Warszawa, dnia 30 sierpnia 2019 r.

Pani
Agnieszka Krauzowicz
Dyrektor
Departamentu Telekomunikacji
Ministerstwo Cyfryzacji

STANOWISKO

ZWIĄZKU PRACODAWCÓW BRANŻY INTERNETOWEJ INTERACTIVE ADVERTISING BUREAU (IAB POLSKA) W/S WNIOSKU ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY W SPRAWIE POSZANOWANIA ŻYCIA PRYWATNEGO ORAZ OCHRONY DANYCH OSOBOWYCH W ŁĄCZNOŚCI ELEKTRONICZNEJ I UCHYLAJĄCE DYREKTYWĘ 2002/58/WE (ROZPORZĄDZENIE W SPRAWIE PRYWATNOŚCI I ŁĄCZNOŚCI ELEKTRONICZNEJ) – W WERSJI Z ZDNIA 26 LIPCA 2019 R.

Szanowna Pani Dyrektor,

W odpowiedzi na zaproszenie Ministerstwa Cyfryzacji do składania stanowisk i opinii odnoszących się do Wniosku Rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej, dalej „**EPR**" oraz „**Rozporządzenie e-Privacy**") Związek Pracodawców Branży Internetowej IAB Polska (dalej: „IAB Polska") pragnie przedstawić swoje stanowisko.

IAB Polska jest organizacją zrzeszającą ponad 200 członków, wśród których znajdują się m.in. największe portale internetowe, sieci reklamowe, domy mediowe i agencje interaktywne. Naszym celem jest zaakcentowanie potrzeby zapewnienia wyważonych przepisów, które będą sprzyjały rozwojowi innowacyjnej gospodarki.

1. Uwagi ogólne

W dniu 26 lipca 2019 r. Rada UE opublikowała kolejną wersję Rozporządzenia e-Privacy z pewnymi zmianami dotyczącymi treści komunikacji elektronicznej, danych i metadanych oraz dalszego przetwarzania metadanych. W naszej ocenie, najnowsza wersja projektu EPR, mimo wprowadzonych zmian, w sposób niedostateczny ulepszyła wyjściowy projekt Komisji

Europejskiej. Projekt nadal nie stanowi podstawy do kompromisu. Dlatego też pragniemy w dalszym ciągu podtrzymać, zgłaszane wcześniej uwagi do projektu rozporządzenia, w tym następujące postulaty.

Projektowane przepisy są szkodliwe dla innowacyjności gospodarki europejskiej, przyczynią się do obniżenia poziomu konkurencyjności firm w Polsce i Europie oraz mogą prowadzić do ograniczenia dostępu do wielu usług i treści. Uważamy, że przyjęcie Projektu w obecnym brzmieniu będzie miało bardzo negatywny wpływ na konkurencyjność i innowacyjność polskich przedsiębiorców. Wpłynie ono niekorzystnie na większość firm sektora cyfrowego: operatorów telekomunikacyjnych, dostawców usług internetowych i treści w Internecie. Uderzy ponadto w branżę reklamy internetowej oraz przedsiębiorców, którzy dzięki niej skutecznie docierają do potencjalnych klientów (zwłaszcza firmy lokalne i MŚP). Wdrożenie tego rozporządzenia będzie miało znaczący wpływ na usługi cyfrowe, dostęp do informacji, i rozrywki przez użytkowników.

Rozporządzenie e-Privacy będzie miało również negatywne konsekwencje dla sektora usług świadczonych drogą elektroniczną (treści, usługi i handel online), gdyż wbrew oczekiwaniom utrzymuje zakazy i ograniczenia dotyczące przetwarzania danych z wykorzystaniem tzw. *cookies*, dalej hamując rozwój innowacyjnych usług w tym sektorze i ograniczając użytkownikom szeroki i bezpłatny dostęp do informacji i rozrywki w Internecie.

