FUNDACJA PANOPTYKON

Warszawa, 21 listopada 2017 r.

Uwagi Fundacji Panoptykon[1] w sprawie propozycji Prezydencji dotyczących projektu rozporządzenia w sprawie prywatności i łączności elektronicznej[2]

Projekt rozporządzenia Parlamentu i Rady w sprawie poszanowania życia prywatnego i ochrony danych osobowych w łączności elektronicznej **(rozporządzenie ePrivacy)** to odpowiedź Komisji Europejskiej na potrzebę lepszej ochrony praw podstawowych, w szczególności poufności komunikacji i prawa do ochrony danych osobowych i życia prywatnego (art. 7 i 8 Karty Praw Podstawowych UE), w obszarze łączności elektronicznej. Rozporządzenie miało przenieść ogólne zasady ochrony prywatności obowiązujące w UE na poziom praktycznych wyzwań, takich jak fakt finansowania usług internetowych przez zyski z komercjalizacji danych osobowych, czy wszechobecność „inteligentnych" sensorów, coraz głębiej ingerujących w naszą prywatność. Co ważne, projekt rozporządzenia ePrivacy reguluje także przepływ danych niemających charakteru osobowego i również w tych sytuacjach gwarantuje poufność komunikacji.

Uwagi ogólne

Zważywszy na ewidentne zagrożenia dla prywatności związane ze sposobem, w jaki działają wiodące firmy z branży interaktywnej i dostawcy treści internetowych, rozporządzenie ePrivacy powinno wprowadzać przejrzyste zasady ochrony danych i poufności komunikacji, sprzyjające rozwojowi modeli biznesowych opartych na zaufaniu i poszanowaniu autonomii informacyjnej użytkowników. Rozporządzenie powinno również uwzględniać perspektywę dalszego rozwoju narzędzi technologicznych umożliwiających głęboką ingerencję w prywatność, takich jak skrypty śledzące czy inteligentne sensory, i uwzględniać związane z tym ryzyka.

Dominujące modele biznesowe są oparte na nieprzejrzystych i niezrozumiałych dla przeciętnego użytkownika Internetu praktykach. Niektóre z nich (np. wymuszanie zgody na przetwarzanie danych) są nielegalne z punktu widzenia już obowiązującego prawa. Zagubienie konsumentów w sieci skryptów śledzących i reklam behawioralnych powoduje, że tracą oni kontrolę nad swoimi danymi. W połączeniu z zalewem źle dobranych reklam oraz wyskakujących okienek, przekłada się to na frustrację i negatywne postawy użytkowników względem serwisów internetowych, agencji marketingowych i samych reklamodawców.

Bardziej świadomi użytkownicy coraz częściej instalują oprogramowanie blokujące reklamy lub wybierają wyszukiwarki i przeglądarki internetowe uniemożliwiające śledzenie. Tym samym aktywnie kontestują model finansowania treści internetowych oparty na komercjalizacji danych. Będąca logiczną konsekwencją tego modelu koncentracja na liczbie odsłon (a nie np. czasie, jaki użytkownik spędza na konkretnej stronie) powoduje dewaluację samych treści oraz niepokojący

[1] Stanowisko przygotowane przez Karolinę Iwańską i Katarzynę Szymielewicz.
[2] Propozycje zmian zawarte w dokumentach z 8 września 2017 r. (11995/17), 6 października 2017 r. (12955/17) i informacje zawarte w nocie z 8 listopada 2017 r. (14062/17).

efekt „równania w dół" w konkurencji między serwisami internetowymi, nawet o charakterze informacyjnym.

