FUNDACJA PANOPTYKON

Warszawa, 25 września 2018 r.

Uwagi Fundacji Panoptykon[1] w sprawie noty Prezydencji dotyczącej prac nad projektem rozporządzenia w sprawie prywatności i łączności elektronicznej[2]

W nawiązaniu do noty Prezydencji dotyczącej nowej wersji rozporządzenia ePrivacy, Fundacja Panoptykon przedstawia poniżej swoje uwagi. Jednocześnie podtrzymujemy uwagi przedstawione w piśmie z 13 lipca, które pozwalamy sobie zacytować poniżej.

1. Wyrażanie zgody poprzez ustawienia przeglądarki

Negatywnie oceniamy wykreślenie motywów 22 i 22a, które wprowadzały dobry standard, zgodnie z którym przekazywanie informacji i zbieranie zgód użytkowników powinno być dla nich jak najwygodniejsze. Celem tych motywów była odpowiedź na problem rosnącej liczby okienek służących do zbierania zgód, z którymi spotykają się obecnie użytkownicy. Motywy te zachęcały firmy do stosowania technologii sprzyjających prywatności (tzw. PET, z ang. *privacy-enhancing technologies*), które pozwalałyby użytkownikom kontrolować wyrażone zgody na poziomie przeglądarki. Efektem wykreślenia tych motywów będzie coraz dalej idące „zasypywanie" użytkowników okienkami proszącymi o wyrażenie zgody, co będzie rodziło ich frustrację, a w kolejnym kroku zobojętnienie i przyzwyczajenie. To ostatnie z wysokim prawdopodobieństwem doprowadzi do tego, że użytkownicy przestaną czytać informacje widoczne w okienkach i będą mimowolnie wyrażali zgodę, chcąc szybciej przejść do interesującego ich serwisu.

Umieszczenie pewnego rodzaju „panelu zarządzania" na poziomie przeglądarki pomogłoby użytkownikom sprawniej i efektywniej kontrolować uprawnienia odwiedzanych przez nich stron internetowych i tym samym zwiększyć ich prywatność oraz poczucie kontroli nad tym, kto i co o nich wie, a także w jakich celach te informacje wykorzystuje. Łatwość zbiorczego zablokowania narzędzi śledzących na poziomie przeglądarki zmusiłaby firmy do dołożenia większych starań, by przekonać użytkowników do wyrażenia zgody, np. na stosowanie technik śledzących ich aktywność w sieci. Pozytywnym efektem tych starań byłaby poprawa przejrzystości funkcjonowania wielu portali i stosowanych przez nich praktyk, w tym praktyk marketingowych.

2. *Cookie walls* (art. 8)

Prezydencja zapowiada dalszą dyskusję na temat uzależniania dostępu do serwisu od wyrażenia zgody na instalację plików cookies w dodatkowych celach (a więc nie tych związanych bezpośrednio ze świadczeniem usługi, ale ze śledzeniem i profilowaniem użytkowników w celach reklamowych). Naszym zdaniem takie rozwiązanie przeczy wyrażonemu w ogólnym rozporządzeniu o ochronie danych (RODO) wymogowi pozyskiwania świadomej i w pełni dobrowolnej zgody na przetwarzanie danych osobowych (motyw 42 i 43 RODO). W

[1] Stanowisko przygotowane przez Karolinę Iwańską.
[2] Nota z 20 września, 12336/18.

szczególności, motyw 42 stanowi, że „wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji".

Wprowadzenie możliwości stosowania przez firmy takiego rozwiązania spowoduje wzmocnienie modelu biznesowego, w którym człowiek, który chce mieć dostęp do informacji i uczestniczyć w dyskusji toczącej się w Internecie, musi zapłacić za to informacjami na swój temat. Naszym zdaniem propozycja Prezydencji wypacza sens zgody i stoi w sprzeczności z celem RODO, którym miało być zwiększenie poszanowania dla praw podstawowych jednostek i umożliwienie im realnej kontroli nad informacjami na swój temat.

