Warszawa, dn. 1 lutego 2017 r.

Generalny Inspektor Ochrony Danych Osobowych
dr Edyta Bielak-Jomaa
ul. Stawki 2
00-001 Warszawa

STANOWISKO
ZWIĄZKU PRACODAWCÓW BRANŻY INTERNETOWEJ INTERACTIVE ADVERTISING BUREAU POLSKA (IAB POLSKA) W SPRAWIE WYTYCZNYCH DOT. PRAWA DO PRZENOSZENIA DANYCH (W RAMACH KONSULTACJI W TOKU PRAC NAD WDROŻENIEM ORODO).

Szanowna Pani Inspektor,

w związku z zaproszeniem GIODO z dn. 20 stycznia 2017 r. wystosowanym w trybie konsultacji w ramach prac nad wdrożeniem ogólnego rozporządzenia o ochronie danych osobowych, przedstawiam stanowisko IAB POLSKA w tym zakresie.

I. Uwaga wstępna

Art. 20 RODO odnosi się do prawa do przenoszenia danych „**dostarczonych**" administratorowi przez osobę, której dane te dotyczą. W naszej ocenie „**dostarczenie**" czegoś wymaga świadomej aktywności użytkownika. Brak jest uzasadnienia dla uznania, że dane „dostarczone" obejmują wszelkie dane jakie są generowane (niejako w tle) w wyniku działalności użytkownika. Podejście proponowane postanowieniem:

"The terms »provided by« includes personal data that relate to the data subject activity or result from the observation of an individual's behavior but not subsequent analysis of that behavior. By contrast, any personal data which have been generated by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability".

stworzy problem natury interpretacyjnej i niepewność prawną. W praktyce trudno jest bowiem postawić wyraźną granicę pomiędzy danymi powstałymi w wyniku obserwacji zachowań użytkownika, a danymi powstałymi w wyniku analizy takich zachowań.

II. Uwagi natury biznesowej i prawnej

1. Skoro przy przenoszeniu danych konieczne jest zapewnienie przez przedsiębiorcę **interoperacyjności formatu**, celem uniknięcia reklamacji klientów i nadmiernych kosztów po stronie przedsiębiorców, wskazane byłoby uzgodnienie zestandaryzowanego formatu/formatów.

2. **Należy doprecyzować na jakim etapie i w jakiej formie miałby być realizowany obowiązek informacyjny rekomendowany przez Grupę Roboczą art. 29**, a dotyczący przekazania informacji o prawie klienta do przenoszenia danych zawsze przed zamknięciem konta/zakończeniem świadczenia usług.

3. **Zdefiniowanie danych generowanych przez działania użytkownika podczas korzystania z usługi jako dane, które podlegają obowiązkowi przeniesienia, powoduje negatywne dla przedsiębiorców implikacje biznesowe**. I tak np. na potrzeby stworzenia dobrze działającego systemu rekomendacji, dostawcy zbierają i analizują dane dot. treści VOD, które użytkownik ogląda, częstotliwości ich oglądania (w tym w jakich godzinach, jak długo, etc.). Są to dane, które mają dla przedsiębiorcy konkretną wartość handlową przekładającą się na możliwość kreowania ofert dopasowanych do oczekiwań klientów i budowania satysfakcji klienta ze świadczonych mu usług. Przedsiębiorca ponosi konkretne koszty, aby dane takie zebrać, niezależnie od kosztów ich dalszej analizy. Powstaje pytanie, czy da się w ogóle rozdzielić dane zebrane do profilowania od ich „oceny/analizy", jako że takie dane są często zbierane na potrzeby świadczenia konkretnych usług w konkretnym serwisie. **Przeniesienie takich danych do innego przedsiębiorcy skutkuje ujawnieniem w pewnym sensie *know-how* poprzedniego dostawcy** (jakie dane zbiera/ pod jakim kątem) i dodatkowo powoduje, że nowy podmiot być może nie będzie już musiał profilować tego klienta u siebie, gdyż „dostanie go już sprofilowanego" np. jako „lubiącego komedie w piątki wieczorem". **W rezultacie, przeniesienie takich danych do innego przedsiębiorcy na żądanie**

użytkownika stanowiłoby istotne naruszenie tajemnicy handlowej przedsiębiorstwa i zasad konkurencji.

