Polityka Dopuszczalnego Użytkowania SellRocket dla Usług Amazon

1. Wprowadzenie

Niniejsza Polityka Dopuszczalnego Użytkowania ("AUP") określa odpowiednie korzystanie z Amazon Selling Partner API (SP-API) i powiązanych usług Amazon przez SellRocket i jego użytkowników. Polityka ta ma na celu zapewnienie zgodności z wytycznymi Amazon, przepisami o ochronie danych (w tym RODO w Europie) oraz najlepszymi praktykami w zakresie bezpieczeństwa danych i prywatności. W związku z przejściem Amazon z Marketplace Web Service (MWS) na nowszy Selling Partner API, zobowiązujemy się do utrzymania najwyższych standardów bezpieczeństwa i ochrony prywatności zgodnie ze zwiększonym naciskiem Amazon na te obszary.

2. Zakres

Niniejsza polityka dotyczy wszystkich użytkowników SellRocket, którzy korzystają z Amazon Selling Partner API w celu zarządzania i rozwijania swojej działalności na platformie Amazon. Obejmuje wszystkie działania związane z integracją SP-API, w tym dostęp do danych zamówień, informacji o realizacji, danych kupujących i innych danych dostępnych za pośrednictwem API. Polityka ta zapewnia, że wszystkie działania wykonywane przy użyciu API są zgodne z warunkami i postanowieniami Amazon, a także z obowiązującymi przepisami prawa, ze szczególnym uwzględnieniem przepisów europejskich, takich jak RODO, gdzie ma to zastosowanie.

3. Dopuszczalne korzystanie z Amazon Services API

3.1 Zgodność z politykami Amazon

SellRocket i jego użytkownicy muszą przestrzegać wszystkich polityk Amazon związanych z korzystaniem z Amazon Selling Partner API, w tym, ale nie wyłącznie:

Umowa dla Programistów Amazon API Services: Użytkownicy muszą przestrzegać warunków określonych w Umowie dla Programistów, w tym wszystkich aktualizacji i poprawek. Użytkownicy powinni regularnie sprawdzać aktualizacje na stronie Amazon "Polityki i Umowy".

Polityka Ochrony Danych (DPP): Użytkownicy muszą przestrzegać DPP Amazon i zapewnić, że wszystkie działania związane z przetwarzaniem danych są prowadzone zgodnie z obowiązującymi przepisami o ochronie danych, w tym zarówno ogólnymi wymogami bezpieczeństwa, jak i dodatkowymi wymogami bezpieczeństwa dotyczącymi przetwarzania Danych Osobowych (PII).

Polityka Dopuszczalnego Użytkowania (AUP): Użytkownicy muszą przestrzegać wytycznych określonych w AUP Amazon, aby zapewnić odpowiednie korzystanie z API, ze zwróceniem uwagi na wersje polityki specyficzne dla danego regionu, gdzie ma to zastosowanie.

3.2 Dozwolone działania

Użytkownicy mogą korzystać z Amazon Selling Partner API wyłącznie do działań dozwolonych przez Amazon, w tym:

Zarządzanie i rozwijanie działalności na platformie Amazon.

Przetwarzanie zamówień i realizacja wymogów wysyłkowych.

Dostęp do danych niezbędnych do zgodności podatkowej i regulacyjnej.

Uczestniczenie w Usługach Amazon w imieniu upoważnionych użytkowników z właściwym uwierzytelnieniem.

Dostęp do danych klientów wyłącznie za wyraźną zgodą i w określonych dozwolonych celach.

Korzystanie z praw wynikających z obowiązujących przepisów, takich jak przenoszenie danych na mocy RODO lub DMA, gdzie ma to zastosowanie.

3.3 Zabronione działania

Użytkownikom zabrania się podejmowania jakichkolwiek działań naruszających polityki Amazon lub obowiązujące przepisy, w tym, ale nie wyłącznie:

Ułatwianie lub promowanie naruszenia jakiejkolwiek umowy między upoważnionymi użytkownikami a Amazon.

Oszukiwanie upoważnionych użytkowników poprzez celową modyfikację informacji.

Obchodzenie polityk lub systemów Amazon w celu uzyskania nieautoryzowanego dostępu do danych.

Wykorzystywanie danych do celów innych niż określone w umowie z upoważnionymi użytkownikami.

Wykorzystywanie danych klientów do celów marketingowych bez wyraźnej zgody.

Przechowywanie PII poza dozwolonym okresem przechowywania wynoszącym 30 dni od dostawy zamówienia.

Udostępnianie danych klientów nieupoważnionym osobom trzecim.

Próby gromadzenia nadmiernych danych, wykraczających poza to, co jest niezbędne do zamierzonego celu (naruszenie zasady minimalizacji danych).

Próby obejścia limitów szybkości i planów użytkowania ustanowionych przez Amazon dla dostępu do API.