Zbędne obostrzenia w tym zakresie są utrzymywane pomimo, iż praktyka ich stosowania pokazała, że regulacje takie i ich konsekwencje (użytkownicy bezrefleksyjnie klikający zgody na *cookies*) są postrzegane jako uciążliwie i zbędne nawet przez użytkowników końcowych. Należy tu wskazać ponownie na negatywne skutki dla całej branży wydawców online, która w dużej mierze utrzymywana jest dzięki wpływom z reklamy. Ten model biznesowy będzie poważnie zagrożony po wejściu w życie zaproponowanych przepisów.

W dalszym ciągu zmianie nie uległy pryncypia lezące u podstaw projektu EPR, który stara się w sposób iluzoryczny zapewnić bezpieczeństwo użytkowników, narażając ich tym samym na niewygodę ciągłego wyrażania zgód. W naszej ocenie RODO w odpowiednim zakresie chroni dane osobowe.

Ustawodawca europejski w sposób niewystarczający wykorzystuje doświadczenia i wnioski zdobyte po wejściu w życie RODO. Naszym zdaniem postanowienia EPR powinny zapewniać podobną elastyczność w zakresie przetwarzania metadanych jak ma to miejsce w RODO (np. poprzez odwołanie do zgodnego dalszego przetwarzania), oczywiście przy zachowaniu odpowiednich zabezpieczeń takich jak anonimizacja czy pseudonimizacja.

Naszym zdaniem zasadne będzie zastosowanie do danych objętych zakresem projektu rozporządzenia wszystkich podstaw przetwarzania wskazanych w RODO (w tym w szczególności uzasadnionego interesu) i nie warunkowania możliwości przetwarzania danych z usług łączności elektronicznej przede wszystkim od zgody użytkownika. Konieczne jest również zapewnienie tzw. „*level playing field*" wszystkim podmiotom przetwarzającym tego samego typu dane w ramach świadczonych podobnych lub substytucyjnych usług.

EPR w jej proponowanym brzmieniu jako podstawową zasadę wprowadza zakaz przetwarzania danych łączności elektronicznej, a dane mogą być przetwarzane jedynie w bardzo wąsko określonych przypadkach, traktowanych jako wyjątek od zakazu. W naszej ocenie, wprowadzenie projektowanych przepisów uniemożliwi przetwarzanie w UE danych w zakresie niezbędnym do rozwoju usług *machine-to-machine* (M2M), Internet Rzeczy (IoT), gospodarki opartej o przetwarzanie danych, przemysłu 4.0 czy autonomicznych pojazdów.

Kolejny już raz przypominamy, że wskazane powyżej usługi i technologie do rozwoju i komercyjnego wdrożenia wymagają nie tylko samej łączności (usługi łączności elektronicznej), ale również możliwości przetwarzania danych (w szczególności metadanych) generowanych w związku z łącznością elektroniczną, bez czego nie powstaną funkcjonalne i bezpieczne usługi, a jest to przecież jeden z kluczowych celów wskazywanych przez KE i polski rząd w Strategii Odpowiedzialnego Rozwoju.

Dotychczas wprowadzone w tym zakresie zmiany do projektu EPR należy uznać za niewystarczające i nie odpowiadające potrzebom branży. Postulujemy nie wprowadzania przepisów, które w praktyce zahamują rozwój europejskiej gospodarki cyfrowej i uniemożliwią lub znacznie utrudnią wykorzystanie potencjału sieci 5G.

W ocenie IAB nie da się stworzyć usług i technologii, które z definicji bazują i wymagają przetwarzania znacznych ilości danych, w oparciu o regulację prawną, która co do zasady zakazuje przetwarzania danych. Co gorsza, przypadki, w których przetwarzanie danych ma być dopuszczalne, wymagają zgody użytkownika (obwarowanej dodatkowymi, zbędnymi rygorami), co jest w oczywistej sprzeczności z automatyzmem przetwarzania danych wymaganym do niezakłóconej komunikacji M2M (na której ma się opierać m.in. przemysł 4.0 czy autonomiczne pojazdy) i tworzenia usług dodanych w oparciu o tą technologię. Dalsze prace nad tym Projektem, obejmujące m.in. propozycję obwarowania przetwarzania danych pochodzących zM2M dodatkowymi zgodami, użytkowników tylko pogłębiają jego negatywne skutki.

