CLOUDFLARE

BIAŁA KSIĘGA

Zasady Cloudflare dotyczące prywatności danych oraz żądań ze strony organów ścigania

Opublikowano 28 stycznia 2021 r.

Wprowadzenie

Sieć i działalność Cloudflare są zbudowane na zaufaniu klientów. Przez cały czas staramy się zdobywać i utrzymywać to zaufanie, tworząc i wdrażając produkty, które pomagają poprawić bezpieczeństwo naszego systemu, szyfrują dane w spoczynku i podczas przesyłania oraz pozwalają naszym klientom ustalić, w jaki sposób jest kontrolowany ruch w różnych lokalizacjach na całym świecie.

Jednak nie wszystkie wyzwania można rozwiązać za pomocą inżynierii. W związku z tym mamy również określone zasady i procedury dotyczące tego, w jaki sposób zarządzamy danymi klientów i użytkowników końcowych w naszych systemach, a także jak postępujemy z żądaniami prawnymi o udostępnienie danych otrzymywanymi od rządów i innych instytucji.

Niniejszy dokument przedstawia te zasady i zawiera linki do bardziej szczegółowych informacji na temat różnych aspektów naszego podejścia do prywatności danych i zgodności z przepisami. W szczególności przedstawiamy tu:

- **Nasz pogląd na zmieniający się krajobraz uwarunkowań dotyczących prywatności danych**
- **Nasze zasady dotyczące prywatności danych i związanych z nimi żądań**

Zmieniający się krajobraz uwarunkowań dotyczących prywatności danych

Eksplozja popularności usług chmurowych oraz fakt, że dane mogą być przechowywane poza krajem zamieszkania osób, które je wygenerowały, stanowi wyzwanie dla rządów prowadzących dochodzenia realizowane przez organy ścigania. Wszelkiego rodzaju dostawcy usług online często stanowią punkt dostępu do tych rejestrów elektronicznych.

Również w przypadku dostawców usług takich jak Cloudflare mogą pojawiać się żądania rządowe dotyczące danych. Działania realizowane przez organy ścigania i inne instytucje rządowe są bardzo ważne. Jednocześnie jednak musimy pamiętać, że dane, których poszukują te podmioty, nie należą do nas. Klienci korzystający z naszych usług obdarzyli nas zaufaniem. Jego utrzymanie ma fundamentalne znaczenie dla naszej działalności i naszych wartości.

Problem potęguje fakt, że różne rządy mają różne standardy ochrony danych osobowych. Na przykład Stany Zjednoczone zabraniają firmom ujawniania treści komunikacji — w tym również rządom spoza Stanów Zjednoczonych — we wszystkich przypadkach, z wyjątkiem niektórych określonych prawnie. Unia Europejska (UE), która od dawna uważa prywatność za podstawowe prawo człowieka, chroni wszystkie dane osobowe w UE w ramach ogólnego rozporządzenia o ochronie danych (RODO). Chociaż te zabezpieczenia pod pewnymi względami się pokrywają, różnią się zarówno pod względem zakresu, jak i osób, którą chronią.

Różnice między ramami prawnymi mają znaczenie, szczególnie w zakresie ustalenia, czy wnioski prawne o informacje kierowane przez obce rządy są zgodne z wymogami dotyczącymi prywatności. Na przykład w ostatnich latach Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wielokrotnie orzekał, że amerykańskie ograniczenia prawne dotyczące gromadzenia danych, wraz z pewnymi dobrowolnymi zobowiązaniami, jak na przykład Privacy Shield (lub poprzednie przepisy, US-EU Safe Harbor) nie są odpowiednie z punktu widzenia zapewnienia zgodności z wymogami UE dotyczącymi prywatności, głównie ze względu na przepisy USA zezwalające władzom na zbieranie informacji na temat obywateli krajów trzecich dla celów wywiadu zagranicznego. Europejska Rada Ochrony Danych (EROD) zajęła stanowisko, że wniosek o udostępnienie danych na mocy prawa karnego USA — poza procesem prawnym, w którym kraje UE utrzymują pewną kontrolę nad udostępnianymi informacjami — nie jest uzasadnioną podstawą przekazywania danych osobowych podlegających RODO.

