

Warszawa, dnia 15 stycznia 2018 r.

Pan
Krzysztof Szubert
Sekretarz Stanu
Pełnomocnik Rządu RP ds. Jednolitego Rynku
Cyfrowego
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

Zgodnie z informacjami zawartymi w programie prac Prezydencji bułgarskiej na pierwszą połowę 2018 r. w części dot. Rady ds. Transportu, Telekomunikacji i Energii, wysiłki Prezydencji skierowane będą m.in. na znalezienie rozwiązań gwarantujących poszanowanie prywatności użytkowników, ochronę danych osobowych i poufność korespondencji, by wzmocnić rozwój innowacji cyfrowych. To oznacza m.in. kontynuację prac nad **projektem rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej uchylającego dyrektywę 2002/58/WE** (dalej: *ePrivacy*).

Związek Pracodawców Branży Internetowej IAB Polska wielokrotnie przedstawiał zarówno stanowisko kierunkowe, jak i szczegółowe uwagi do treści projektu, w tym dotyczące jego niezgodności z RODO i negocjowanym Kodeksem Łączności Elektronicznej, a przedstawiciele naszych firm członkowskich osobiście wyjaśniali obawy związane z przyjęciem rozporządzenia w zaproponowanej przez Komisję Europejską formie na spotkaniu z udziałem Pana Ministra, posła sprawozdawcy z Parlamentu Europejskiego pana Michała Boniego oraz przedstawicieli Komisji Europejskiej i interesariuszy, które odbyło się 11 października 2017 r. w Stałym Przedstawicielstwie Rzeczypospolitej Polskiej przy Unii Europejskiej w Brukseli.

Wyrażamy zadowolenie, że w następstwie ww. działań została nawiązana ścisła współpraca z Ministerstwem także na poziomie roboczym, która – mamy nadzieje – będzie rozwijana na dalszym etapie negocjacji.

Mając na względzie fakt, iż Parlament Europejski przyjął niewielką większością głosów niekorzystny z punktu widzenia biznesu internetowego mandat do negocjacji z Radą dot. *ePrivacy*, a prezydencja estońska zakończyła swoje prace przedstawiając 5 grudnia 2017 r. na poziomie roboczym tekst kompromisowy, który także nie odpowiada postulatam branży internetowej, pragniemy jeszcze raz – przed pierwszym spotkaniem grupy roboczej TELE pod przewodnictwem bułgarskim - nakreślić główne wątki stanowiska IAB Polska, a także doprecyzować pewne kwestie szczegółowe.

Najkorzystniejszym rozwiązaniem postulowanym przez branżę internetową byłoby zaprzestanie prac nad projektem rozporządzenia *ePrivacy* i pozostawienie w tym obszarze rozwiązań regulowanych obowiązującą dyrektywą, która ewentualnie powinna zostać jedynie dostosowana do aktualnych rozwiązań technologicznych.

Jeżeli jednak, z uwagi na poczyniony do tej pory postęp w negocjacjach nad projektem rozporządzenia *ePrivacy*, ww. rozwiązanie nie wydaje się możliwe do zrealizowania, postulujemy aby Polska przyłączyła się do budującej się koalicji państw członkowskich, które postulują jak największe ograniczenie rozwiązań, które są niebezpieczne dla rozwoju branży internetowej i innowacyjnych, przyjaznych dla klientów usług.

Dodatkowo, zwracamy uwagę, że nie jest już możliwe dochowanie zakładanego przez Komisję Europejską terminu wejścia w życie rozporządzenia *ePrivacy* łącznie z rozporządzeniem RODO, czyli 25 maja 2018 r., dlatego też uważamy, że jeżeli negocjacje nad projektem rozporządzenia *ePrivacy* będą toczyć się dalej, to powinny przebiegać spokojnie, z dbałością o jakość wypracowanych finalnie rozwiązań, a bez zbędnej presji ze strony Komisji Europejskiej, której zależy na zakończeniu wszystkich negocjacji w obszarze Jednolitego Rynku Cyfrowego, co stanowi polityczny priorytet Komisji Europejskiej, do końca br. Uważamy, iż priorytety polityczne nie mogą być realizowane kosztem jakości stanowionego prawa oraz że korzystniej będzie najpierw poobserwować praktyczne funkcjonowanie rozwiązań RODO, a dopiero następnie wypełnić ewentualne luki dot. ochrony prywatności.