W opinii Fundacji Panoptykon rozporządzenie ePrivacy powinno odpowiadać na przywołane powyżej problemy. To szansa na wzmocnienie ochrony autonomii informacyjnej użytkowników i stworzenie reguł gry promujących etyczne modele biznesowe, zbudowane na zaufaniu, otwartej komunikacji z użytkownikami i wysokiej jakości usługach (np. rzetelnych serwisach informacyjnych). Z drugiej strony – obserwując kierunek zmian proponowanych przez Prezydencję i państwa członkowskie – dostrzegamy poważne ryzyko wypaczenia sensu reformy przepisów o ochronie danych osobowych. Zgodnie z notą Prezydencji z 8 listopada br., rozporządzenie ePrivacy ma mieć charakter lex specjalis w stosunku do ogólnego rozporządzenia o ochronie danych **(RODO)**, jednocześnie przewidując istotne wyłomy (o których piszemy w drugiej części stanowiska) w już przyjętych standardach ochrony danych osobowych.

Wejście w życie tak ukształtowanego aktu prawnego w stosunkowo krótkim czasie po rozpoczęciu stosowania RODO może doprowadzić do chaosu, zwiększyć niepewność co do prawa i wygenerować dodatkowe zakłócenia na rynku oraz w funkcjonowaniu organów państwa – choćby nowego Urzędu Ochrony Danych Osobowych, który będzie musiał zweryfikować swoje orzecznictwo i sposób postępowania wobec firm świadczących usługi internetowe i telekomunikacyjne.

Uwagi szczegółowe

Odnosząc się do ostatnich propozycji Prezydencji, w szczególności przepisów z Rozdziału II projektu rozporządzenia (art. 5-10), dostrzegamy, że przewidują one niższy standard ochrony prywatności użytkowników Internetu i poufności komunikacji niż propozycje wypracowane przez Komisję ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) przyjęte przez Parlament Europejski 26 października 2017 r. Nasze dodatkowe zaniepokojenie budzi kierunek zmian zarysowany w nocie Prezydencji z 8 listopada br., a w szczególności: dalsze poszerzanie podstaw przetwarzania danych, dopuszczenie – w szerszym zakresie niż przewidziane w aktualnym tekście projektu – śledzenia urządzeń końcowych na potrzeby marketingowe, likwidacja obowiązku wprowadzenia sprzyjających prywatności domyślnych ustawień oprogramowania umożliwiającego komunikację, obowiązkowa retencja danych.

Poniżej przekazujemy uwagi do propozycji przepisów, które z naszej perspektywy budzą największe zaniepokojenie. Podkreślamy również, że w kontekście zaproponowanych przez Prezydencję poprawek aktualne pozostają uwagi, które Fundacja Panoptykon skierowała do Ministerstwa Cyfryzacji w pismach z 17 stycznia i 4 sierpnia 2017 r.

1. **Podstawy przetwarzania**

W odniesieniu do dopuszczalnych podstaw prawnych przetwarzania danych pochodzących z łączności elektronicznej (obejmujących zarówno treść, jak i metadane) postulujemy nierozszerzanie dopuszczalnych podstaw przetwarzania o uzasadniony interes administratora oraz bezpośrednie odwołanie się do zasad proporcjonalności i minimalizacji danych ujętych w RODO. Ta konkretna podstawa prawna ma sens w bezpośredniej relacji między podmiotem i administratorem danych, szczególnie kiedy te podmioty łączy stała relacja umowna, umożliwiająca dwustronną komunikację (w tym bezproblemowe wyrażenie sprzeciwu przez podmiot danych).

Rozporządzenie ePrivacy dotyczy sytuacji, w których – ze względu na złożoność ekosystemu łączności elektronicznej – często mamy do czynienia z tzw. podmiotami trzecimi i rozbudowanym łańcuchem pośredników w komunikacji. Konstrukcja uzasadnionego interesu administratora zastosowana do takich sytuacji otworzyłaby bardzo szeroko możliwość przetwarzania danych poza kontrolą osób, których te dane dotyczą.

Ponadto, stoimy na stanowisku, że podstawy prawne przetwarzania metadanych oraz treści komunikacji powinny być do siebie jak najbardziej zbliżone, z uwagi na pojawiające się często wątpliwości, jak zakwalifikować daną informację.