W istocie rzeczy spór dotyczy tego, czy jeden rząd może korzystać z nakazów prawnych lub innych procedur prawnych w celu uzyskania dostępu do danych na temat obywateli innego kraju. Ta dyskusja toczy się nie tylko w Europie. Chociaż reakcje różnych krajów w zakresie stosowanych zasad nie są spójne, coraz więcej z nich postrzega dostęp do danych swoich obywateli jako problem bezpieczeństwa narodowego.

Zasady Cloudflare dotyczące prywatności danych i związanych z nimi żądań

Firma Cloudflare od dawna utrzymuje zasady mające na celu rozwiązanie problemów dotyczących dostępu do danych osobowych. Robimy to zarówno z przekonania o słuszności takiego podejścia, jak i dlatego, że kolizje przepisów, które dziś obserwujemy, wydawały nam się nieuniknione. Nasze zasady obejmują następujące kwestie:

- Publiczne zobowiązania dotyczące tego, jak traktujemy dane prywatne oraz jak podchodzimy do żądań organów ścigania dotyczących tych danych.
- Sposób informowania naszych klientów o żądaniach dotyczących danych.

Ogólnie rzecz biorąc, w przypadku kolizji między dwoma różnymi standardami prawnymi, domyślnie wybieramy ten, który zapewnia największą ochronę prywatności. Jednocześnie zawsze wymagamy stosowania procedury prawnej. Mamy świadomość tego, że gdy brama dla ujawnienia danych zostanie otwarta, jej zamknięcie może być trudne.

Nasze publiczne zobowiązania dotyczące prywatnych danych i wniosków organów ścigania

Zaczynając od naszego pierwszego raportu dotyczącego przejrzystości, w którym szczegółowo przedstawiliśmy wnioski organów ścigania o udostępnienie danych w 2013 r., przyjęliśmy publiczne zobowiązania odnośnie sposobu, w jaki podchodzimy do wniosków o udostępnienie danych, a także publicznych oświadczeń dotyczących rzeczy, których nigdy nie robiliśmy. Publiczne oświadczenia na temat rzeczy, których nigdy nie robiliśmy, nazywamy „kanarkami”, z założeniem, że pełnią one rolę sygnalizacyjną wobec świata zewnętrznego.

Te „kanarki” spełniają dwie funkcje. Po pierwsze, są one publicznym oświadczeniem, że nie podjęlibyśmy danych działań dobrowolnie. Po drugie, mogą być mechanizmem przekazywania informacji — poprzez usunięcie oświadczeń ze strony — których w przeciwnym razie nie moglibyśmy ujawnić.

Podmioty regulacyjne zaczęły doceniać wartość zobowiązań dotyczących prywatności, szczególnie gdy mogą być one wyegzekwowane umową. Rzeczywiście, zobowiązania, które od lat zawieramy w naszych raportach dotyczących przejrzystości, są dokładnie tym samym rodzajem zobowiązań, które Komisja Europejska zaleciła w swoich projektach standardowych klauzul umownych dotyczących zgodności z RODO.

Kluczowe przykłady naszych zobowiązań w momencie publikacji niniejszego dokumentu:

