FUNDACJA PANOPTYKON

Warszawa, 9 lipca 2020 r.

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

W nawiązaniu do noty Prezydencji (*discussion paper*) dot. art. 6-6d i art. 8 projektu rozporządzenia ePrivacy, przedstawiamy następujące uwagi:

1. **Sprzeciw wobec możliwości śledzenia w oparciu o uzasadniony interes**

- **W zakresie pytania (a)(ii) dotyczącego art. 6b** postulujemy, aby polski rząd opowiedział się **za opcją nr 2**.

W naszej opinii wprowadzenie możliwości przetwarzania metadanych w celu „*statistical counting*", zgodnie z propozycją przedstawioną w opcji nr 2, **odpowiada na uzasadnione potrzeby podmiotów objętych regulacją**. Pojęcie „uzasadnionego interesu" jest bardzo podatne na interpretacje (na co dowodów dostarcza praktyka stosowania RODO). Wprowadzenie takiej podstawy przetwarzania metadanych, nawet jeśli jej wykorzystanie jest obwarowane dodatkowymi gwarancjami, **może stworzyć niebezpieczny wyłom** w ochronie poufności komunikacji użytkowników końcowych.

W wersji proponowanej w opcji nr 1 powołanie się na uzasadniony interes byłoby wykluczone, gdyby informacje zgromadzone w ten sposób służyły do budowania profilu użytkownika lub gdyby informacje te zawierały tzw. dane wrażliwe. **W praktyce ocena, czy któraś z tych sytuacji ma miejsce, jest niezwykle trudna.** W kontekście pierwszej przesłanki dotychczasowe doświadczenia z dwóch lat obowiązywania przepisów RODO wskazują, że użytkownikom niezwykle trudno jest uzyskać dostęp do ich profilu behawioralnego i zweryfikować, jakie dane zostały wykorzystane do zbudowania tego profilu[3]. Fundacja Panoptykon podjęła w tej sprawie wiele interwencji, które pokazały, że firmy z branży reklamy internetowej tworzą szereg barier uniemożliwiających użytkownikom dostęp do własnych danych (przed Prezesem Urzędu Ochrony Danych Osobowych toczą się dwa postępowania w tej sprawie[4]). Z kolei na obiektywne trudności związane z ustalaniem, kiedy informacje pochodzące z metadanych mogą być uznane

[1] Stanowisko przygotowane przez Karolinę Iwańską.

[2] Nota z dnia 6 lipca 2020 r. nr 9243/20.

[3] Fundacja Panoptykon, *Dwa lata RODO: „testy zderzeniowe" na dwie gwiazdki*, 25 maja 2020, https://panoptykon.org/audyt-rodo

[4] Fundacja Panoptykon, skargi na polskie portale ws. dostępu do profili marketingowych, https://panoptykon.org/biblio/skargi-na-polskie-portale-w-sprawie-dostepu-do-profili-marketingowych

za dane wrażliwe, wskazuje chociażby brytyjski urząd ochrony danych – Information Commissioner's Office – w raporcie poświęconym branży reklamy internetowej[5].

Podsumowując, wprowadzone gwarancje – choć słuszne – **są w praktyce niezwykle trudne, jeśli nie niemożliwe, do zrealizowania.** Jest to problematyczne zarówno z perspektywy firm, dla których stanowi to wyzwanie techniczne i organizacyjne, ale również użytkowników, którzy w praktyce nie mają możliwości ustalenia, jak informacje z metadanych są wykorzystywane, przez co nie mogą skutecznie zidentyfikować nadużyć i dochodzić swoich praw.

- **W zakresie pytania (a)(iii) dotyczącego art. 8** również postulujemy, aby polski rząd sprzeciwił się możliwości wprowadzenia uzasadnionego interesu jako podstawy uzyskiwania dostępu do informacji z urządzeń końcowych użytkowników, wybierając **opcję nr 2 z zastrzeżeniami**, o których piszemy w kolejnych punktach.