4. Interpretacja Grupy Roboczej art. 29 **uznająca za dane** dostarczone przez podmiot dane, w tym także meta dane, tzw. *raw data* oraz wszystkie dane wygenerowane przez aktywność użytkownika (search data, history of service, traffic data, location data), w tym dane dotyczące korzystania z usług administratora danych, które są danymi eksploatacyjnymi, opartymi najczęściej o logi systemowe, statystyki – **jest interpretacją zbyt rozszerzającą**, przez co sprzeczną z motywem (68) ORODO. W konsekwencji, stosowanie takiej wykładni może powodować znaczne utrudnienia w wykonaniu prawa do przeniesienia danych po stronie użytkownika (podmiotu danych).

5. Tak szerokie ujęcie „danych osobowych" i rozszerzenie ich na metadane/cookies i tym podobne informacje o charakterze w zasadzie bardziej technicznym niż osobowym, jest bardzo daleko idącym i bardzo trudnym do zrealizowania ograniczeniem dla dostawców usług telekomunikacyjnych i dostawców usług w Internecie, gdyż prowadzi de facto do realizacji kopiowania i udostępniania baz danych zbieranych/tworzonych przez użytkownika. **Przeciętny konsument, który zażąda przeniesienia wszystkich swoich danych, nie zdaje sobie sprawy z istnienia pewnych danych na jego temat w systemach dostawcy, w tym o danych objętych tajemnicą telekomunikacyjną.** Zrealizowanie wytycznych wskazanych w niniejszym dokumencie Grupy Roboczej art. 29 oznacza w praktyce istotne zagrożenie dla tajemnicy telekomunikacyjnej, a to wszystko „w imię" źle pojętej wygody użytkownika w zakresie zapewnienie przenoszenia treści, np. na portalach społecznościowych. Podkreślić jednocześnie należy, iż administrator co do zasady **nie przetwarza danych jako administrator**, a w niektórych usługach jedynie jako processor, hostingodawca.

6. Podane powyżej przykłady obejmują dane nie tylko eksploatacyjne ale także statystyki, które **mogą być objęte nie tylko tajemnicę telekomunikacyjną, ale również tajemnicą przedsiębiorstwa administratora danych osobowych**, jak na przykład bieżące playlisty wskazujące jakich utworów użytkownik najczęściej słuchał, czy które filmy z platformy VOD oglądał. Tak szeroki zakres danych ujawnia firmom konkurencyjnym zakres świadczonej na rzecz danego podmiotu usługi a także (ze względu na łatwość przeliczenia pojedynczych streamingów według dostępnych publicznie cenników) pozwala na dokładne obliczenie przychodów danego konkurenta z określonej usługi.

7. **Wydaje się, że spseudonimizowane dane zgromadzone dzięki plikom cookies nadane przez stronę trzecią powinny być objęte wyłączeniem opisanym w art. 11 ust. 1 RODO**. Cel ich przetwarzania nie zmierza bowiem do identyfikacji użytkowników Internetu, a identyfikacja oparta o art. 11 ust. 2 zawsze niesie wątpliwości co do tożsamości rzeczywistego użytkownika urządzenia. Rozszerzenie prawa do przenoszenia danych na dane zawarte w cookies stron trzecich niesie ponadto wątpliwości co do podmiotu, który powinien zrealizować obowiązek administratora danych polegający na udostepnieniu danych: jeśli mieliby to być dostawcy usług, z których to stron czy aplikacji użytkownik korzysta, to powstaje wątpliwość, którym innym dostawcom i jakie dane mieliby oni dostarczyć; jeśli zaś ów obowiązek powinny wykonać strony trzecie, to powstają poważne trudności natury technicznej, a ponadto – jak wcześniej wskazano – przeniesienie takich danych do innego przedsiębiorcy na żądanie użytkownika stanowiłoby istotne naruszenie tajemnicy handlowej przedsiębiorstwa i zasad konkurencji.

8. W opinii IAB Polska, zasadnym jest przyjęcie założenia, że dane takie, jako przetwarzane dla celów prywatnych podmiotu danych, powinny być do nowej usługi skopiowane i przeniesione **przez użytkownika samodzielnie**.