- **Nigdy nie zainstalowaliśmy oprogramowania ani sprzętu organów ścigania w naszej sieci ani też nie dostarczaliśmy kanału treści przechodzących przez naszą sieć**: jako firma zajmująca się bezpieczeństwem wiemy, że utrzymanie kontroli nad dostępem do naszych sieci jest absolutnie najważniejsze. Dlatego nasz zespół ds. bezpieczeństwa koncentruje się na kontrolach dostępu, rejestrowaniu danych i monitorowaniu, a także przechodzi wiele ocen w ciągu roku przeprowadzanych przez podmioty zewnętrzne. Chcemy mieć pewność, że nasi klienci rozumieją, że od tych kontroli nie ma wyjątku dla organów ścigania czy instytucji rządowych. Dlatego oświadczamy, że firma Cloudflare nigdy nie zainstalowała oprogramowania ani sprzętu organów ścigania w jakimkolwiek miejscu naszej sieci, jak również nigdy nie przekazywaliśmy żadnej organizacji rządowej treści naszych klientów przechodzących przez naszą sieć.
- **Nigdy nie udostępnialiśmy kluczy szyfrowania ani uwierzytelniania**: Cloudflare uważa, że silne szyfrowanie zarówno treści, jak i metadanych, jest niezbędne dla zapewnienia prywatności w Internecie. Jeśli dany kraj uniemożliwia innemu rządowi dostęp do danych osobowych swoich obywateli, pierwszym krokiem powinno być szyfrowanie tych danych osobowych. Klienci i organy regulacyjne muszą jednak mieć również pewność, że samo szyfrowanie jest godne zaufania. Zobowiązujemy się więc, że nigdy nie przekazaliśmy nikomu kluczy szyfrowania ani uwierzytelniania — zarówno naszych, jak i naszych klientów — oraz że nigdy nie osłabiliśmy, nie naruszyliśmy ani nie podważyliśmy naszego szyfrowania na żądanie organów ścigania ani innych stron trzecich.
- **Nigdy nie modyfikowaliśmy treści klientów ani żądań DNS**: nie uważamy, że nasze systemy powinny być wykorzystywane do kierowania ludzi na strony, których nie zamierzali odwiedzać, ani do zmieniania treści przekazywanych online. W związku z tym publicznie ogłosiliśmy, że nigdy nie modyfikowaliśmy treści klientów ani nie zmienialiśmy zamierzonego miejsca docelowego odpowiedzi DNS na żądanie organów ścigania ani innych stron trzecich.
- **Przejrzystość w zakresie potencjalnych przypadków złamania zobowiązań**: zobowiązaliśmy się do kwestionowania, w razie konieczności na drodze sądowej, każdego wniosku prawnego dążącego do zmuszenia nas do naruszenia tych zobowiązań. Chcemy w czytelny sposób pokazać naszym klientom, ale także rządom na całym świecie, gdzie wyznaczamy granice.

Chociaż nasza ogólna filozofia dotycząca ochrony danych pozostaje niezmieniona od czasu naszego powstania, od czasu do czasu dostosowujemy nasze zobowiązania, aby odzwierciedlać najnowsze zmiany w naszych produktach i politykach. Ostateczna, aktualna lista tych zobowiązań jest dostępna na stronie raportu dotyczącego przejrzystości.

Przekazywanie naszym klientom powiadomień o wnioskach rządowych

Cloudflare od dawna uważa, że nasi klienci zasługują na powiadomienie, gdy ktokolwiek — w tym organy ścigania lub inne podmioty rządowe — wykorzystuje proces prawny w celu żądania udostępnienia ich danych. Takie powiadomienie umożliwia naszym klientom zakwestionowanie żądania, jeśli mają wątpliwości.

Od samego początku naszej działalności prowadzimy politykę powiadamiania naszych klientów. W styczniu 2013 r., gdy mieliśmy mniej niż 30 pracowników, FBI pojawiło się w naszych drzwiach z nakazem National Security Letter, żądając informacji na temat klienta i zakazując nam omawiania tych kwestii z kimkolwiek poza naszymi prawnikami. W tamtym czasie nakazy National Security Letter były praktycznie pozbawione nadzoru, mogły być wydawane i egzekwowane przez jedną komórkę rządu Stanów Zjednoczonych, a ich adresatom nieustannie kneblowano usta, uniemożliwiając wypowiadanie się na ich temat.