2. Sprzeciw wobec motywu 21 (śledzenie jako niezbędne do świadczenia usługi finansowanej z reklam)

Odnosząc się do pytania nr 1, które Prezydencja kieruje do opcji nr 2 w kontekście art. 8, chcielibyśmy ponownie przytoczyć uwagi przesłane Ministerstwu w piśmie z 5 lutego 2019 r.[6] **Stanowczo sprzeciwiamy się brzmieniu motywu 21** z kompromisu przedstawionego przez Prezydencję fińską w dokumencie 14068/19:

> *In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar devices and has accepted such use.*

- **Drastyczne obniżenie standardu wynikającego z RODO**

U podstaw tej zmiany leży założenie, że śledzenie aktywności użytkowników w Internecie w celach reklamowych jest nieodłącznym elementem usług, których źródłem finansowania są reklamy. **Takie podejście otwiera furtkę do permanentnego śledzenia aktywności użytkowników bez ich zgody, co drastycznie obniża standardy wynikające z RODO.** Tymczasem taki czy inny model biznesowy wybrany przez podmiot świadczący usługę nie może uzasadniać ingerencji w prawa podstawowe użytkowników.

Wysoki stopień ingerencji w prywatność technik stosowanych przy dopasowywaniu reklamy behawioralnej wielokrotnie podkreślała Grupa Robocza Art. 29, m.in. w Opinii 2/2010 w sprawie internetowej reklamy behawioralnej (WP 171). W tej opinii Grupa stanowczo opowiedziała się za wyraźną zgodą, jako podstawą prawną takiego przetwarzania danych. Z kolei w wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania (WP 251), Grupa Robocza wskazała, że w kontekście reklamy targetowanej może

---

[5] ICO, *Update report into adtech and real-time bidding,* 20 czerwca 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

[6] https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_epri-vacy_5.02.2019.pdf

również dochodzić do podejmowania zautomatyzowanych decyzji, o których mowa w art. 22 RODO.

Sformułowanie „has accepted such use" jest niejednoznaczne w kontekście przepisów RODO, ponieważ nie odwołuje się do terminu „consent", standardowo używanego na określenie zgody. W konsekwencji może to doprowadzić do zamieszczania postanowień dotyczących stosowania ciasteczek i podobnych technologii w celach śledzenia i profilowania użytkowników w regulaminach usług, których treści użytkownicy – ze względu na istotną nierównowagę sił – **nie mają możliwości negocjować z dostawcami usług**.

Konsekwencją zaproponowanego rozwiązania będzie w praktyce zmuszenie użytkowników do przekazywania ich danych do celów reklamowych, **wbrew ich intencjom i oczekiwaniom** i poza jakąkolwiek kontrolą. Przykładowo, osoba korzystająca z aplikacji fitness oczekuje, że usługa, którą ta aplikacja świadczy, polega na monitorowaniu czasu i trasy treningów, i to w tym celu użytkownik pozwala aplikacji śledzić m.in. swój stan zdrowia czy lokalizację. **Nie sposób jednak uznać, że nieodłączną częścią tej usługi jest wykorzystywanie tego typu informacji w celach reklamowych**, zwłaszcza, jeśli weźmiemy pod uwagę, że nawet historia przeglądanych stron czy historia lokalizacji mogą ujawniać dane wrażliwe, np. informacje o zdrowiu, wyznaniu, poglądach politycznych czy seksualności.

Ekosystem reklamy targetowanej jest **wyjątkowo skomplikowany technicznie i nietransparentny**. Nawet profilując użytkowników w oparciu o zgodę (tak jak ma to obecnie miejsce na większości portali), firmy nie przekazują użytkownikom wystarczających informacji na temat funkcjonowania tych mechanizmów, a **użytkownicy nie mają możliwości ich kwestionować**, o czym piszemy w pkt. 1 powyżej. Wprowadzenie wytrychu polegającego na możliwości śledzenia użytkowników bez ich zgody, w ramach oferowanej usługi, nie przyczyni się do podwyższenia świadomości użytkowników, wręcz przeciwnie – **wzmocni ich poczucie braku kontroli nad informacjami na swój temat w Internecie**. W reakcji na masowe naruszanie przepisów RODO w ramach ekosystemu reklamy behawioralnej, Fundacja Panoptykon złożyła 28 stycznia 2019 r. do Prezesa Urzędu Ochrony Danych Osobowych skargi na Google i Interactive Advertising Bureau – podmioty, które są faktycznymi regulatorami tego rynku[7]. Analogiczne skargi zostały złożone w 15 europejskich krajach[8]. W tym samym dniu opublikowaliśmy raport „Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem"[9], w którym opisujemy techniczny przebieg procesu doboru reklamy behawioralnej (tzw. mechanizm *real-time bidding*) oraz związane z nim negatywne konsekwencje dla prywatności użytkowników.

