FUNDACJA PANOPTYKON

Warszawa, 15 stycznia 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 tematów, które będą dyskutowane na posiedzeniu grupy roboczej H5 17 stycznia 2018 r., Fundacja Panoptykon podtrzymuje uwagi zawarte w poprzednio przesłanych stanowiskach (w szczególności w piśmie z 21 listopada 2017 r.), a dodatkowo poniżej przekazuje dalsze uwagi dotyczące wybranych zagadnień:

1. Podstawy przetwarzania danych niestanowiących treści przekazu (art. 6 ust. 2 projektu rozporządzenia)

Stanowczo sprzeciwiamy się propozycji rozszerzenia podstaw przetwarzania metadanych o przesłankę uzasadnionego interesu administratora. Uważamy, że przesłanka ta ze względu na swoją niedookreśloność wiąże się z bardzo wysokim ryzykiem nadużyć. Wprowadzenie takiej podstawy przetwarzania spowoduje poważne ograniczenie autonomii informacyjnej użytkowników oraz pogłębi frustrację związaną z poczuciem utraty kontroli nad informacjami na ich temat w Internecie. Tymczasem zadaniem rozporządzenia ePrivacy powinno być wykreowanie jasnych i przejrzystych zasad ochrony poufności, które sprzyjać będą wzmacnianiu modeli biznesowych opartych na budowaniu zaufania pomiędzy biznesem a konsumentami.

Negatywnie oceniamy także propozycję wprowadzenia możliwości dalszego przetwarzania danych bez zgody użytkownika dla celów innych niż te, dla których dane zostały pierwotnie zebrane. Rozwiązanie to jest niezgodne z zasadą ograniczenia celu przetwarzania, na której oparte jest ogólne rozporządzenie o ochronie danych. Efektem tej propozycji będzie wprowadzenie niebezpiecznego wytrychu, który może posłużyć do przetwarzania danych dla celów komercyjnych bez zgody użytkownika, zwłaszcza biorąc pod uwagę obecne realia biznesowe i stosowane natarczywe i nieprzejrzyste metody śledzenia zachowań użytkowników w sieci. Wprowadzenie możliwości dalszego przetwarzania spowoduje znaczące osłabienie pozycji użytkownika, który – udostępniając przedsiębiorcy dane potrzebne do wykonania usługi – nie będzie w stanie przewidzieć, do jakich celów dane te będą następnie wykorzystane.

2. Instalacja plików cookies i inne techniki śledzące (art. 8)

Zdecydowanie sprzeciwiamy się przedstawionej w nocie Prezydencji opcji nr 3[3], zgodnie z którą wymóg uzyskania zgody na instalację plików cookies lub stosowanie innych technik śledzących w sytuacji, gdy ich funkcją jest dostarczanie reklamy targetowanej, należy zastąpić możliwością wyrażenia sprzeciwu przez użytkowników. Oparcie stosowania technik śledzących dla celów reklamowych na przesłance uzasadnionego interesu jest bardzo poważnym ograniczeniem autonomii użytkownika, a ponadto wiąże się z ogromnym ryzykiem nadużyć – obecne praktyki

[1] Stanowisko przygotowane przez Karolinę Iwańską i Katarzynę Szymielewicz.
[2] Nota z 11 stycznia 2018 r., 5165/18.
[3] Por. s. 21 noty.

przedsiębiorców śledzących użytkowników w celach profilowania i targetowania pozostają dalekie od przejrzystości i potrafią w sposób uporczywy śledzić zachowania użytkownika w Internecie również po opuszczeniu przez niego konkretnej witryny. Spowoduje to powrót do rozwiązań przewidzianych w dyrektywie 2002/58/EC sprzed jej nowelizacji w 2009 r., a tym samym wypaczenie sensu reformy ochrony danych osobowych w Unii Europejskiej poprzez utratę przez użytkowników kontroli nad ich danymi i brak możliwości skutecznego sprzeciwienia się natarczywym praktykom.