Zdajemy sobie sprawę, że mogą wystąpić pewne okoliczności, w których czasowe ograniczenie ujawniania informacji nałożone przez organy ścigania może być odpowiednie dla utrzymania skuteczności dochodzenia. Uważamy jednak, że rząd powinien być również zobowiązany do uzasadniania każdego postanowienia o zachowaniu poufności oraz że wszelkie postanowienia tego rodzaju powinny być wyraźnie ograniczone czasowo — do minimalnego okresu niezbędnego dla danego celu. W związku z tym podjęliśmy współpracę z organizacją Electronic Frontier Foundation w celu prawnego podważenia nakazu. Wynikła z tego sprawa sądowa trwała przez kilka lat i nie mogliśmy wypowiadać się na ten temat do 2017 r. Ostatecznie jednak FBI wycofało nakaz.

Ponieważ sądy amerykańskie zasugerowały, że nakazy zachowania poufności informacji na czas nieokreślony stwarzają problemy konstytucyjne, Departament Sprawiedliwości Stanów Zjednoczonych w 2017 r. wydał wytyczne nakazujące prokuraturze federalnej ograniczenie długości nakazów zachowania poufności do maksymalnie jednego roku oprócz sytuacji, gdy zachodzą wyjątkowe okoliczności. Nie powstrzymało to jednak wszystkich amerykańskich organów ścigania przed dążeniem do narzucenia bezterminowego nakazu zachowania poufności. Na dzień publikacji niniejszego artykułu otrzymaliśmy od 2017 r. co najmniej 28 nakazów zachowania poufności, w których nie podano daty końcowej. We współpracy z organizacją American Civil Liberties Union (ACLU) firma Cloudflare zagroziła postępowaniem sądowym za każdym razem, gdy otrzymaliśmy takie bezterminowy nakaz zachowania poufności. W każdym przypadku rząd dodał limity czasowe w odniesieniu do wymogów zachowania poufności zawartych w tych nakazach, umożliwiając nam informowanie naszych klientów o otrzymanych żądaniach.

Postępowanie w przypadku kolizji prawa

Utrzymanie zgodności z przepisami, takimi jak RODO, szczególnie w obliczu nakazów prawnych, które mogą nas stawiać w trudnej sytuacji związanej z koniecznością naruszenia tych przepisów, wymaga zaangażowania sądów. Dostawca usług taki jak Cloudflare może zwrócić się do sądu o umorzenie wniosków prawnych ze względu na kolizję przepisów. Zobowiązaliśmy się zarówno w naszych oświadczeniach publicznych, jak i w załączniku dotyczącym przetwarzania danych (DPA), że podejmiemy ten krok, jeśli będzie to konieczne, aby uniknąć takiego konfliktu. Uważamy, że konflikt powinien zostać zepchnięty z powrotem na jego miejsce — między dwa rządy kłócące się o to, kto powinien być uprawniony do dostępu do informacji.

Wnioski

Ten artykuł to tylko wprowadzenie do naszych szerokich, dogłębnych zobowiązań w zakresie prywatności danych.

Więcej informacji na ich temat można znaleźć w następujących artykułach:

- Nasza ogólna polityka prywatności: opis tego, jakie dane zbieramy i udostępniamy oraz w jaki sposób je wykorzystujemy, a także inne typowe kwestie dotyczące prywatności.
- Nasz raport dotyczący przejrzystości: aktualne informacje na temat otrzymanych przez nas wniosków prawnych dotyczących ujawnienia informacji o naszych klientach.
- Nasza strona główna dotycząca prywatności danych i zgodności z przepisami: najnowsze ogłoszenia dotyczące sposobu, w jaki nasze zasady i produkty zaspokajają potrzeby w obszarze prywatności i zgodności.

Prowadzenie globalnej sieci, która chroni dane klientów i użytkowników końcowych — a także jest zgodna z różnymi przepisami dotyczącymi prywatności na całym świecie — wymaga powrotu do wartości, za którymi opowiadamy się od najwcześniejszych dni naszej działalności: należy postępować zgodnie z zasadami i przejrzystością, szanować prywatność, wymagać należytego procesu i informować klientów, aby mogli podejmować własne decyzje dotyczące swoich danych.

+44 20 3514 6970 | enterprise@cloudflare.com | cloudflare.com/pl-pl

REV:BDES-5987.2024JUL29