Konsultacje Komisji - Całościowe podejście do kwestii ochrony danych osobowych w UE

Wstęp

Niniejszy dokument zawiera odpowiedź Związku Pracodawców Branży Internetowej Interactive Advertising Bureau Polska na Konsultację w sprawie całościowego podejścia Komisji Europejskiej do kwestii ochrony danych osobowych w Unii Europejskiej.

IAB Polska uznaje, że aktualne pozostają podstawowe cele Dyrektywy 95/46, tj. ochrona wolności i praw podstawowych osób fizycznych, w tym ich prawa do prywatności w zakresie przetwarzania danych osobowych oraz zapewnienie swobodnego przepływu danych osobowych między Państwami Członkowskimi. Cele te powinny zawsze być brane pod uwagę przy przygotowywaniu całościowego podejścia do kwestii ochrony danych osobowych, którego dotyczy konsultacja będąca przedmiotem niniejszego dokumentu.

Kluczowe dla proponowanego całościowego podejścia do ochrony danych osobowych w Unii Europejskiej powinno być **zrównoważenie ram ochrony danych osobowych z podstawowym prawem do informacji i swobodą przepływu informacji**. W dobie społeczeństwa informacyjnego oraz gospodarki opartej o wiedzę, przepływ informacji stał się powszechną praktyką, która wzmacnia i wpływa na dalszy rozwój społeczno-ekonomiczny. W tych warunkach istotne jest zapewnienie skutecznych mechanizmów ochrony gromadzonych informacji o charakterze danych osobowych. Jednocześnie, w naszej ocenie, Unia Europejska powinna zwrócić uwagę na **zapewnienie równowagi pomiędzy wartością, jaką stanowi ochrona danych osobowych a potrzebami rozwoju Rynku Wewnętrznego Unii Europejskiej i jego konkurencyjności**.

Uwagi szczegółowe

Ad. 1.

Popieramy dążenie Komisji do poprawienia regulacji dotyczących ochrony danych osobowych w sposób zgodny z potrzebami rozwoju Rynku Wewnętrznego. Podniesienie poziomu harmonizacji ustawodawstwa Państw Członkowskich w tym zakresie ma szansę podnieść poziom pewności prawa, zmniejszyć obciążenia administracyjne i wyrównać szanse pomiędzy podmiotami przetwarzającymi dane osobowe.

Podkreślenia wymaga w szczególności konieczność usprawnień w zakresie **międzynarodowych transferów danych osobowych**. Zasady Unii Europejskiej dotyczące międzynarodowych transferów danych nie przystają do nowoczesnego obrotu. Koncentrują się na gromadzeniu i przetwarzaniu danych osobowych w ścisłym odniesieniu

do lokalizacji. Takie podejście jest szczególnie niedostosowane do usług typu *cloud computing*, co jest szkodliwe zwłaszcza dla europejskich przedsiębiorstw, którym zależy na wykorzystaniu szans biznesowych związanych z tymi usługami. Modernizacja obowiązujących ram prawnych stanowi okazję do wypracowania bardziej dostosowanych i elastycznych mechanizmów, bez zmniejszania potencjału innowacyjnego, szans wzrostu zatrudnienia i rozwoju Rynku Wewnętrznego.

Ponadto, w ocenie IAB Polska, funkcjonujący obecnie model w zakresie międzynarodowych transferów danych osobowych i część z przyjętych w jego ramach instytucji nie sprawdza się w praktyce. Dotyczy to w szczególności: uprawnień Komisji do stwierdzenia adekwatności prawa państwa trzecich (z których Komisja korzysta zbyt rzadko); odmiennego rozumienia w państwach członkowskich samego pojęcia „adekwatności" (np. w regulacji polskiej mowa jest o gwarancjach ochrony „przynajmniej takich, jakie obowiązują na terytorium RP", co w konsekwencji prowadzić może do eksterytorialności stosowania prawa krajowego/unijnego); przekonania, że zaangażowanie organów nadzorczych w proces autoryzacji transferów danych, pozwoli zapewnić im kontrolę nad występującymi obecnie masowo operacjami takiego transferu; a także m.in. zbyt wąsko zdefiniowanych w art. 26 Dyrektywy 95/46/WE wyjątków, które w poszczególnych państwach członkowskich rozumiane i stosowane są odmiennie (tytułem przykładu: polska ustawa wymaga formy pisemnej dla zgody osoby zainteresowanej na przekazanie jej danych osobowych do państwa trzeciego).

W naszej ocenie, odpowiedzialność za zapewnienie właściwego poziomu ochrony danych osobowych powinna spoczywać na administratorze (tj. eksporterze) danych, bez względu na to czy przetwarza on dane na terytorium państwa macierzystego, w obrębie UE/EOG, czy też w państwie trzecim. Jeśli eksporter stosuje zatwierdzone mechanizmy eksportu danych osobowych (np. modelowe klauzule umowne lub Wiążące Reguły Korporacyjne, które to instrumenty z pewnością wymagają dalszego udoskonalania na szczeblu unijnym), to nie powinny być na niego nakładane dodatkowe wymogi lokalne, takie jak zezwolenie czy notyfikacja władz.