Jednocześnie dostrzegamy i rozumiemy problemy zgłaszane przez biznes, wynikające z zawężenia przesłanek przetwarzania danych – w tym danych o charakterze nieosobowym – w kontekście świadczenia i rozliczania istotnych dla użytkowników usług (również o charakterze dodatkowym). O ile zatem sprzeciwiamy się poszerzaniu tych przesłanek w celach marketingowych czy prowadzenia szeroko pojętej analizy danych, o tyle zgadzamy się z potrzebą doprecyzowania lub poszerzenia przesłanek przetwarzania danych w celach takich jak możliwość świadczenia dodatkowych usług, monitorowanie ruchu na stronie czy rozliczenie realizowanych usług (także w relacji z podmiotami trzecimi – np. w kontekście remarketingu, o ile nie ingeruje to w prywatność użytkowników).

2. Domyślne ustawienia prywatności

Brzmienie art. 10 projektu rozporządzenia ePrivacy zaproponowane przez Prezydencję nie uwzględnia podnoszonej przez nas w poprzednich pismach potrzeby zagwarantowania tego, że ustawienia prywatności w oprogramowaniu umożliwiającym komunikację w opcji domyślnej będą uniemożliwiały śledzenie przez podmioty trzecie. Jest 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.

3. Cookie-walls

W wersji projektu zaproponowanej przez Prezydencję nie znalazł się wyraźny zakaz ograniczania użytkownikom dostępu do usług w sytuacji niewyrażenia zgody na śledzenie w celach marketingowych, w tym instalację plików cookies (tzw. *cookie-walls*). Korzystanie z *cookie-walls* jest nie do pogodzenia z przewidzianym w RODO wymogiem pozyskiwania świadomej i w pełni dobrowolnej zgody na przetwarzanie danych osobowych (motyw 42 i 43 RODO). Nie mniej jednak doprecyzowanie tej kwestii w rozporządzeniu ePrivacy mogłoby wyeliminować wątpliwości interpretacyjne i uciąć dyskusje powracające w debacie publicznej.

Ze względu na powszechność stosowania *cookie-walls* i dalekosiężne konsekwencje wymuszania zgody na przetwarzanie danych (pliki cookies i inne narzędzia wykorzystywane przez podmioty z branży reklamowej mogą w sposób uporczywy śledzić zachowania użytkownika również po opuszczeniu przez niego konkretnej witryny oraz umożliwiać przekazywanie danych podmiotom trzecim i ich integrowanie), ten wątek ma duże znaczenie dla ochrony autonomii informacyjnej użytkowników.

Wprowadzenie wyraźnego zakazu stosowania *cookie-walls* może przyczynić się do wzrostu jakości świadczonych w Internecie usług, a nawet przynieść korzyści firmom świadczącym usługi marketingowe. 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. Zakaz stosowania *cookie-walls* może również ułatwić rozwój serwisów i usług finansowanych z opłat uiszczanych przez użytkowników i opartych na dostarczaniu wysokiej jakości treści.

***

Podsumowując, Fundacja Panoptykon postuluje, aby Rząd RP podczas posiedzeń Rady i jej grup roboczych dążył do wprowadzenia w projekcie rozporządzenia ePrivacy zmian zapewniających wysoki standard ochrony prywatności użytkowników i poufności komunikacji. Jednocześnie nie sprzeciwiamy się racjonalnym i nie podważającym zasad wynikających z RODO zmianom postulowanym przez środowiska biznesowe. Stoimy na stanowisku, że silna ochrona praw podstawowych nie stoi na przeszkodzie rozwojowi innowacyjnych modeli biznesowych. Wręcz przeciwnie – dzięki wprowadzeniu rozwiązań promujących przejrzystość, otwartą komunikację w relacji firm z użytkownikami i podejmowanie przez nich świadomych decyzji w zarządzaniu swoimi danymi, rozporządzenie przyczyni się do wzrostu zaufania użytkowników do biznesu. W dłuższym horyzoncie czasowym to podejście może skutkować większą konkurencyjnością i innowacyjnością europejskich modeli biznesowych i skuteczniejszymi komunikatami reklamowymi, w połączeniu z efektywną ochroną sfery prywatnej użytkowników.