- **Niewłaściwa odpowiedź na złą sytuację finansową wydawców internetowych**

Wprowadzenie możliwości śledzenia użytkowników w celach reklamowych jako niezbędnego do świadczenia usługi jest motywowane troską o dochody internetowych wydawców. Nie negując istoty tego problemu, uważamy, że jego **źródło leży gdzie indziej**, a poświęcenie chronionego Kartą Praw Podstawowych prawa do prywatności jest skrajnie **nieproporcjonalnym środkiem**, które nie tylko tego problemu nie rozwiąże, co wręcz go pogłębi.

---

[7] https://panoptykon.org/biblio/skargi-fundacji-panoptykon-na-iab-i-google

[8] Fundacja Panoptykon, Skargi na Google'a i IAB trafiły już do 15 krajów, 4 czerwca 2019, https://panoptykon.org/wiadomosc/skargi-na-googlea-i-iab-trafily-juz-do-15-krajow

[9] https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf

System reklamy internetowej opartej o dane behawioralne o użytkownikach Internetu jest **skrajnie niekorzystny dla wydawców internetowych**[10]. W praktyce są oni zmuszeni konkurować o klientów – reklamodawców – z dominującymi platformami internetowymi takimi jak Facebook i Google, które dysponują o wiele bardziej szczegółowymi i rozbudowanymi profilami użytkowników. Ponieważ utrzymanie infrastruktury technicznej do śledzenia i profilowania użytkowników jest kosztowne, a ilość danych pozostawianych na stronie samego wydawcy (tzw. *first-party data*) niewielka, wydawcy korzystają z usług różnego rodzaju pośredników reklamowych, których zadaniem jest łączenie informacji o użytkownikach z różnych stron i różnych urządzeń (tzw. cross-site i cross-device tracking). Zgodnie z danymi opublikowanymi przez brytyjską gazetę The Guardian, opłaty pobierane przez tych pośredników wynoszą aż 70% całej kwoty, jaką za reklamę zapłacił reklamodawca[11]. To oznacza, że **na 1 złotówkę wydaną na reklamę, do wydawcy trafi zaledwie 30 gr**. Nawet dane samej branży reklamy internetowej, która jest bardziej ostrożna w swoich szacunkach, pokazują, że tzw. podatek adtechowy wynosi minimum 55% kwoty wydanej na reklamę[12].

Co więcej, pod koniec 2019 r. opublikowane zostały wyniki pierwszego tego typu badania naukowego, które pokazało, że **wydawcy zarabiają jedynie 4% więcej na reklamie behawioralnej** (czyli wykorzystującej informacje o odwiedzających) niż na reklamie kontekstowej (czyli dostosowanej do kontekstu strony)[13]. W praktyce **wydawcy mogą nawet na reklamie behawioralnej tracić**, ponieważ – jak przyznają naukowcy – badanie nie uwzględnia to kosztów infrastruktury technicznej, którą muszą zapewnić wydawcy po swojej stronie, jak i kosztów obsługi prawnej i dostosowania się do wymogów RODO.

Ciekawy jest również przykład holenderskiego wydawcy Ster, który **po przejściu w pełni na reklamę kontekstową zanotował nie tylko brak spadku, ale wzrost przychodów z reklamy**[14], i to również w okresie pandemii, który był wyjątkowo ciężki dla branży reklamy internetowej[15]. Na wyższe zarobki wydawców, którzy stawiają na reklamę kontekstową wskazują również dane opublikowane przez firmę Kobler — norweskiego pośrednika reklamy kontekstowej[16].

Podsumowując, wytrych wprowadzony w motywie 21 może doprowadzić do tego, że po pierwsze: wydawcy chcący konkurować o pieniądze reklamodawców z Facebookiem i Googlem będą w dalszym ciągu **zależni od warunków dyktowanych przez pośredników reklamy internetowej i same platformy** (jedna z podstawowych usług Google'a – Google Authorized

---

[10] Zob. Fundacja Panoptykon, *10 grzechów reklamy internetowej*, 28 stycznia 2020, https://panoptykon.org/10-grzechow-reklamy-internetowej

[11] https://mediatel.co.uk/news/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory/

[12] https://www.adweek.com/digital/3-benefits-resulting-from-ad-tech-tax-cuts/

[13] https://techcrunch.com/2019/05/31/targeted-ads-offer-little-extra-value-for-online-publishers-study-suggests/

[14] Ster, *A Future without advertising cookies*, https://www.ster.nl/media/h5ehvtx3/ster_a-future-without-advertising-cookies.pdf

[15] Brave, *New data shows publisher revenue impact of cutting 3rd party trackers*, https://brave.com/npo/

[16] Kobler, *Study of Effects of Contextual Targeting on News*, https://kobler.no/contextual-insights/

Buyers — polega właśnie na pośredniczeniu pomiędzy wydawcami a reklamodawcami). Po drugie: **alternatywne modele biznesowe, np. oparte na reklamie kontekstowej, często dostarczane przez europejskie MŚP, nie będą miały możliwości się rozwinąć** i przekonać wydawców, że nie tylko nie stracą finansowo, wybierając reklamę kontekstową, ale wręcz znacznie polepszą swoją sytuację. Po trzecie: **wydawcy mogą stracić jeszcze więcej czytelników** w sytuacji, gdy czytelnicy poczują, że wydawcy nie szanują ich prywatności i wykorzystują informacje o nich bez ich zgody.