Na końcu tej części pragniemy również w dalszym ciągu zwrócić uwagę na konieczność zapewnienia w projekcie EPR siatki pojęciowej spójnej z innymi unijnymi aktami prawnymi.

2. Zgodność EPR z RODO

IAB, docenia wysiłki kolejnych Prezydencji zmierzające do uspójnienia projektu Rozporządzenia oraz ogólnego rozporządzenia o ochronie danych (RODO). Doceniamy, iż zakres projektu został ograniczony tylko do danych zawierających dane osobowe (art. 1), a nie tak jak w poprzednich projektach do wszystkich danych łączności elektronicznej. Jednakże, projekt ciągle zawiera zapisy dotyczące komunikacji M2M i szczegółowe przepisy zakazujące przetwarzania metadanych, co znacznie rozszerza zakres tego projektu w stosunku do RODO.

Objęcie całej komunikacji maszynowej rozporządzeniem, jest nadmiarowe, gdyż nie każda taka komunikacja zawiera dane osobowe. A wobec bardzo szerokiej definicji danych osobowych z RODO, rozróżnienie kiedy przekazywane dane nieosobowe, a kiedy nie, może być trudne. Ponadto, narazi to na zwiększone koszty producentów połączonych urządzeń, gdyż będą musieli oni dostosować się do EPR, mimo iż ich urządzenia niekoniecznie będą przekazywać

dane osobowe. Objęcie tego dopiero powstającego rynku tak intruzywną regulacją może mieć efekt mrożący i postawić europejskie firmy w niekorzystnej sytuacji wobec globalnych konkurentów.

3. Poufność i bezpieczeństwo komunikacji nadrzędnym celem EPR

Zdaniem IAB, prawdziwym celem EPR i jego wartością dodaną powinna być koncentracja na poufności komunikacji i jej bezpieczeństwie, a nie ochronie danych osobowych, które są już dostatecznie chronione przez RODO.

Obecnie projekt w dalszym ciągu zaciera i miesza te dwie różne kwestie, które wynikają z różnych podstaw prawnych: poufność komunikacji (art. 7 Karty Praw Podstawowych) i ochrona danych/prywatności (art. 8 Karty Praw Podstawowych). Chociaż te dwa prawa są ze sobą ściśle powiązane, to są odrębne. Celem RODO jest wdrożenie i uszczegółowienie przepisów art. 8 (i art. 16 TFUE), z kolei EPR powinien wprowadzić w życie art. 7. Poprzez większą koncentrację projektu EPR na danych nakłada on, naszym zdaniem nadmiarowe obowiązki, niepotrzebnie regulując i wychodząc poza zakres RODO (np. metadane, czy komunikację M2M).

Apelujemy, aby skierować wysiłki legislacyjne na zapewnienie, aby EPR dostateczne silnie chroniło poufność i bezpieczeństwo komunikacji elektronicznej. Jednocześnie wzywamy, aby uniknąć nadmiernej regulacji, która mogłaby niepotrzebnie osłabić konkurencyjność gospodarczą Europy lub nałożyć nieproporcjonalne obciążenia na europejskich innowatorów cyfrowych, szczególnie w powstających dziedzinach uczenia maszynowego i sztucznej inteligencji.

4. Podsumowanie i ocena zmian zawartych w projekcie EPR z 26 lipca 2019 r.

Artykuł 6 – dozwolone przetwarzanie danych łączności elektronicznej

W zakresie art. 6 przewiduje przede wszystkim zmiany redakcyjne i upraszczające. Najbardziej widoczną zmianą jest wprowadzenie podziału art. 6 EPR na cztery odrębne przepisy, co ma spowodować większą przejrzystość regulacji. Każdy przepis reguluje przetwarzanie określonego rodzaju danych:

- art. 6 - wszystkie dane dotyczące łączności elektronicznej (treść i metadane);
- art. 6a - treści z zakresu łączności elektronicznej;
- art. 6b - metadane dotyczące łączności elektronicznej;
- art. 6c - dalsze przetwarzanie metadanych z zakresu łączności elektronicznej.