4. Ochrona i bezpieczeństwo danych

4.1 Dostęp do danych i bezpieczeństwo

SellRocket i jego użytkownicy muszą wdrożyć odpowiednie środki bezpieczeństwa w celu ochrony danych, do których uzyskano dostęp za pośrednictwem Amazon Selling Partner API. Obejmuje to:

Zapewnienie, że dostęp do danych jest ograniczony wyłącznie do upoważnionego personelu poprzez kontrole dostępu oparte na rolach.

Wdrażanie środków technicznych i organizacyjnych zapobiegających nieautoryzowanemu dostępowi, ujawnieniu lub wykorzystaniu danych.

Szyfrowanie wszystkich PII zarówno w spoczynku, jak i podczas przesyłania, przy użyciu standardowych metod szyfrowania.

Wdrażanie mechanizmów zapobiegania utracie danych (DLP) w celu ochrony PII.

Przestrzeganie Polityki Ochrony Danych Amazon i wszystkich obowiązujących przepisów o ochronie danych.

Stosowanie bezpiecznych metod uwierzytelniania, w tym OAuth 2.0 (Login with Amazon) do dostępu do API.

Regularne oceny bezpieczeństwa i zarządzanie podatnościami dla systemów współpracujących z SP-API.

Wdrażanie odpowiedniego rejestrowania i monitorowania w celu wykrywania incydentów bezpieczeństwa.

4.2 Wykorzystanie danych

Użytkownicy muszą zapewnić, że dane uzyskane za pośrednictwem Amazon Selling Partner API są wykorzystywane wyłącznie do dozwolonych celów, w tym:

Realizacja wymogów wysyłkowych dla zamówień realizowanych przez sprzedawcę.

Spełnianie wymogów prawnych, w tym podatkowych i regulacyjnych.

Przetwarzanie zamówień i zapewnianie obsługi klienta związanej z tymi zamówieniami.

Niewykorzystywanie danych do marketingu, fabrykowania recenzji lub jakichkolwiek celów, które nie zostały wyraźnie autoryzowane.

Przetwarzanie PII wyłącznie w określonych celach autoryzowanych przez Amazon, takich jak działania związane z podatkami i wysyłką.

Przestrzeganie zasady ograniczenia celu zgodnie z RODO dla działalności w Europie.

4.3 Udostępnianie danych

Użytkownicy nie mogą ujawniać ani udostępniać danych nieupoważnionym stronom, chyba że jest to wymagane przez prawo lub w dozwolonych celach. Wszelkie udostępnianie danych musi odbywać się zgodnie z obowiązującymi przepisami o ochronie danych i politykami Amazon. Szczególną uwagę należy zwrócić na PII, które powinny być udostępniane tylko w absolutnie niezbędnych przypadkach i z odpowiednimi zabezpieczeniami.

W przypadku działalności w Europie, użytkownicy muszą zapewnić, że wszyscy zewnętrzni podmioty przetwarzające dane spełniają wymagania RODO i mają odpowiednie umowy o przetwarzaniu danych.

4.4 Przechowywanie i minimalizacja danych

Przechowywanie danych: PII uzyskane za pośrednictwem SP-API muszą zostać usunięte w ciągu 30 dni od dostawy zamówienia, chyba że ich przechowywanie jest wymagane przez obowiązujące przepisy lub do celów podatkowych. Dane niebędące PII powinny być przechowywane tylko tak długo, jak jest to konieczne do celów, dla których zostały zebrane.

Minimalizacja danych: SellRocket i jego użytkownicy będą gromadzić i przetwarzać tylko dane niezbędne do zamierzonego celu, zgodnie z zasadą minimalizacji danych. Dostęp do PII powinien być ograniczony tylko do tego, co jest wymagane do określonych potrzeb operacyjnych.

Dokumentacja: Użytkownicy muszą prowadzić dokumentację swoich polityk przechowywania danych i być w stanie wykazać zgodność na żądanie.

5. Przejście z MWS na SP-API

W związku z przejściem Amazon z Marketplace Web Service (MWS) na nowszy Selling Partner API, SellRocket i jego użytkownicy muszą:

Przestrzegać wytycznych Amazon dotyczących migracji z MWS na SP-API.

Przyjąć wzmocnione środki bezpieczeństwa wymagane przez SP-API, które przewyższają te z MWS.

Zaktualizować metody uwierzytelniania, aby korzystać z OAuth 2.0 (Login with Amazon) zgodnie z wymogami SP-API.

Przejrzeć i zaktualizować praktyki przetwarzania danych, aby spełnić bardziej rygorystyczne wymagania dotyczące ochrony danych SP-API.

Zapewnić, że wszystkie aplikacje korzystające z API są zarejestrowane i autoryzowane zgodnie z wymogami SP-API.

6. Plan reagowania na incydenty

W przypadku naruszenia danych lub incydentu bezpieczeństwa dotyczącego danych uzyskanych za pośrednictwem SP-API, SellRocket i jego użytkownicy muszą:

Natychmiast powstrzymać naruszenie i ocenić jego zakres i wpływ.

Powiadomić Amazon w ciągu 48 godzin od odkrycia naruszenia, zgodnie z wymogami Polityki Ochrony Danych.

