Warszawa, 16.07.2020

Czy musimy mieć zgodę na ciasteczka? Wskazówek irlandzkiego organu ciąg dalszy

Kontynuujemy wpis z ubiegłego miesiąca [https://www.isecure.pl/blog/ciasteczko-po-irlandzku-czyli-irlandzki-organ-nadzorczy-o-plikach-cookies/]. Opisałem w nim wnioski z dokonanego przez Irlandzki Organ Ochrony Danych Osobowych (IDPC – Irish Data Protection Commision) audytu stron internetowych 38 administratorów danych. Teraz nadszedł czas na przedstawienie wskazówek, jakie zaprezentował wspomniany organ.

Wstępne rozważania organu o plikach śledzących

Na wstępie IDPC zaznacza, że nie tylko ciasteczkami człowiek żyje. Na urządzenie użytkownika strony internetowej wgrywane są również inne pliki śledzące. Przykładowo można wskazać przycisk „lubię to" popularnego serwisu społecznościowego oraz inne narzędzia udostępniające treści w mediach społecznościowych. Urząd wskazuje, że na technologie typu piksele, śledzenie lokalizacji czy inny sposób zostawiania po sobie śladu w Internecie wymagana jest zgoda użytkownika. Nie jest to jednak wymóg opisany w RODO, a wynikający z dyrektywy ePrivacy, która wpływa na kształt prawa telekomunikacyjnego i to tam należy poszukiwać odpowiednich regulacji w tym zakresie. Dalej IDPC wskazuje, że przepisy dotyczą nie tylko sytuacji, gdy „pliki śledzące" zawierają informacje o danych osobowych, ale również, gdy przechowywana w nich jest jakakolwiek informacja np. identyfikator cookies. Takie identyfikatory są dalej przetwarzane, udostępniane i wykorzystywane do targetowania lub profilowania osób po ich tzw. cyfrowym śladzie. Wówczas, jak zauważył irlandzki organ, wracamy na grunt przepisów RODO, gdzie motyw 30 zawiera stwierdzenie, że osoby fizyczne mogą być powiązane z identyfikatorami on-line dostarczonymi przez aplikacje czy protokoły adresu www, co umożliwia profilowanie i prowadzi do ich identyfikacji.

Jeżeli zgoda – to zgodna z RODO

Polska ustawa Prawo telekomunikacyjne w art. 174 stanowi, że do zgody abonenta zastosowanie mają przepisy o ochronie danych osobowych. Podobnego zdania jest IDPC wskazując, że zgoda w przypadku ciasteczek wymagana jest na podstawie odrębnych przepisów, mianowicie z dyrektywy ePrivacy i Prawa telekomunikacyjnego, jednak warunki jej wyrażenia powinny odpowiadać tym opisanym w RODO. I tak, zgoda udzielona przez użytkownika strony internetowej powinna być dobrowolna, konkretna, świadoma, jednoznaczna, wyrażona poprzez złożenie oświadczenia lub wyraźne działanie potwierdzające.

Nie zawsze zgoda jest potrzebna

Irlandzki organ wskazuje dwa przypadki, w których zgoda nie jest wymagana:

- do komunikacji z podmiotem danych

- do ciasteczek niezbędnych.

Używając ciasteczek identyfikujących rozmówcę, umożliwiających przesyłanie informacji, transmisję pakietu danych, w tym wykorzystując pliki cookies do wykrycia błędów transferu lub utraty danych czy rozdzielenia ruchu sieciowego – nie jest potrzebna zgoda. Podobnie jest z ciasteczkami np. dla obsługi sklepu on-line, aby zakupy nie zniknęły z koszyka. Jednak w sytuacji, gdy strona biura podróży przez 4 lata chce zapamiętać nasze preferencje związane z wycieczką, to takie przetwarzanie powinno być oparte na zgodzie.

