Wyniki audytu zgodności procesów przetwarzania danych osobowych na stronach przyklad.pl i przyklad.com

Jakub Orlik, kontakt@kuba-orlik.name

2022-01-02

Wyniki audytu

Niniejszy raport dotyczy stron przyklad.pl oraz przyklad.com. Strony te korzystają z tego samego mechanizmu pozyskiwania zgody, oraz powołują się na tę samą politykę prywatności.

W trakcie audytu autor używał przeglądarki Firefox 95.0 z wyłączoną funkcją ochrony przed śledzeniem, uruchomionej pod systemem GNU/Linux, i analizował ruch sieciowy za pomocą wbudowanych w nią narzędzi.

przyklad.pl

Zakres wysyłanych danych

Strona przyklad.pl przed wyrażeniem zgody przez użytkownika wysyła dane do następujących podmiotów:

- **adocean.pl**

  Zapytania do domeny adocean.pl są opatrywane identyfikatorem internetowym, który nie jest pobierany z Cookie. Identyfikator wykorzystuje metody fingerprintingu i jest w stanie utożsamić użytkownika korzystającego np. z trybu Incognito. Wyłączenie cookies w przeglądarce nie powoduje zaniechania tego fingerprintingu. Zapytania te są też opatrywane ID z cookies. Mając na uwadze, że te identyfikatory śledzą także ruch na innych stronach internetowych, ciężko będzie poprawnie tutaj zastosować inną niż zgoda podstawę prawną.

  Rekomendacja: skrypty adocean.pl powinny ładować się albo dopiero po otrzymaniu zgody użytkownika, albo powinny być sandboxowane. Sandboxing może polegać na wyłączeniu wysyłania fingerprintu przeglądarki w query param `id` oraz ustawianiu cookiesów dostępnych tylko w ramach strony przyklad.pl. W tym drugim wypadku można powoływać się na

uzasadniony interes, bo przetwarzane są tylko dane konieczne do realizacji celu.

Zwracam uwagę, że nawet w sytuacji powoływania się na uzasadniony interes, nie można automatycznie wczytywać skryptów odpowiedzialnych za targetowanie reklam. Zgodnie z treścią Wytycznych 8/2020 EROD dotyczące targetowania użytkowników mediów społecznościowych, par 54:

> EROD przypomina, że w przypadkach, w których administrator zamierza powołać się na prawnie uzasadniony interes, należy starannie rozważyć obowiązki w zakresie przejrzystości i prawo do sprzeciwu. Osoby, których dane dotyczą, **powinny mieć możliwość wyrażenia sprzeciwu wobec przetwarzania ich danych do celów związanych z targetowaniem PRZED rozpoczęciem przetwarzania**.

- **gemius.pl**

  Dane wysyłane do tej domeny są silnie zaobfuskowane. Aby w pełni określić ich wrażliwość, trzeba byłoby wysłać zapytania do Gemiusa o to, jakie informacje niosą ze sobą parametry `id`, `fpdata` oraz `lsdata`.

- **securepubads.g.doubleclick.net, Google**

  Właścicielowi domeny ujawniane są: identyfikator internetowy przechowywany w cookies oraz część historii przeglądania.

Mechanizm pozyskiwania zgody

- **Klarowność przeznaczenia przycisków zawartych w CMP**

  Po kliknięciu przycisku „Ustawienia zaawansowane" pojawia się lista celów przetwarzania danych. W niektórych pozycjach do wyboru są dwa pola do zaznaczenia: „zezwalam" oraz „uzasadniony interes".

  Po pierwsze, wprowadza to w użytkowniku pewnego rodzaju niepewność. W sytuacji, kiedy widzę, że w jednej pozycji jest zaznaczony automatycznie „Uzasadniony Interes", to czy jakbym dodatkowo zaznaczył opcję „zezwalam", to czy coś by się zmieniło?

  Po drugie, w rezolucji Parlamentu Europejskiego z dnia 25 marca 2021 r. w sprawie sprawozdania Komisji z oceny wdrożenia ogólnego rozporządzenia o ochronie danych po dwóch latach jego stosowania (2020/2717(RSP)) (pkt 5) Parlament „wzywa organy odpowiedzialne za nadzór nad ochroną danych do sprecyzowania, że administratorzy danych powinni stosować *tylko jedną podstawę prawną* dla każdego celu przetwarzania"

  Rekomendacja: dodanie opisu suwaków („sprzeciw / brak sprzeciwu"). Wybranie tylko jednej podstawy prawnej do danego celu przetwarzania danych (teraz niektóre cele mają dwie podstawy).

- **Brak przycisku „nie wyrażam zgody”**

  Jednym z warunków koniecznych do tego, aby zgoda była ważną podstawą prawną jest brak negatywnych konsekwencji za niewyrażenie zgody (motyw (42) preambuły rozporządzenia 2016/679).