Kolejna widoczna zmiana to wprowadzenie w nowym art. 6 (dot. wszystkich danych) ogólnej zasady, zgodnie z którą dane te mogą być przetwarzane tylko przez okres niezbędny do realizacji dozwolonych celów oraz jeżeli cele te nie mogą zostać osiągnięte poprzez przetwarzanie informacji, które stały się anonimowe.

Jak zostało wskazane we wprowadzeniu do projektu EPR z 26 lipca 2019 r. wyciągniecie powyższych regulacji przed nawias (wcześniej były rozsiane po poprzedniej wersji art. 6) miało jednoznacznie potwierdzić ich uniwersalne zastosowanie w zakresie danych dotyczących łączności elektronicznej. W naszej ocenie objęcie tą regulacją tak szerokiego spektrum danych należy uznać za nadmiarowe. Takie stanowisko w zakresie danych dot. łączności elektronicznej prezentujemy od dawna i jest ono nadal aktualne.

Na marginesie warto również zwrócić uwagę na zasadne zmiany wprowadzone w nowym art. 6 ust. 1 lit. d), art. 7 ust. 4 oraz art. 11 EPR, które były postulowane uprzednio w toku konsultacji i mają na celu zapewnienie spójności całości EPR w zakresie możliwości wprowadzania przez państwa członkowskie UE bardziej restrykcyjnych regulacji w stosunku do omawianego projektu.

IAB docenia rozszerzenie legalnych podstaw dla dozwolonego przetwarzania metadanych (w celu ochrony ważnych interesów dla życia jednostki oraz w celach naukowych i statystycznych), jednakże zmiany te są naszym zdaniem niewystarczające. Zgadzamy się, że ochrona danych osobowych jest wartością, którą należy chronić. Jednak RODO, naszym zdaniem dobrze wywiązuje się z tego zadania. Natomiast zapisywanie, w prawie, iż w tak innowacyjnym sektorze jak sektor cyfrowy, aby zacząć świadczyć pewne jakieś usług konieczna będzie zgoda (przewiduje to motyw 17) nie ma nic wspólnego z rzekomo popieraną przez KE nieskrępowaną innowacyjnością. IAB uważa, iż w biznesie dozwolone powinny być wszystkie te czynności, które są legalne, a czasy, kiedy należy zapytać się instytucji publicznych o zgodę należą do słusznie minionych. Niepokoi nas zmiana tego podejścia.

Artykuł 8 – ochrona informacji w urządzeniach użytkowników końcowych

Jako zasadne należy ocenić zmiany dokonane w zakresie art. 8 EPR. W zakresie ust. 1 pkt (c) zostało usunięte ograniczenie ujętego tam wyłączenia tylko do usług społeczeństwa informacyjnego – usunięcie słów „*information society*". W ust. 1 pkt (e) usunięte zostało słowo „*security*", co zwiększa zakres aktualizacji korzystających zawartego tam wyłączenia.

Natomiast niezrozumiała jest dla nas zastosowana w motywie 21a oraz art. 8 (da) logika zmiany, zgodnie z którą tylko dostawcy usług społeczeństwa informacyjnego uzyskiwaliby możliwość zbierania i wykorzystywania danych z urządzeń końcowych (*end-users' terminal equipment information*) do celów związanych z utrzymaniem/przywróceniem bezpieczeństwa usług, zapobieganiu fraudom i wykrywania błędów technicznych. Podejście takie jest wyraźnie dyskryminacyjne w stosunku do dostawców usług łączności elektronicznej i kompletnie nieuzasadnione z punktu widzenia bezpieczeństwa usług i użytkowników. Z tego względu postulujemy zmianę treści art. 8 (da) na:

(da) it is necessary to maintain and restore the security of information society services and electronic communications services, prevent fraud or detect technical faults for the duration necessary for that purpose; or

Jednocześnie, cieszy wykreślenie ostatniego zdania z motywu 21(a), co było przez nas poprzednio postulowane:

Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of the information society service, such as IoT (for instance connected devices, such as connected thermostats), requested by the end-user.