9. Na marginesie należy również podkreślić, że najczęściej **dostawca poczty elektronicznej w ogóle nie przetwarza danych** takich jak: kontakty, książka adresowa, korespondencja e-mail, w tym dane osobowe osób trzecich, lecz jedynie je hostuje na rzecz użytkownika. Nie są to również dane wygenerowane w trakcie korzystania z poczty, gdyż dane w postaci adresów innych osób użytkownik samodzielnie utrwala w narzędziach, a administrator jedynie hostuje je w swoim systemie. Wobec powyższego dane te nie powinny być włączane do pojęcia danych osobowych dostarczonych administratorowi do przetwarzania.

10. IAB Polska wskazuje, że jeszcze więcej wątpliwości budzi przykład wskazujący na obsługę płatności, zakupów i innych danych z wykorzystaniem kart lojalnościowych podmiotu danych, a to ze względu na **powszechność faktu, iż programy lojalnościowe z opcją zakupów online obsługują rożne typy podmiotów, każdy w zupełnie innym zakresie przetwarzania danych osobowych** (np. odrębnie podmiot udostępniający platformę online, odrębnie sklepy, odrębnie operator samych płatności). Podmioty te nie

mają wzajemnie dostępu do danych statystycznych swoich usług, w szczególności operatorzy płatności nie mają podstaw do udostępniania danych z kart płatniczych. Dane o transakcjach i ich wartościach mogą przy tym stanowić tajemnicę przedsiębiorstwa.

11. Dodatkowo, wbrew założeniom ORODO, wytyczna, aby stosować narzędzia API do transmisji i odbioru danych umożliwiające interoperacyjność i *re-use* takich danych, prowadzi do konieczności uspójnienia narzędzi i formatów przez administratorów danych, co **nie zawsze będzie możliwe technicznie oraz generuje znaczące koszty takich operacji**. API, w zakresie serwisów społecznościowych czy poczty, przy zastosowaniu wytycznych o przenaszalności danych hostowanych (a nie przetwarzanych przez administratora na podstawie zgody lub w wykonaniu umowy z użytkownikiem, udostępnionych temu administratorowi), prowadzi do konieczności dopasowania technologii i jej zmian tak aby zapewnić *re-use* danych podmiotowi danych u nowego administratora.

12. W tym kontekście pojawia się również wątpliwość czy **dane „wygenerowane" miałyby być transmitowane tylko na wyraźny wniosek użytkownika**? Należy zauważyć, iż podmiot danych może nie być zainteresowany przenaszalnością bazy danych. Chcąc przenieść pocztę elektroniczną lub profil społecznościowy do innego dostawcy usługi (nowy ADO) – może zakładać przeniesienie jedynie samego konta użytkownika, które spełnia dokładnie definicje z art. 20 ORODO, tj. dane przekazane ADO na podstawie zgody lub do wykonania umowy oraz przetwarzane przez ADO.

13. Nie jest również wiadome jaki jest cel przeniesienia danych wygenerowanych oraz hostowanych wraz z danymi udostępnionymi przez podmiot danych (zakres wynikający wprost z art. 20 i motywu 68 ORODO), jeśli nowy administrator nie powinien tych danych przetwarzać? Dodatkowo, pojawia się również szereg **pytań dotyczących przechowywania danych**, mianowicie kto powinien tworzyć i obsługiwać strefy bezpieczeństwa, w których dane mają się znaleźć przed ich odbiorem przez nowego ADO? Czy taka strefa ma być zaszyfrowana w API, czy może w sieci lub na serwerze podmiotu trzeciego? Jaka jest podstawa prawna tych działań?

14. Należy również wskazać, że z uwagi na brak możliwości technicznej kontrolowania przez użytkownika transmisji danych przez API, **nie jest możliwe zrealizowanie wytycznej**

wskazującej, iż przenoszone dane przed pobraniem ich przez nowego administratora mają być pod kontrolą wnioskującego użytkownika.