3. Dalsze przetwarzanie metadanych (art. 6)

Prezydencja proponuje wprowadzenie w art. 6 ust. 2a i ust. 2aa możliwości dalszego przetwarzania metadanych dla innych celów niż te, do których metadane zostały pierwotnie zebrane, pod warunkiem spełnienia „testu kompatybilności".

Naszym zdaniem ta propozycja powoduje ogromne ryzyko dla użytkowników, które nie zostanie złagodzone poprzez zaproponowane środki ostrożności. Jak podkreślaliśmy w poprzednich pismach, same automatycznie zebrane metadane (takie jak lokalizacja czy aktywność internetowa) tworzą profil użytkownika, który może zawierać informacje o charakterze wrażliwym. Pseudonimizacja w tym kontekście niekoniecznie zapobiegnie reidentyfikacji, ponieważ ilość danych oraz ich szczegółowość i tak pozwoli wyróżnić konkretną osobę.

Chcemy zauważyć, że taka sama regulacja znalazła się w art. 6 ust. 4 RODO. Choć jest ona wadliwa i rodzi podobne wątpliwości jak opisane w akapicie wyżej, to nie widzimy sensu powielania tego przepisu w rozporządzeniu ePrivacy. Naszym zdaniem spowoduje to wiele problemów praktycznych i interpretacyjnych związanych z dostosowaniem się różnych podmiotów z jednej strony do wymogów formułowanych przez RODO, a z drugiej – przez rozporządzenie ePrivacy.

Dodatkowo nieprecyzyjne, otwarte na niebezpieczne interpretacje brzmienie tej propozycji może wręcz doprowadzić w praktyce do utworzenia nowej podstawy prawnej przetwarzania metadanych – pewnego rodzaju uzasadnionego interesu. Jak wskazywaliśmy w poprzednich pismach, **metadane mogą zawierać wiele informacji wrażliwych, których przetwarzanie w oparciu o uzasadniony interes jest niezgodne z art. 9 ust. 1 i 2 RODO**.

4. Wykreślenie art. 10 (*privacy by default*)

Stanowczo sprzeciwiamy się propozycji wykreślenia w całości artykułu 10, który dotyczy ustawień prywatności. Wykreślenie tego przepisu byłoby zasadne tylko wtedy, gdyby jednocześnie w projekcie znalazło się odesłanie w tym zakresie do ogólnych przepisów RODO, a dokładniej do art. 25, który reguluje m.in. zasadę domyślnych ustawień prywatności (*privacy by default*). Jednak z uzasadnienia, jakie przedstawia Prezydencja, nie wynika, aby to było jej zamiarem – Prezydencja wyraźnie wskazuje, że motywacją do wykreślenia tego przepisu jest poczucie, że stanowi on zbytnie obciążenie m.in. dla twórców przeglądarek.

Efektem wykreślenia tego artykułu będzie możliwość takiego projektowania narzędzi technologicznych (przeglądarek, aplikacji), których ustawienia domyślnie będą pozwalały na ingerowanie w prywatność użytkowników i śledzenie ich aktywności internetowej. **Prywatność w opcji domyślnej to standard wynikający z RODO (por. art. 25 ust. 2 RODO), który powinien bezwzględnie zostać utrzymany w odniesieniu do producentów urządzeń**

końcowych oraz aplikacji internetowych. Nieuwzględnienie tej zasady w odniesieniu do danych pochodzących z łączności elektronicznej byłoby olbrzymim wyłomem, stawiającym pod znakiem zapytania sens całej reformy przepisów o ochronie danych. Gwarancje ochrony prywatności w wersji domyślnej to najprostszy i najskuteczniejszy sposób na wyeliminowanie złych praktyk i nadużyć związanych z przekazywaniem danych podmiotom trzecim i śledzeniem zachowań użytkowników poza ich kontrolą.

***

Podsumowując, Fundacja Panoptykon postuluje, aby Rząd RP podczas posiedzenia grupy roboczej dążył do wprowadzenia w projekcie zmian zapewniających wysoki standard ochrony prywatności użytkowników i poufności komunikacji, zwłaszcza poprzez poparcie zakazu *cookie walls*, sprzeciw wobec propozycji wprowadzenia art. 6 ust. 2a i 2aa oraz wykreślenia art. 10 i motywów 22 i 22a.