  W aktualnej formie CMP sprawia, że niewyrażenie zgody na wszystkie cele oparte o zgodę wymaga więcej kliknięć i wysiłku kognitywnego, niż wyrażenie zgody na wszystkie cele przetwarzania. Zachodzą zatem negatywne konsekwencje przy niewyrażeniu zgody. W takiej sytuacji można podważać ważność wszystkich zgód wyrażonych za pomocą aktualnie zaimplementowanego CMP.

- **Niespójność podstaw prawnych**

  Zastanawiające jest, dlaczego jako podstawę prawną do celu „Pomiar wydajności treści” dla PRZYKLAD S.A. używana jest tylko „zgoda”, ale dla partnerów IAB jest już „uzasadniony interes”. Ponownie przez brak wskazania o /czyj/ i o /jaki/ uzasadniony interes dokładnie chodzi, trudno jest na podstawie samej lektury CMP określić, co dokładnie będzie się działo z danymi użytkownika.

Główne rekomendacje

- zastosowanie się do rekomendacji dotyczących konkretnych domen, ujętych w sekcji „Zakres wysyłanych danych”
- dodanie widocznego na pierwszym ekranie CMP, przycisku „nie wyrażam zgody i wyrażam sprzeciw wobec wszystkich niekoniecznych do wyświetlenia strony procesów przetwarzania moich danych osobowych”, w prawym dolnym rogu, stylem i rozmiarem nieodróżniającego się od przycisku „Akceptuję i przechodzę do serwisu”
- Strony z polityką prywatności nie można przeczytać bez odkliknięcia okienka ze zgodami (https://polityka-prywatnosci.przyklad.pl/). Aby użytkownik mógł podjąć w pełni świadomą zgodę, powinien móc być w stanie przeczytać politykę prywatności przed zaakceptowaniem procesów opisanych w wyskakującym okienku. Zaleca się usunięcie skryptów śledzących i CMP z domeny polityka-prywatnosci.przyklad.pl
- Ustawienie nagłówka `Referrer-Policy` w głównej odpowiedzi HTTP strony na wartość `no-referrer`. To spowoduje, że przeglądarka nie będzie wysyłać nagłówka `Referer` ujawniającego podmiotom trzecim część historii przeglądania użytkowników strony.

przyklad.com

Właściwie wszystkie wytyczne dotyczące portalu `przyklad.pl` mają także zastosowanie do portalu `przyklad.com`. Portal `przyklad.com` ujawnia jednak bez zgody użytkownika większą ilość danych, większej liczbie podmiotów.

Dla zwięzłości, niniejsza sekcja zostanie poświęcona tylko tym potencjalnie problematycznymi procesami przetwarzania danych, które nie zachodzą na portalu przyklad.pl.

Szczególne zastrzeżenia budzą zapytania do następujących domen:

- **adservice.google.com**

  Do domeny są wysyłane dane w zakresie identyfikatora internetowego z Cookie i część historii przeglądania.

  Google zajmuje się targetowaniem reklam i subdomena `adservice` służy właśnie do obsługi reklam. Nie mogę wykluczyć, że te dane są wykorzystywane w celu targetowania użytkowników. Zatem na mocy wytycznych 8/2020 EROD, par. 54, możliwość wyrażenia sprzeciwu wobec takiego przetwarzania danych powinna być udostępniona użytkownikowi przed rozpoczęciem takiego przetwarzania. Innymi słowy – te skrypty nie powinny się wczytywać, zanim użytkownik nie podejmie decyzji odnośnie wyrażenia (lub nie) sprzeciwu na takie przetwarzanie.

- **facebook.com**

  Facebookowi ujawniane są dane w zakresie identyfikatora interentowego Użytkownika (z Cookie) i część historii przeglądania (nagłówek Referer, parametr 'href' w queryparams).

  Autor audytu nie widzi tutaj możliwości powoływania się na inną niż zgoda podstawę prawną. Skrypty facebooka powinny ładować się dopiero po wyrażeniu zgody w CMP, nie wcześniej.

- **twitter.com**

  Na podstronie z artykułem są też osadzone skrypty Twittera. Twitterowi zostają ujawnione identyfikator internetowy Użytkownika (z Cookies) oraz część historii przeglądania (query params: $\text{widget}_{\text{origin}}$).

  Podobnie jak w przypadku Facebooka, autor nie widzi możliwości powoływania się w tym wypadku na inną niż zgoda podstawę prawną. Skrypty twittera powinny ładować się dopiero po wyrażeniu zgody w CMP, nie wcześniej.

- **nextclick.pl**

  Właścicielowi domeny `nextclick.pl` są ujawniane: część historii przeglądania Użytkownika (w query params, parametr `url` w zapytaniu o =nextclick.pl/widget/core.js=).

  Tak jak w przypadku Facebooka i Twittera, autor nie widzi możliwości powoływania się w tym wypadku na inną niż zgoda podstawę prawną. Skrypty nextclick.pl powinny ładować się dopiero po wyrażeniu zgody w CMP, nie wcześniej.