Warszawa, dnia 11 maja 2018 r.

Ministerstwo Cyfryzacji
Departament Telekomunikacji
Wydział Regulacyjny
Ul. Królewska 27
00-060 Warszawa

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 PRZYGOTOWANEJ PRZEZ PREZYDENCJĘ BUŁGARSKĄ

Szanowni Państwo,

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.

1. Wstęp

Na samym wstępie pragniemy podtrzymać, zgłaszane wcześniej przez środowisko przedsiębiorców internetowych uwagi do projektu rozporządzenia, w tym przede wszystkim wielokrotnie powtarzane następujące postulaty natury ogólnej. Uważamy, że projektowane przepisy są szkodliwe dla innowacyjności gospodarki europejskiej oraz postawią one w niekorzystnej sytuacji europejskie firmy wobec ich globalnych rywali. Dodatkowo, regulacja zapewni tylko iluzoryczne bezpieczeństwo użytkowników (RODO naszym zdaniem już odpowiednio dobrze chroni dane osobowe) narażając ich tym samym na niewygodę ciągłego

wyrażania zgód. Naszym zdaniem konieczne jest uwzględnienie w pracach nad projektem EPR doświadczeń i wniosków zdobytych po wejściu w życie RODO

Należy zwrócić uwagę, iż EPR w jego 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. Wprowadzenie projektowanych przepisów praktycznie 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. Te usługi i technologie do swojego 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.

Postulujemy niewprowadzanie przepisów, które w praktyce zahamują rozwój europejskiej gospodarki cyfrowej i uniemożliwią lub znacznie utrudnią wykorzystanie potencjału sieci 5G dla rozwoju innowacyjnych rozwiązań i usług uwzględniających potrzeby społeczeństwa XXI wieku przy zachowaniu proporcjonalnych, transparentnych, sprawiedliwych i faktycznie efektywnych zasad ochrony bezpieczeństwa i prywatności danych i użytkowników,

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 tę technologię. Dalsze prace nad tym Projektem, obejmujące m.in. propozycję obwarowania przetwarzania danych pochodzących z M2M dodatkowymi zgodami użytkowników tylko pogłębiają jego negatywne skutki.

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.

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.

EPR 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 automatycznie 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.

IAB Polska nie kwestionuje potrzeby zapewnienia ochrony danych osobowych, jednakże zwraca uwagę, że restrykcyjne przepisy RODO gwarantują już dostateczną ochronę prywatności użytkowników. Dlatego, 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.

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

2. Prawdziwa wartość dodana 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 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 powinno 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 pewności, aby EPR dostatecznie 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.

3. Zgodność EPR z RODO

IAB, docenia wysiłki Prezydencji zmierzające do uspójnienia projektu EPR oraz 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 są 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.

Co więcej, EPR ciągle, mimo wielokrotnych wezwań strony biznesu, przewiduje ograniczone możliwości przetwarzania metadanych ze względu na uzasadniony interes (co jest możliwe zgodnie z RODO). Obecnie "uzasadniony interes" jest uzasadnieniem dla przetwarzania danych, o ile interesy te nie są sprzeczne z prawami podstawowymi i swobodami użytkowników. Podczas gdy zgodnie z RODO "uzasadniony interes" jako podstawa przetwarzania danych jest elastyczny i ma charakter otwarty. Skutkiem tego użytkownicy napotykać będą liczne i rozpraszające prośby o zgodę od producentów urządzeń, operatorów sieci, dostawców systemów operacyjnych i twórców aplikacji – czyli powtórzy się problem banera „cookies" na stronach, który rozporządzenie EPR stara się naprawić. Ponadto, ponieważ uzyskiwanie zgody nie w każdym przypadku okazuje się praktyczne, niektóre funkcje urządzeń i funkcje oprogramowania, które są obecnie automatycznie dostarczane, mogą zostać zatrzymane, chyba że zostanie zmieniony artykuł 8 projektu.

4. Przetwarzanie metadanych

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 wywiąże się z tego zadania. Natomiast zapisywanie w prawie, iż w tak innowacyjnym sektorze jak sektor cyfrowy, aby zacząć świadczyć pewne usługi 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.

Ponadto postulujemy dodanie nowych punktów f,h,i:

NEW (f) it is within the legitimate interests of the provider of the terminal equipment and its operating software, an electronic communications service or an information society service, except where such interests are overridden by the interests or fundamental rights and freedoms of the end-user.

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 organisational 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.

NEW (i) it is necessary to comply with a legal obligation under Union or Member State law.

W zakresie art. 10, postulujemy przywrócenie poprzedniej wersji zapisu ustępu 2a:

"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"

Postulujemy również dodanie pkt 2aa:

2aa. Privacy settings referred to in par. 1 shall not preclude service providers form 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.

Pragniemy zwrócić uwagę, iż zgodnie z projektem 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. Marketing bezpośredni

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

6. Metadane geolokalizacyjne

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.

Nowy 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 wysyłany 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 EPR, czy też nie.

7. Dane z urządzeń końcowych

Z podobnych względów, niezrozumiała jest 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, zapobieganiem fraudom i wykrywaniem 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

oraz wykreślenie ostatniego (dodanego w ostatniej wersji projektu) zdania z motywu 21 (a): ***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.***

8. Zgoda użytkownika na zapisywanie i odczytywanie informacji z plików cookies

Na końcu motywu 22a dodano nowe zdanie 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.