W odniesieniu do opcji nr 4 **postulujemy wprowadzenie w tekście projektu wyraźnego zakazu tzw. cookie walls**, polegających na uniemożliwieniu użytkownikowi dostępu do usługi w przypadku braku wyrażenia zgody na instalację plików cookies na jego urządzeniu. Przywołany w nocie motyw 25 dyrektywy 2002/58/EC przeczy wyrażonej w ogólnym rozporządzeniu idei świadomej zgody na przetwarzanie danych (motyw 42 i 43 RODO). Wprowadzenie zakazu stosowania *cookie walls* może w dodatku przynieść pozytywne rezultaty i przyczynić się do wzrostu jakości świadczonych w Internecie usług. Użytkownicy, którzy – rzetelnie poinformowani o zasadach działania narzędzi śledzących – dobrowolnie wyrażą zgodę na monitorowanie ich zachowań w celach reklamowych, otrzymają reklamy lepiej dopasowane do swoich potrzeb. Rozwiązanie to będzie korzystne również dla reklamodawców i podmiotów pośredniczących (agencji reklamowych, podmiotów prowadzących serwisy oparte na reklamach), którzy dzięki przejrzystym zasadom odzyskają zaufanie internautów. Opieranie modeli biznesowych przede wszystkim na dochodach z reklam i w konsekwencji walka serwisów o kliknięcia, powoduje dostosowywanie komunikatów do masowego odbiorcy-konsumenta i tym samym dewaluację treści w Internecie. Z tego powodu zakaz stosowania *cookie walls* może również doprowadzić do dynamicznego rozwoju modeli biznesowych finansowanych z opłat uiszczanych przez użytkowników i opartych na dostarczaniu wysokiej jakości treści.

3. Domyślne ustawienia prywatności (art. 10)

Podtrzymujemy podnoszony przez nas w poprzednich pismach postulat wprowadzenia w oprogramowaniu umożliwiającym komunikację elektroniczną **domyślnych ustawień prywatności, które będą uniemożliwiały śledzenie przez podmioty trzecie**. Nieuwzględnienie takiego postanowienia spowoduje nieuzasadniony brak zachowania w odniesieniu do danych pochodzących z łączności elektronicznej standardu domyślnej ochrony prywatności wynikającego z RODO, wyrażonego w art. 25 ust. 2. Wprowadzenie wysokich gwarancji ochrony prywatności już w wersji domyślnej pozwoli użytkownikowi w świadomy sposób wyrazić zgodę na przekazywanie danych innym podmiotom.

Dlatego też negatywnie oceniamy zaproponowaną opcję 0 (ze względu na brak wymogu zapewnienia *privacy by default* w ostatniej propozycji Prezydencji dotyczącej tego przepisu[4]), jak również opcję 1, zgodnie z którą nie tylko nie zostanie wprowadzony wymóg zapewnienia wysokiego poziomu prywatności w wersji domyślnej, ale w dodatku oprogramowanie w ogóle nie będzie wymagało zaakceptowania ustawień prywatności w momencie instalacji. Uważamy, że opcja nr 2 polegająca na umożliwieniu użytkownikowi akceptacji plików cookies lub innych technik śledzących dla konkretnych witryn internetowych na poziomie oprogramowania (np. przeglądarki internetowej) ma sens, pod warunkiem, że ustawienia domyślne oprogramowania będą w jak najwyższym stopniu sprzyjały prywatności.

[4] Nota Prezydencji z 8 września 2017 r., 11995/17.

***

Podsumowując, Fundacja Panoptykon postuluje, aby Rząd RP podczas posiedzenia grupy roboczej H5 17 stycznia 2018 r. dążył do wprowadzenia w projekcie zmian zapewniających wysoki standard ochrony prywatności użytkowników i poufności komunikacji, zwłaszcza poprzez sprzeciw na propozycje rozszerzenia podstaw przetwarzania danych i przesłanek dla stosowania technik śledzących. Postulujemy, aby Rząd RP dążył do wprowadzenia zakazu *cookie walls* i zapewnienia wysokiego poziomu ochrony prywatności w ustawieniach domyślnych oprogramowania.

Stoimy na stanowisku, że silna ochrona praw podstawowych nie stoi na przeszkodzie rozwojowi innowacyjnych modeli biznesowych. Wręcz przeciwnie – dzięki wprowadzeniu regulacji prawnych sprzyjających stosowaniu przejrzystych narzędzi doboru treści i podejmowaniu przez użytkowników świadomych decyzji dotyczących udostępniania dotyczących ich danych, rozporządzenie przyczyni się do wzrostu zaufania użytkowników do biznesu. Efektem tego będzie większa konkurencyjność i innowacyjność europejskich modeli biznesowych, skuteczniejsze komunikaty reklamowe i efektywna ochrona sfery prywatnej użytkowników.