> ***ePrivacy, w połączeniu z procedowanym w Komisji Europejskiej pakietem Digital Services Act, który ma na celu zmniejszyć dominację platform internetowych, może stanowić systemową odpowiedź na problem kiepskiej sytuacji finansowej wydawców internetowych oraz wzmocnić zaufanie pomiędzy nimi a ich czytelnikami.***

3. Narzędzia kontrolne dla użytkowników

Jednocześnie, dostrzegamy wiele problemów związanych z koniecznością ciągłego pytania użytkowników o zgodę na wykorzystywanie informacji na ich temat.

Badacze Internetu i organy nadzorcze podnoszą niezwykle istotny problem zmęczenia zgodą („consent fatigue")[17], który sprawia, że użytkownikiem klikającym „zgadzam się" kieruje nie tyle chęć wyrażenia świadomej i poinformowanej zgody na śledzenie, co raczej chęć pozbycia się baneru informacyjnego, który blokuje dostęp do zawartości strony.

W poprzednich wersjach ePrivacy widoczna była intencja polepszenia internetowego doświadczenia użytkowników poprzez wprowadzenie zasady poufności i prywatności by design i by default oraz możliwości kontrolowania ustawień prywatności poprzez przeglądarki lub inne zewnętrzne narzędzia. Postulujemy, aby polski rząd podniósł konieczność przywrócenia i rozwinięcia tych przepisów.

- **Przywrócenie zasady poufności i prywatności by design i by default (art. 10 w wersji z lipca 2018 r.)**

Efektem wykreślenia art. 10 w wersji przedstawionej w lipcu 2018 r. (por. uwagi Fundacji z dn. 13 lipca 2018 r.[18]) będzie możliwość takiego projektowania narzędzi technologicznych (przeglądarek, aplikacji), których ustawienia domyślnie będą pozwalały na ingerowanie w prywatność użytkowników i poufność ich komunikacji. 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**

---

[17] C. Utz i inni, *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, https://arxiv.org/pdf/1909.02638.pdf;

B. Schermer i inni, *The crisis of consent: How stronger legal protection may lead to weaker consent in data protection*, https://www.researchgate.net/publication/271922021_The_crisis_of_consent_How_stronger_legal_protection_may_lead_to_weaker_consent_in_data_protection,

[18] https://panoptykon.org/sites/default/files/stanowiska/panoptykon_mc_stanowisko_eprivacy_13.07.2018.pdf

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 oraz zapewnienie najwyższej ochrony również tym użytkownikom, którzy nie mają wiedzy technicznej pozwalającej na zrozumienie konsekwencji zaproponowanych ustawień.

- **Wprowadzenie możliwości kontrolowania ustawień prywatności przez przeglądarkę lub inne zewnętrzne narzędzie:**

Postulujemy przywrócenie wykreślonych we wrześniu 2018 r. 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.

Co ważne, ten „panel zarządzania" **nie musi być zerojedynkowy** (tzn. wysyłać tylko sygnał „śledź" lub „nie śledź" w stosunku do wszystkich), ale może określać w sposób bardziej granularny, jakie dane mogą być wykorzystywane, a jakie nie oraz tworzyć listy stron, którym użytkownik ufa i którym chce pozwolić wykorzystywać informacje na swój temat.

***

Podsumowując, Fundacja Panoptykon postuluje, by Rząd RP opowiedział się przeciwko wprowadzeniu możliwości powoływania się na uzasadniony interes przy przetwarzaniu metadanych (art. 6) lub danych z urządzeń końcowych użytkowników (art. 8), sprzeciwił się możliwości dostępu do danych z urządzeń końcowych w celach niezbędnych do świadczenia usług finansowanych w drodze reklamy (motyw 21) i zgłosił postulat przywrócenia narzędzi kontrolnych dla użytkowników końcowych, jakie zostały zaproponowane w poprzednich wersjach rozporządzenia.