

Warszawa, dnia 15 stycznia 2021 r.

Departament Zarządzania Danymi
Kancelaria Prezesa Rady Ministrów

**UZUPEŁNIENIE STANOWISKA ZWIĄZKU PRACODAWCÓW BRANŻY
INTERNETOWEJ INTERACTIVE ADVERTISING BUREAU (IAB POLSKA) DO
PROJEKTU ROZPORZĄDZENIA W SPRAWIE ZARZĄDZANIA DANymi (DATA
GOVERNANCE ACT) Z DNIA 25 LISTOPADA 2020 ROKU**

Szanowni Państwo,

W uzupełnieniu do stanowiska IAB Polska z dnia 17 grudnia 2020 r. dot. projektu unijnego rozporządzenia w sprawie zarządzania danymi, tzw. **Data Governance Act** (dalej jako: „Rozporządzenie”), poniżej przedstawiamy bardziej szczegółowe uwagi do rozwiązań zaproponowanych w Rozporządzeniu:

- **Warunki ponownego wykorzystywania niektórych kategorii danych chronionych będących w posiadaniu organów sektora publicznego (art. 5):**
 - Obawiamy się, że pozostawienie decyzji w sprawie warunków udostępniania danych do ponownego wykorzystania każdemu organowi sektora publicznego spowoduje rozdrobnienie rynku i złożone obciążenia regulacyjne dla ponownych użytkowników danych. Uniemożliwi to realizację głównego celu Rozporządzenia. Dlatego zachęcamy do ustanowienia takich warunków na szczeblu unijnym, aby zapewnić jak największą harmonizację przepisów.
 - Ostrzegamy przed nieuzasadnionymi ograniczeniami w międzynarodowym przepływie danych, które mogą znacznie ograniczyć wybór technologii przez podmioty zajmujące się ponownym przetwarzaniem danych i ich potencjału innowacyjnego.
 - Propozycje legislacyjne upoważniają Komisję do wydawania decyzji stwierdzających odpowiedni poziom ochrony, w których określa się, że rozwiązania prawne, nadzorcze i wykonawcze państwa trzeciego "zapewniają ochronę własności intelektualnej i tajemnic handlowych w sposób zasadniczo równoważny z ochroną zapewnioną przez prawo Unii". Na podstawie doświadczeń związanych z RODO, dostępność takich decyzji jest bardzo ograniczona (na przykład ze względu na ograniczone zasoby). W związku z tym zachęcamy do ustanowienia jasnych i praktycznych ścieżek dla ponownych użytkowników danych w celu legalnego ich przekazywania w przypadku braku decyzji o odpowiedniej ochronie, takich jak Standardowe Klauzule Umowne, zatwierdzone Kodeksy Postępowania itp. z zastosowaniem podejścia

opartego na ryzyku przy uwzględnieniu wrażliwości danych.

- Zgodnie z projektem organy sektora publicznego mogą nałożyć obowiązek dostępu do danych i ich ponownego wykorzystania w bezpiecznym środowisku przetwarzania **dostarczanym** i kontrolowanym przez sektor publiczny. Niweluje to możliwość korzystania z wysoce bezpiecznych środowisk oferowanych przez sektor prywatny, takich jak środowiska chmur obliczeniowych. W związku z tym, w dalszych pracach zachęcamy do skupienia się na kontroli dostępu do danych i ich bezpieczeństwie, a nie na ich własności lub na dostawcach podstawowej infrastruktury. Uważamy, że bezpieczeństwo publicznych chmur obliczeniowych może być bardziej solidne, skalowalne i efektywne kosztowo niż rozwiązania rządowe. Potwierdzają to niezależne badania, w tym ocena ryzyka związanego z przetwarzaniem danych w chmurach obliczeniowych, przeprowadzona przez Agencję Bezpieczeństwa Cyberprzestrzeni (ENISA) Unii Europejskiej. Należy zatem skreślić słowo "dostarczane", ponieważ wydaje się, że usługi w chmurze nie mogą być wykorzystywane do takiego "bezpiecznego środowiska przetwarzania".
- Art. 5 (5) zdanie 2 zawiera problematyczną regułę, która powinna zostać usunięta. Uprawnia organ sektora publicznego do weryfikacji wszelkich wyników przetwarzania danych, podjętych przez podmiot ponownie wykorzystujący dane oraz zastrzega sobie prawo do zakazania wykorzystywania wyników zawierających informacje zagrażające prawom i interesom osób trzecich. Jest to „Miecz Damoklesa” wiszący nad każdym podmiotem ponownie wykorzystującym dane. Możliwość interwencji jest zbyt szeroka, gdy odnosi się jedynie do praw i interesów osób trzecich bez dalszych zabezpieczeń.

Z poważaniem,

A handwritten signature in black ink, appearing to read 'W. Schmidt', with a stylized flourish at the end.

Włodzimierz Schmidt
Prezes Zarządu