Cookies analityczne

IDPC zaznacza, że w przypadku plików analitycznych, czyli wspomagających administratora strony www w zbieraniu danych o np. unikalnych użytkownikach, niezbędne jest uprzednie pozyskanie zgody. Co więcej, w przypadku przetwarzania danych analitycznych przez podmioty trzecie, organ zauważa, że możemy mieć do czynienia ze współadministrowaniem lub powierzeniem przetwarzania, a rolę w konkretnym procesie wyznacza jego cel. Ponadto IDPC stoi na stanowisku, że plików analitycznych nie można uznać za pliki niezbędne do działania strony internetowej, przez co przed ich wykorzystaniem powinna być uzyskana zgoda od użytkowników strony www oraz udzielana im przejrzysta informacja o sposobie przetwarzania danych w polityce prywatności.

Jak uzyskać zgodę na ciasteczka?

Jak zaznacza Irlandzki urząd ochrony danych, większość witryn internetowych posiada wyskakujące okienko informujące o ciasteczkach razem z linkiem do polityki cookies i w tym aspekcie wskazuje, że baner nie powinien w żaden sposób nakłaniać użytkownika do zaakceptowania zgody, a obok przycisku zatwierdzającego powinien być przycisk umożliwiający ich odrzucenie. Godne zauważenia jest także podejście organu do milczenia i braku działania użytkownika. Według IDPC taka bierność nie może stanowić o zgodzie na pliki cookies. Nie można także uzyskać zgody „domyślnej" na ustawienia plików cookies informując o akceptacji ciasteczek poprzez dalsze użytkowanie strony (jej przewijanie). Warto dodatkowo podkreślić, że w polityce cookies można zrealizować obowiązek informacyjny. IDPC wskazuje, że zgodnie z ePrivacy użytkownik powinien otrzymać wyczerpujące informacje na temat korzystania z plików cookies, a poinformowanie w sposób jasny i kompleksowy, zgodnie ze stanowiskiem urzędu, oznacza spełnienie wymogu przejrzystości obowiązku informacyjnego (art. 12-14 RODO), przy czym urząd jest świadomy, że treść polityki cookies w tym aspekcie może powielić się z polityką prywatności strony internetowej.

Co dalej ze zgodą?

Będąc administratorem strony internetowej należy umożliwić swoim użytkownikom wycofanie zgody na wykorzystywanie plików cookies. Proces ten powinien być równie łatwy, jak jej pozyskanie. Nie powinno się także łączyć zgód na przetwarzanie danych do różnych celów. IDPC potwierdza możliwość zastosowania warstwowego informowania o plikach cookies i wyrażania zgody na ich użycie, jednakże trzeba pamiętać, że w drugiej warstwie, po przejściu do wyboru preferencji użytkownika, zgody nie powinny być domyślnie zaznaczone na „tak" bez ingerencji osoby przeglądającej stronę internetową (co wynika z dobrze znanej zasady domyślnej ochrony danych *privacy by default*).

Żadne przepisy nie precyzują, jak długo powinny być przechowywane pliki cookies. Z tym większym zaskoczeniem możemy przeczytać w wytycznych organu zalecenie, aby uzyskiwać potwierdzenie wyrażonej zgody co 6 miesięcy. IDPC wskazuje, że dobrą praktyką byłoby korzystanie z panelu opcji wyboru, który zawsze pozwoli kontrolować wgrywane pliki cookies, niemniej takie podejście dla wielu może wydawać się czymś abstrakcyjnym. Obecnie przyjmuje się, że raz uzyskana zgoda jest ważna do odwołania, a ewentualne jej potwierdzenie wymagane jest w przypadku zmian celów lub sposobów przetwarzania. Irlandzki organ w tym wypadku bardzo wysoko stawia poprzeczkę wymagając nie tylko cyklicznego potwierdzania zgody, ale także dokonywania tego wyjątkowo często, bo aż co 6 miesięcy.

To i jeszcze więcej

Więcej ciekawych spostrzeżeń Irlandzki organ zamieścił w pełnej wersji swoich wytycznych "Ciasteczka i inne technologie śledzące" z kwietnia 2020 roku, które znajdują się pod adresem: https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf.
Warto zapoznać się z całym dokumentem, gdyż oprócz odniesień do RODO i przywołania wyroku w sprawie Planet49 z października 2019 r. można także znaleźć np. omówienie *cookie banneru* z przyciskiem „Ok, rozumiem!", a niestety nie wszystko można zmieścić w krótkim wpisie na blogu.

Przemysław Siarka, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.