lub złośliwych.

§5. Zasoby współdzielone i uczciwe użycie

1. W usługach współdzielonych Klient zobowiązuje się korzystać z zasobów (CPU, RAM, I/O, transfer, procesy, zapytania) w sposób niezakłócający pracy innych klientów.
2. Zakazane jest nadmierne lub destrukcyjne obciążanie środowiska, w szczególności przez:
    1. źle zoptymalizowane skrypty i zapytania,
    2. niekontrolowane zadania cykliczne,
    3. nieautoryzowane koparki kryptowalut,
    4. usługi generujące sztuczny ruch.
3. W razie naruszeń Usługodawca może zastosować limitowanie zasobów, wyłączenie procesu/usługi lub czasowe zawieszenie konta bez uprzedzenia.

§6. Bezpieczeństwo techniczne i obowiązki prewencyjne Klienta

1. Klient zobowiązuje się:
    1. utrzymywać aktualne i wspierane wersje systemów, aplikacji i wtyczek,
    2. stosować silne hasła i rotację haseł,
    3. niezwłocznie usuwać wykryte luki i podatności,
    4. zabezpieczać stacje administratorów i kanały dostępu.
2. Klient zobowiązuje się nie przechowywać w Usługach danych wrażliwych kryptograficznie (np. haseł w postaci jawnej, kluczy prywatnych bez zabezpieczeń) bez adekwatnych mechanizmów ochrony.
3. Klient ma obowiązek niezwłocznie zgłosić Usługodawcy każdy incydent bezpieczeństwa mogący wpływać na Usługę lub infrastrukturę Usługodawcy.

§7. Zgłoszenia nadużyć (abuse desk)

1. Zgłoszenia abuse przyjmowane są pod adresem: biuro@seo-partner.pl
2. Zgłoszenie powinno zawierać co najmniej:
    1. identyfikację zasobu (domena, IP, konto, URL),
    2. opis naruszenia,
    3. datę i godzinę zdarzenia,
    4. materiał dowodowy (logi, nagłówki e-mail, zrzuty, linki).
3. Usługodawca samodzielnie ocenia wiarygodność zgłoszenia i zakres niezbędnych działań.
4. Usługodawca może żądać od Klienta wyjaśnień, logów i dokumentów; brak współpracy traktowany jest jako istotne naruszenie Umowy.

§8. Uprawnienia kontrolne Usługodawcy

1. W celu ochrony infrastruktury i realizacji obowiązków prawnych Usługodawca jest uprawniony do:
    1. monitorowania parametrów technicznych i ruchu sieciowego na poziomie metadanych,
    2. automatycznego wykrywania sygnatur nadużyć,
    3. czasowego blokowania ruchu lub dostępu z określonych źródeł,
    4. izolowania środowiska Klienta.
2. Działania, o których mowa w ust. 1, podejmowane są z poszanowaniem tajemnicy komunikacji, przepisów o ochronie danych i zasady proporcjonalności.
3. Usługodawca może przekazać informacje dotyczące nadużyć dostawcom infrastruktury, operatorom bezpieczeństwa oraz właściwym organom, jeżeli jest to niezbędne do przeciwdziałania nadużyciom lub wymagane prawem.

§9. Treści bezprawne i procedura notice-and-action

1. W przypadku uzyskania wiarygodnej informacji o bezprawnym charakterze danych lub działań Klienta, Usługodawca może niezwłocznie:
    1. uniemożliwić dostęp do danych,
    2. zawiesić usługę lub jej część,
    3. zabezpieczyć materiał dowodowy.
2. Usługodawca może poinformować Klienta o podjętych działaniach, chyba że jest to niedopuszczalne z uwagi na przepisy prawa, decyzję organu lub konieczność zabezpieczenia postępowania.

3. Przywrócenie Usługi może nastąpić po usunięciu przyczyny naruszenia i przedstawieniu wiarygodnych wyjaśnień przez Klienta.

§10. Sankcje umowne za naruszenie AUP

1. W przypadku naruszenia AUP Usługodawca może, według własnego uznania i adekwatnie do skali ryzyka:
    1. wystosować ostrzeżenie i wyznaczyć termin usunięcia naruszenia,
    2. zastosować ograniczenia funkcjonalne,
    3. czasowo zawiesić Usługę,
    4. trwale zablokować dostęp do Usługi,
    5. rozwiązać Umowę ze skutkiem natychmiastowym.
2. W przypadkach pilnych (zagrożenie bezpieczeństwa, ryzyko szkody, żądanie organu, naruszenia masowe) Usługodawca może zastosować sankcje natychmiast, bez uprzedzenia.
3. Zastosowanie środków z niniejszego paragrafu nie wyłącza prawa Usługodawcy do dochodzenia odszkodowania i zwrotu kosztów obsługi incydentu.

§11. Koszty incydentów i czynności ponadstandardowych

1. Jeżeli naruszenie AUP wynika z działania lub zaniechania Klienta, Usługodawca może obciążyć Klienta kosztami:
    1. analizy incydentu,
    2. prac naprawczych,
    3. przywrócenia środowiska do stanu zgodnego z Umową,
    4. obsługi zgłoszeń podmiotów trzecich i organów.
2. Rozliczenie następuje według Cennika lub stawek godzinowych określonych w dokumentach umownych.

§12. Relacja do MSA i dokumentów zewnętrznych

1. AUP stosuje się łącznie z MSA, DPA, Załącznikami Usługowymi i Cennikiem.
2. W razie sprzeczności pierwszeństwo mają zasady hierarchii dokumentów określone w §24 MSA.
3. Jeżeli nadużycie dotyczy usługi bazowej podmiotu trzeciego, zastosowanie mają również wiążące polityki tego podmiotu w zakresie niezbędnym do świadczenia Usługi w modelu back-to-back.

§13. Zmiany AUP

1. Usługodawca może zmienić AUP z ważnych przyczyn, w szczególności:
    1. zmian przepisów prawa,
    2. zmian standardów bezpieczeństwa,
    3. zmian wymagań dostawców infrastruktury,
    4. pojawienia się nowych zagrożeń.
2. O zmianie AUP Usługodawca informuje Klienta co najmniej 14 dni przed wejściem zmian w życie, chyba że zmiana musi zostać wdrożona niezwłocznie ze względów bezpieczeństwa lub prawnych.

§14. Postanowienia końcowe

1. AUP wchodzi w życie z dniem wejścia w życie MSA albo z dniem wskazanym w komunikacie Usługodawcy.
2. AUP obowiązuje przez cały okres świadczenia Usług.
3. W zakresie nieuregulowanym zastosowanie mają postanowienia MSA i przepisy prawa powszechnie obowiązującego.