Powiadomić osoby, których dane dotyczą, oraz organy regulacyjne zgodnie z obowiązującymi przepisami, w tym wymogami RODO dotyczącymi zgłaszania naruszeń w przypadku działalności w Europie.

Udokumentować incydent, w tym jego przyczyny i kroki podjęte w celu jego naprawienia.

Wdrożyć środki zapobiegające podobnym incydentom w przyszłości.

W pełni współpracować z Amazon i odpowiednimi władzami w każdym dochodzeniu dotyczącym incydentu.

7. Obowiązki użytkownika

Użytkownicy są odpowiedzialni za zapewnienie, że ich korzystanie z Amazon Selling Partner API jest zgodne z niniejszą polityką i wszystkimi obowiązującymi przepisami. Użytkownicy muszą:

Dostarczać dokładne i aktualne informacje podczas rejestracji w celu uzyskania dostępu do API.

Dbać o bezpieczeństwo swoich identyfikatorów konta i poświadczeń.

Wdrażać wszystkie wymagane środki bezpieczeństwa do obsługi PII.

Uzyskać wyraźną zgodę przed dostępem do danych klientów, gdy jest to wymagane.

Usunąć PII w ciągu 30 dni od dostawy zamówienia, chyba że ich przechowywanie jest prawnie wymagane.

Natychmiast powiadomić SellRocket o nieautoryzowanym dostępie lub wykorzystaniu ich konta.

Regularnie przeglądać polityki Amazon pod kątem aktualizacji lub zmian, które mogą wpłynąć na zgodność.

Zapewnić zgodność z wymogami specyficznymi dla danego regionu, szczególnie RODO dla działalności w Europie.

Respektować prawa podmiotów danych określone w obowiązujących przepisach o ochronie danych.

8. Regularne audyty i przeglądy

SellRocket będzie przeprowadzać regularne audyty i przeglądy w celu zapewnienia zgodności z niniejszą polityką i wymogami Amazon:

Kwartalne wewnętrzne audyty działań związanych z przetwarzaniem danych i środków bezpieczeństwa.

Coroczny kompleksowy przegląd wszystkich integracji SP-API i praktyk przetwarzania danych.

Regularne monitorowanie zmian w politykach Amazon i wdrażanie niezbędnych dostosowań.

Prowadzenie szczegółowych dzienników dostępu do API i działań związanych z przetwarzaniem danych do celów audytu.

Przeprowadzanie ocen bezpieczeństwa i testów penetracyjnych systemów, które współpracują z SP-API.

Dokumentowanie wszystkich działań audytowych i wysiłków naprawczych.

9. Prawa użytkowników i żądania

SellRocket respektuje prawa osób, których dane są przetwarzane za pośrednictwem Amazon Selling Partner API. Użytkownicy mogą korzystać ze swoich praw wynikających z obowiązujących przepisów o ochronie danych poprzez:

Składanie wniosków o dostęp do swoich danych osobowych.

Żądanie poprawienia niedokładnych danych osobowych.

Żądanie usunięcia swoich danych osobowych, z zastrzeżeniem wymogów prawnych dotyczących ich przechowywania.

Sprzeciwianie się przetwarzaniu swoich danych osobowych do określonych celów.

Wycofanie zgody na przetwarzanie swoich danych osobowych.

Żądanie informacji o tym, jak ich dane są wykorzystywane i udostępniane.

Żądanie przeniesienia swoich danych do innego dostawcy usług (przenoszenie danych).

SellRocket odpowie na takie żądania w ciągu 30 dni, zgodnie z obowiązującymi przepisami o ochronie danych.

10. Zgodność z wymogami regionalnymi

SellRocket i jego użytkownicy muszą przestrzegać regionalnych wymogów dotyczących ochrony danych podczas przetwarzania danych za pośrednictwem SP-API:

W przypadku użytkowników w Europejskim Obszarze Gospodarczym (EOG) wymagana jest zgodność z Ogólnym Rozporządzeniem o Ochronie Danych (RODO), w tym:

Ustanowienie i udokumentowanie odpowiednich podstaw prawnych przetwarzania danych

Wdrożenie ochrony danych w fazie projektowania i domyślnej ochrony danych

Przeprowadzanie Ocen Wpływu na Ochronę Danych, gdy jest to wymagane

Respektowanie rozszerzonych praw podmiotów danych

W przypadku użytkowników w innych regionach wymagana jest zgodność z obowiązującymi lokalnymi przepisami i regulacjami dotyczącymi ochrony danych.

Szczególną uwagę należy zwrócić na transgraniczne transfery danych, zapewniając odpowiednie zabezpieczenia, takie jak Standardowe Klauzule Umowne dla transferów poza EOG.

W stosownych przypadkach, zgodność z wymogami Aktu o Rynkach Cyfrowych (DMA) związanymi z dostępem do danych i ich przenoszeniem.

11. Informacje kontaktowe

W przypadku pytań, wątpliwości lub zgłoszeń dotyczących niniejszej polityki lub naszych praktyk w zakresie danych, prosimy o kontakt z naszym Inspektorem Ochrony Danych pod adresem