III. Poniżej przedstawione zostały inne przykłady problemów i wątpliwości, jakie rodzić będą zalecenia zawarte w dokumencie Grupy Roboczej art. 29

1. W sytuacji, gdy klient zwraca się do dostawcy usług z żądaniem (czy to ma być na wniosek?), żeby dostawca przeniósł jego dane do innego podmiotu (nawet z innej branży)
   (a) Czy dostawca ma na ten wniosek zebrać wszelkie dane jakie użytkownik „dostarczył" mu w tym szerokim rozumieniu w trakcie umowy tj. faktyczne dane osobowe (np. imię, PESEL), dane z reklamacji (np. o chorobie, zmianie adresu), płatnościach (np. numer konta/karty płatniczej); wygenerował przy korzystaniu z usług (p. bilingi), ale też własne oceny/profilowanie tego klienta pod kątem ofert/ oceny wiarygodności płatniczej, czy ma przekazać informacje o jego usługach (np. jakie VOD kupował i kiedy), treści wyrażonych zgód, a nawet odpowiedziach klienta na podejmowane działania marketingowe, nagrania wszystkich rozmów z tym klientem i po prostu przekazać np. do jakiejś innej (być może nieznanej dostawcy) firmy?
   (b) Czy dostawca ma badać wiarygodność podmiotu biorcy (skoro administrator ma obowiązek dbać o dane) i może odmówić przekazania danych, jeśli podmiot biorca nie jest wiarygodny? Czy jest uprawiony do ujawnienia mu tajemnicy telekomunikacyjnej? Czy podmiot który otrzyma dane objęte tajemnicą (a np. nie jest operatorem telekomunikacyjnym., np. bank) ma prawo przetwarzać takie dane tylko dlatego, że klient tego żąda?
   (c) Jeśli administrator danych osobowych będzie pobierał dodatkowe dane na podstawie art. 11 ust. 2 RODO przy okazji przetwarzania danych dla celów niewymagających identyfikacji, to jaki zakres danych powinien uznać za wystarczający, aby zachować zasadę adekwatności, a jednocześnie wykluczyć możliwość naruszenia art. 20 ust. 4 mówiącego o zapobieganiu niekorzystnemu wpływowi na prawa i wolności innych osób?
   (d) Czy dostawca ma pytać jaki zakres danych klient chce przekazać i wskazywać klientowi dokładnie jakie dane i w jakiej formie posiada?
   (e) Czy klient powinien wyrazić zgodę na przetwarzanie tych danych przez podmiot biorcy?

(f) Komu/czemu ma służyć przekazanie między przedsiębiorcami informacji o kliencie np. Jan Kowalski, PESEL xyz ? Czy podmiot, który otrzymał dane,powinien badać ich prawidłowość, kompletność, aktualność?

(g) Czy podmiot biorca danych wskazany przez klienta ma prawo odmówić przyjęcia tych danych lub jakiegoś ich zakresu, wiedząc że ich przetwarzanie nie jest niezbędne do realizacji umowy na daną usługę lub że nie miałby podstaw prawnych do ich przetwarzania?

2. Należy również wskazać, że przenaszalność danych rozszerzona według interpretacji Grupy Roboczej art. 29 w zakresie poczty webmail na książki adresowe, kontakty, a także całość korespondencji, nie tylko powoduje problemy po stronie administratora danych transmitującego taki zbiór danych (czyli w praktyce kopię bazy danych przechowywanych na rzecz podmiotu danych, który tych danych nie przetwarza), ale także generuje **dodatkowe ryzyka**:

   (a) odbierający takie dane nowy administrator ma (zgodnie z wytycznymi) nie przetwarzać takich danych lub włączyć je jako zbiór danych do usługi dla podmiotu tych danych, co **oznacza obowiązek przetwarzania takiego zbioru danych przez nowego administratora,** co najmniej w celu stwierdzenia, których danych nie powinien importować do nowej usługi. Powstaje zatem pytanie o podstawę prawną takiego przetwarzania, ze szczególnym uwzględnieniem, iż zbiór danych zawiera dane podmiotów trzecich, które nie wyraziły zgody ani też nie wiedzą o transmisji ich danych.

   (b) powstaje również pytanie, czy nowy administrator (który dokona pobrania takich danych jako zbioru) **ma obowiązek informowania podmiotów trzecich o przetwarzaniu ich danych** pochodzących od użytkownika? Czy też, skoro ich nie przetwarza, dane te nie powinny być przedmiotem realizowanego prawa do przenaszalności danych?

Z poważaniem,

Włodzimierz Schmidt
Prezes Zarządu