Mamy nadzieję, że zmiana ta utrzyma się w toku dalszych prac.

Art. 10 – opcje dot. ustawień prywatności

Jednocześnie, z zadowoleniem przyjmujemy propozycję usunięcia art. 10 i wyrażamy nadzieję, że zmiana ta zostanie zachowana.

W trakcie dyskusji na temat wniosku w sprawie Rozporządzenia e-Privacy art. 10 budził wiele obaw i kontrowersji, które dotyczyły nadmiernego obciążenia przeglądarek i aplikacji, aspektu konkurencyjności, związku z karami za nieprzestrzeganie przepisów oraz wpływu tego przepisu na sytuację użytkowników końcowych np. kwestia „zmęczenia" zgodami. W świetle powyższego, przepis budził wątpliwości co do jego faktycznej wartości dodanej.

Pragniemy zwrócić uwagę, iż zgodnie z EPR, gdy usługodawca posiada zgodę użytkownika na realizację określonych celów z wykorzystaniem technologii opartych o *cookies*, będzie on mógł umieścić *cookies* we wskazanych celach na urządzeniu użytkownika. Tym samym, przeglądarka nie powinna co do zasady blokować usługodawcom możliwości umieszczania plików *cookies*. Z tego względu należy zapewnić, że obowiązek przeglądarki będzie się ograniczać do wysłania sygnału do usługodawców, którzy będą następnie weryfikować, czy posiadają zgodę (inne podstawy prawne) na wykorzystywanie technologii opartych o *cookies*.

5. Pozostałe uwagi

Marketing bezpośredni

Pozytywnie oceniamy usunięcie z tekstu (motywy i artykuły) dot. marketingu bezpośredniego (*direct marketing*) słowa „*present/presented*" i wyrażamy nadzieję, że zmiana ta zostanie zachowana.

Metadane geolokalizacyjne

W dalszym ciągu postulujemy rewizję podejścia do koncepcji zbierania i przetwarzania metadanych geolokalizacyjnych na potrzeby statystyczne, naukowe, oraz na potrzeby

tworzenia innowacyjnych usług/systemów/produktów które mogą przyczynić się do wzrostu bezpieczeństwa obywateli, poprawy sprawności ruchu miejskiego, czy jakości życia.

Jak IAB Polska wskazywało już uprzednio, motyw 17aa wyraźnie wskazuje jak cenne mogą być tego typu dane oraz warunki, na jakich dopuszcza się przetwarzanie danych statystycznych bez konieczności uzyskania zgody użytkownika (m.in. anonimizacja). Jednocześnie jednak, użytkownik otrzymuje prawo do sprzeciwu – *opt-out* (motywy 17aa i 17 b). Podejście takie stawia pod znakiem zapytania wiarygodność i reprezentatywność całego zbioru danych statystycznych zebranych z danego miejsca w danym czasie.

Wyobraźmy sobie bowiem, że na potrzeby wprowadzenia systemu usprawnienia ruchu i zwiększenia jego bezpieczeństwa zbierane są dane lokalizacyjne z jakiegoś skrzyżowania celem zmierzenia natężenia ruchu i że przez to skrzyżowanie przejeżdża 1000 pojazdów w danej jednostce czasu. Dane takie mógłby zbierać np. operator telekomunikacyjny i po zanonimizowaniu, przekazywać stronie trzeciej, której są one niezbędne do prowadzenia prac nad systemem. Jeżeli jedna trzecia użytkowników/kierowców tych pojazdów wyraziłaby sprzeciw co do zbierania ich danych lokalizacyjnych, otrzymane dane dot. wolumenu ruchu w tymże miejscu wskazałyby jedynie 666 pojazdów, co stanowiłoby liczbę przekłamaną i nie stanowiącą żadnej wartości statystycznej. Powstają także istotne wątpliwości, co do sposobu w jaki użytkownik miałby być informowany o fakcie zbierania danych lokalizacyjnych w takiej sytuacji (informacje dostępne/wiszące przed skrzyżowaniem, czy SMS wysyłane do użytkowników zbliżających się do skrzyżowania byłyby całkowicie nieadekwatnym rozwiązaniem).