Powyższe zdanie jest sprzeczne z art. 8 ust. 1 b) w związku z art. 4a ust. 2 projektu EPR. Oba ww. przepisy czytane razem stanowią, że na zapisanie i odczytanie informacji z plików cookies każdy podmiot, który taką technologię stosuje, musi pozyskać zgodę użytkownika (z zastrzeżeniem wyjątków, w których projekt rozporządzenia takiej zgody nie wymaga). Jednocześnie art. 4a ust. 2 jednoznacznie stanowi, że:

[…] for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.

Tym samym projekt rozporządzenia wprost dopuszcza możliwość wyrażenia analizowanej zgody przez ustawienia przeglądarki (albo innego oprogramowania służącego temu samemu celowi). W scenariuszu, w którym zgody na cookies są wyrażane przez ustawienia przeglądarki, w procesie wyrażania takiej zgody udział biorą co najmniej dwa podmioty, z których żaden nie ma kontroli, a tym samym nie może ponosić odpowiedzialności za drugi:

a) podmiot, który w swoim serwisie www wykorzystuje pliki cookies, który będzie obowiązany co najmniej do poinformowania użytkownika o wykorzystywanych plikach cookies i o możliwości zarządzania ustawieniami prywatności z poziomu przeglądarki internetowej (co do zasady dostawca usługi społeczeństwa informacyjnego);
b) dostawca przeglądarki internetowej, której ustawienia są wykorzystywane do wyrażenia albo niewyrażenia analizowanej zgody;

Każda przeglądarka ma inne zasady i mechanizmy dotyczące zarządzania wykorzystaniem plików cookies. Różnice pomiędzy przeglądarkami potrafią być znaczące zarówno w zakresie wielości ustawień i poziomów prywatności, jak i łatwości dostępu i obsługi tych funkcjonalności przez przeciętnego użytkownika. Kilka najpopularniejszych przeglądarek internetowych pochodzi od globalnych dostawców i ma zasięg globalny, w związku z czym nawet najwięksi krajowi dostawcy usług społeczeństwa informacyjnego nie mają w zasadzie żadnego wpływu na to, jak wyglądają ustawienia prywatności w poszczególnych przeglądarkach. Tym samym całkowicie nieuzasadnione jest założenie, że za każdy problem i ewentualną nieprawidłowość

w wyrażaniu zgód z wykorzystaniem ustawień przeglądarki internetowej, całkowitą i wyłączną odpowiedzialność ma ponosić dostawca usługi społeczeństwa informacyjnego.

Zdanie dodane na końcu motywu 22a, przesądzające, że w każdym przypadku, za wszelkie potencjalne nieprawidłowości w procesie informowania, pozyskiwania i zapisywania zgody użytkownika na cookies, wyłączną odpowiedzialność (w tym w szczególności ryzyko kar pieniężnych i ewentualnie odpowiedzialności cywilnej albo karnej – w zależności od ostatecznego kształtu przepisów rozporządzenia i przepisów krajowych) ponosi dostawca usług społeczeństwa informacyjnego jest – w świetle powyżej przedstawionej argumentacji – całkowicie nieuzasadnione, w szczególności jeśli wyrażenie takich zgód odbywa się przez ustawienia przeglądarki internetowej.

W związku z powyższym z motywu 22a należy usunąć ostatnie zdanie. Należy zwrócić uwagę, że bez tego zdania w motywie 22a ustalenie zasad, zakresu i podziału odpowiedzialności pomiędzy dostawców usług społeczeństwa informacyjnego a dostawców przeglądarek internetowych będzie się odbywało na gruncie art. 4a ust. 2, art. 8 ust. 1 oraz art. 10 projektu rozporządzenia EPR, z uwzględnieniem faktycznych ról, zadań i obowiązków tych dwóch kategorii podmiotów w procesie pozyskiwania zgód na cookies z wykorzystaniem ustawień przeglądarek, bez sztucznego i nieuzasadnionego przesądzania w motywie, w sposób sprzeczny z brzmieniem samych przepisów, że cała odpowiedzialność w każdym przypadku spada na dostawców usługi społeczeństwa informacyjnego.

Ponadto, należy pamiętać, że dostawca usługi może na swojej stronie internetowej realizować inną kategoryzację cookies (wraz z poziomem wyrażania zgód na różne rodzaje cookies) niż wynikałoby to z ustawień przeglądarki stosowanej przez użytkownika. Jeżeli dostawca ma być odpowiedzialny za ew. naruszenia związane ze zgodą użytkownika na cookies, powinno to mieć miejsce wyłącznie w sytuacji, gdy użytkownik świadomie wyrazi swą zgodę na podstawie opcji cookies udostępnianych przez tego dostawcę, tym samym rezygnując dla tej konkretnej witryny z opcji ustawienia zgody poprzez przeglądarkę. Z kolei brak aktywności użytkownika w tym zakresie, byłby równoznaczny z obowiązkiem respektowania przez dostawcę zgody wyrażonej przez użytkownika poprzez ustawienia cookies w przeglądarce.

Niezależnie od powyższych uwag, należy podkreślić, iż motyw rozporządzenia nie jest właściwym miejscem do określania zasad odpowiedzialności za naruszenie przepisów. Tekst motywu nie może zawierać treści normatywnej niemającej swojego odzwierciedlenia w treści samych przepisów, tym bardziej tekst motywu nie może być sprzeczny z tekstem samych przepisów. Zagadnienie zasad, zakresu i rodzaju odpowiedzialności za naruszenia przepisów rozporządzenia to materia, która może zostać uregulowana tylko i wyłącznie w tekście przepisów rozporządzenia, a postanowienia motywów mogą jedynie wyjaśniać i pomagać w interpretacji tych przepisów.

Dodatkowo, jesteśmy przeciwni dodaniu w art.19 punktów (da) i (db) 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

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