W projekcie rozporządzenia *ePrivacy* szczególnie zależy nam na następujących kwestiach:

- utrzymaniu wprowadzonego w ostatniej wersji dokumentu w **art.3 ust.1 (a)** pojęcia „*content in transmission*”, wskazując jednocześnie na konieczność zachowania

spójności takiego podejścia przy wszystkich odniesieniach w dokumencie do słowa „*content*”, w tym w definicji w art. 4;

- usunięciu z **art.3 ust.1 (cc)** słów “*or presenting*”, tak aby zapis brzmiał: “*the sending or ~~presenting~~ of direct marketing communications to end-users who are in the Union*”. Na bazie obecnej wersji przepisu, można byłoby przyjąć, że każdy baner reklamowy pojawiający się na stronie www podpada pod te ograniczenia, co byłoby nadmiernym, nieuzasadnionym i szkodliwym ograniczeniem reklamy, jak również obowiązkiem nieproporcjonalnym do celów rozporządzenia. Konsekwentnie, dla zachowania spójności aktu, postulujemy analogiczne zmiany dot. prezentowania komunikacji marketingowej w **art.4 ust.3 (f) oraz art.16 ust.1 i 2**;
- **wyłączeniu** usług komunikacji interpersonalnej z zakresu *ePrivacy* w **art. 4 ust. 2 ancillary services**. W obecnym brzmieniu obejmuje on usługi, które pełnią funkcję dodatkową do usługi głównej, np. komunikatory pozwalające na rozstrzygnięcie sporów on-line (ADR) na platformach pozwalających na zawieranie umów pomiędzy użytkownikami;
- **usunięciu z art.4a ust.3** zapisu dot. cyklicznego przypominania użytkownikom o możliwości wycofania zgody, jako że taka praktyka będzie uciążliwa i irytująca dla większości użytkowników;
- przywróceniu pierwotnego brzmienia przepisu z **art.5 ust.1**, którego istotą była ochrona tajemnicy komunikowania się, a nie zakaz przetwarzania danych. Zakaz wszelkiego przetwarzania danych jest niezgodny z filozofią RODO, jak również z art. 1 ust. 2 niniejszego rozporządzenia, który ustanawia swobodę przepływu danych w ramach UE (a taki przepływ jest bez wątpienia przetwarzaniem danych, co z kolei na mocy obecnie proponowanego brzmienia art. 5 ust. 1 tego rozporządzenia miałyby być zakazane);
- **usunięciu art. 6** (*permitted processing of electronic communications data*). Stoimy na stanowisku, iż przetwarzanie *electronic communications data* (w tym *metadata* i *content*) powinno podlegać takim samym przesłankom przetwarzania, jakie zostały przyjęte w RODO dla przetwarzania danych osobowych osób prywatnych. Jeżeli jednak okaże się to niemożliwe, ewentualnie jako minimum proponujemy dodanie uzasadnionego interesu jako dozwolonego celu przetwarzania metadanych i contentu pochodzących z łączności elektronicznej. Ewentualnie, należy zmienić art. 6 w następujący sposób: ust. 3 powinien zostać uzupełniony - analogicznie do art. 6 ust 2 b - o możliwość przetwarzania treści komunikatów, jeśli wynika to z zawartej przez użytkownika umowy i użytkownik został o tym uprzednio poinformowany. Dotyczy to możliwości

przetwarzania danych w przypadku rozpatrywania reklamacji, rozstrzygania sporów pomiędzy użytkownikami w ramach mechanizmów ADR oferowanych m.in. przez niektóre platformy internetowe. Proponujemy dodanie do ustępu 3 lit c. zgodnie z którą: *it is necessary for **performance of the contract to which the end-user is party, including billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services as well as for the purpose of ADR mechanisms or...***;