Postulujemy, aby zasady zbierania i przetwarzania danych geolokalizacyjnych były identyczne dla wszystkich podmiotów dokonujących tych czynności i podlegały wyłącznie RODO. Zastosowanie w EPR specjalnych przepisów w tym zakresie tylko w odniesieniu do podmiotów świadczących usługi łączności elektronicznej uniemożliwi efektywny rozwój nowych potrzebnych rozwiązań i usług, w tym planowanych na bazie sieci 5G. Ponadto należy podkreślić, że z punktu widzenia użytkownika końcowego bardziej istotne jest, aby pewne typy danych (w tym metadanych geolokalizacyjnych, czy danych wrażliwych) podlegały takim samym zasadom ochrony, bez względu na to jaki podmiot je przetwarza i czy jest on objęty rygorami Rozporządzenia e-Privacy, czy też nie.

Zgoda użytkownika na zapisywanie i odczytywanie informacji z plików cookies

Z zadowoleniem przyjmujemy usunięcie z tekstu motywu 22a ostatniego zdania o następującym brzmieniu:

The responsibility for obtaining consent with the storage of a cookie and for any penalties for breach of duty lies on the information society service provider.

Jednocześnie wyrażamy nadzieję, że zmiana ta zostanie utrzymana.

Regulacje dot. walki z pornografią dziecięcą

W naszej ocenie niejasne są przesłanki i cel wprowadzenia nowych zapisów do art. 29 ust. 3. Nie jest dla nas jasne, z jakiego powodu kwestia walki z pornografią dziecięcą ma w projekcie EPR własne, odrębne regulacje, podczas gdy takich odrębnych regulacji nie ma w odniesieniu do walki z innymi, nielegalnymi treściami, np. o charakterze terrorystycznym. O ile potrzeba walki z pornografią dziecięcą jest w pełni zrozumiała, o tyle takie podejście grozi fragmentaryzacją przepisów EPR i rodzi pytania o przewarzanie danych w zakresie niezbędnym do walki z innymi niż pornografia dziecięca typami nielegalnych treści. Wydaje się, że zasady zbierania i przetwarzania danych na potrzeby walki z nielegalnymi treściami powinny być takie same dla wszystkich podmiotów objętych EPR i opierać się na proporcjonalnych i przejrzystych przesłankach, aby cel któremu służą mógł być efektywnie osiągnięty. Dodatkowo nie jest dla nas jasne, dlaczego wskazany przepis ma charakter czasowy, tzn. ma przestać obowiązywać w określonej dacie (obecnie nieznanej). Nie znając szerzej przyczyn dodania tych zapisów, nie podejmujemy się ich szczegółowej oceny.

Wytyczne Europejskiej Rady Ochrony Danych

Jesteśmy przeciwni dodaniu w art.19 pkt (da) i (db) przepisów odnoszących się do wydawania przez European Data Protection Board wytycznych, rekomendacji, w szczególności w zakresie punktu (da). Biorąc pod uwagę szybki rozwój technologii, aplikacji i usług, rekomendacje takie mogą szybko się dezaktualizować, ponadto dotychczasowe doświadczenia z wytycznymi dot. RODO wydawanymi przez Grupę Roboczą art. 29 wskazują, iż wytyczne takie często podlegają dużej arbitralności i wyraźnie wykraczają poza zakres regulacji do których się odnoszą. Z tego względu postulujemy wykreślenie punktów (da) i (db) z art. 19.

Z poważaniem,

Włodzimierz Schmidt
Prezes Zarządu

Do wiadomości:

Pan Michał Pukaluk, Dyrektor Departamentu Polityki Międzynarodowej

Związek Pracodawców Branży Internetowej IAB Polska
ul. Puławska 39 lok. 77 02-508 Warszawa tel. +48 22 415 54 44 fax +48 22 212 87 74
www.iab.org.pl