- **usunięciu art. 7** (*storage and erasure of electronic communications data*). W przypadku pozostawienia tego artykułu, pragniemy zgłosić duże wątpliwości co do celowości dodania odnoszącego się do metadanych zapisu w art.7 ust.2: „*Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.*” Nie jest także jasne, jakie wynikałyby z niego obowiązki dla dostawcy usług, np. gdyby była konieczność zapewnienia przenoszalności metadanych, byłby to obowiązek nadmiarowy. Podobnie uważamy także za niezasadne umieszczenie tego samego zapisu w art. 7 ust.1;
- **usunięciu artykułu 8** i poddaniu kwestii przetwarzania danych gromadzonych w oparciu o technologie wykorzystujące *cookies* pod RODO. Ewentualnie należy rozważyć dodanie do art. 8 przesłanki uzasadnionego interesu. Pozwoli to na każdorazową ocenę m.in. inwazyjności konkretnej technologii w prywatność, celów, w jakich dane są przetwarzane i podstaw prawnych przetwarzania. Obecny stan, w którym katalog przetwarzania danych osobowych wg RODO jest znacznie szerszy niż proponowane w projekcie *ePrivacy* podstawy korzystania z technologii wykorzystujących *cookies* – z których znaczna część nie bazuje na przetwarzaniu danych osobowych - jest całkowicie niezrozumiały. Jako docelowy, tzn. będący efektem kompromisu pomiędzy Radą a Parlamentem tekst proponujemy brzmienie artykułu wskazane w dokumencie *Joint Amendments of the European publishing, media, and advertising industries* z 30 listopada 2017 r. Ponadto za konieczne uważamy dodanie w **art. 8 ust.1** kolejnych podpunktów o następującym brzmieniu:
(aa) processing is necessary for the performance of a contract to which the end user is party or in order to take steps at the request of the end user prior to entering into a contract"
(f) it is necessary for compliance with a legal obligation.

Artykuł ten powinien zostać uzupełniony o dodatkową przesłankę, pozwalającą na przetwarzanie danych, jeśli jest to konieczne dla spełnienia wymogów narzuconych przez prawo. W szczególności taka podstawa jest konieczna w świetle wymogów stawianych przez art. 10 *ePrivacy*, w tym wymóg, aby oprogramowanie zainstalowane przed datą wejścia w życie rozporządzenia zostało dostosowane / zaktualizowane do nowych wymogów (art. 10 ust. 3 projektu rozporządzenia *ePrivacy*). Bez tej podstawy prawnej przetwarzana, konieczne będzie uzyskanie zgody użytkownika na aktualizację oprogramowania, również w tych przypadkach, gdzie aktualizacja jest wymagana przez przepisy prawa (np. art. 10 ust. 3). Pojawi się również problem odpowiedzialności i kar finansowych za brak aktualizacji wymaganych prawem, gdzie przyczyną braku aktualizacji jest brak zgody użytkownika.

NEW (g) it is necessary for billing, calculating payments, detecting or stopping fraudulent, abusive, or otherwise unauthorised use of information society services; or
NEW (f) it is necessary to maintain or restore the security of information society services and services, or detect technical faults and/or errors and/or attacks against information society services, for the duration necessary for that purpose

NEW (h) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the user of the terminal equipment can take to stop or minimise the collection. The collection of such information shall be conditional on the application of appropriate technical measures and the application of organizational measures, which shall include inter alia pseudonymisation, to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679.

- **usunięciu art. 10** – postulat ten został już przedłożony w dokumencie *Joint Amendments of the European publishing, media, and advertising industries* z 30 listopada 2017 r. Jeżeli usunięcie art. 10 wydaje się niemożliwe, postulujemy następującą zmianę jego brzmienia, z uwagi na konieczność zapewnienia, że obowiązek przeglądarki będzie się ograniczać do wysłania sygnału do usługodawców, którzy będą następnie weryfikować, czy posiadają zgodę (albo inne podstawy prawne) na wykorzystywanie technologii opartych o *cookies*.

Article 10 Information and options for privacy settings to be provided

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third **any other parties than the end-user** from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

2. Upon installation **or first usage**, the software **referred to in paragraph 1** shall inform the end-user about the privacy settings options and, to continue with the installation **or usage**, require the end-user to consent to a setting.

2a. The software referred to in paragraph 1 shall provide in a clear manner easy ways for end-users to change the privacy setting consented to under paragraph 2 at any time during the use.

2aa. Privacy settings referred to in par. 1 shall not preclude service providers from storing information on the terminal equipment of an end-user or processing information already stored on that equipment if the service provider has a valid legal ground, including end user content, for such processing.

Dodatkowo, żeby zapewnić, że ustawienia przeglądarki nie będą barierą dla usługodawców, którzy posiadają podstawę do wykorzystywania technologii opartych na *cookies*, w tym zgodę użytkownika, warto dodać w motywie 22:

(22) (...) Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored. **This should not however exclude storing information on the terminal equipment of an end-user or processing information already stored on that equipment by service providers that have legal ground for processing data under article 8, including consent.**

W pozostałym zakresie podtrzymujemy wcześniej zgłoszone uwagi i postulaty. W razie dodatkowych pytań i wątpliwości pozostajemy do dyspozycji.

Z poważaniem,

A handwritten signature in black ink, appearing to read 'W. Schmidt', with a long, sweeping flourish extending to the right.

Włodzimierz Schmidt

Prezes Zarządu