Stoimy również na stanowisku, że niezwykle istotnym elementem wzmocnienia perspektywy Rynku Wewnętrznego w odniesieniu do danych osobowych jest ochrona przed nieadekwatną odpowiedzialnością tych dostawców usług internetowych, którzy przetwarzając dane osobowe działają jako pośrednicy (np. platformy hostingowe). **Odpowiedzialność pośredników powinna być ograniczona**, zgodnie z obowiązującymi zasadami wyrażonymi w regulacjach europejskich w dziedzinach takich jak prawo autorskie. Odpowiedzialność pośredników jest istotna wtedy, kiedy podmiot danych lub osoba trzecia określa środki za pomocą których przetwarzane będą dane osobowe przez dostawcę usług. Aktualne prawo ochrony danych osobowych nie zna koncepcji pośrednika, opierając się wyłącznie na zestawie praw i obowiązków podmiotów, których dotyczą dane,

administratorów danych (którzy określają cele i środki przetwarzania danych) oraz przetwarzających dane (którzy dokonują przetwarzania danych w imieniu administratora danych). Podział ten, w realiach współczesnej gospodarki, nie odzwierciedla w pełni skomplikowanych relacji, jakie zachodzą pomiędzy podmiotami, uczestniczącymi w procesie przetwarzania danych.

Ograniczenie odpowiedzialności pośredników ma kluczowe znaczenia dla gospodarki internetowej. Dyrektywy Unii Europejskiej dotyczące prywatności i prawa autorskiego definiują pośredników w odmienny sposób. Dodatkowo, każda z definicji podlegała dalszej ewolucji i zatraciła przejrzystość wskutek różnych interpretacji prawnych pojęcia. Obecna sytuacja prowadzi do braku pewności prawa koniecznej dla funkcjonowania platform hostingowych, hamując innowacje i wzrost gospodarczy. Dyrektywa 2000/31/WE ustanawia ograniczenie odpowiedzialności dla pośredników w przypadku spełnienia określonych przesłanek. Dyrektywa te nie stosuje się jednak wprost do zagadnień ochrony prywatności i danych osobowych.

To zagadnienie powinno zostać objęte zakresem przedmiotowym ograniczenia odpowiedzialności pośredników przewidzianego w Dyrektywie 2000/31/WE. Ponadto, przyszłe europejskie prawo ochrony danych osobowych powinno wyraźnie przesądzać, że platformy hostingowe nie są podmiotami kontrolującymi dane osobowe. W szczególności powinno zostać przeprowadzone wyraźne rozgraniczenie pomiędzy danymi osobowymi użytkowników usług on-line, w stosunku do których dostawca usług pozostaje administratorem, a danymi (w tym danymi osobowymi) umieszczonymi w ramach oferowanej usługi (na przykład: umieszczenie danych w ramach „książki telefonicznej" on-line / umieszczenie zdjęcia na portalu „randkowym", czy umieszczenie treści w ramach statusu na własnym koncie) przez użytkownika – w stosunku, do których dostawca usługi w żadnym wypadku nie pozostaje administratorem danych osobowych. Przyjęcie odmiennej koncepcji oznaczałoby, że dostawca usług on-line pozostaje administratorem danych osobowych, których rodzaju i zakresu nie jest w stanie przewidzieć.

W wielu przypadkach pośrednicy są natomiast podmiotami przetwarzającymi dane osobowe i wobec tego działają wyłącznie w imieniu administratora danych. Przyszłe prawo powinno w jasny sposób stanowić, że ostateczna odpowiedzialność za zgodność z regulacjami w zakresie ochrony danych osobowych spoczywa na podmiocie kontrolującym dane, czyli użytkowniku usługi.

W kontekście prac nad nowym ujęciem podmiotowego aspektu przetwarzania danych osobowych, niezbędne wydaje się również w naszej ocenie uregulowanie kwestii związanych z**podpowierzaniem danych osobowych do przetwarzania** (sub-processing). Milczenie w tym zakresie art. 17 Dyrektywy 95/46/WE, a jej wzorem i wielu ustawodawstw krajowych (w tym polskiego), ocenić należy jako istotną wadę obecnej regulacji. Podobnie oceniać należy

brak ujednolicenia w przepisach dyrektywy wymogów w zakresie zabezpieczenia danych osobowych, co prowadzi do powstawania znacznych różnić w tym zakresie w poszczególnych państwach członkowskich.

Ad. 2.1.1.

W naszej ocenie, **koncepcja danych osobowych** wymaga doprecyzowania. Obecne ramy tej koncepcji wyznaczone przez dychotomię “umożliwiające identyfikację”-“nieumożliwiające identyfikacji” nie są pomocne w ochronie praw osób, których dotyczą dane. W Unii Europejskiej powinna zostać wypracowana praktyczna definicja danych osobowych, oparta na racjonalnym prawdopodobieństwie identyfikacji. Definicja ta – poza zagwarantowaniem możliwie wysokiego poziomu pewności prawa (czego nie sposób odnieść w obecnym stanie prawnym do przetwarzania tego rodzaju danych jak np. numery IP) – powinna również niejako „zachęcać” podmioty przetwarzające dane osobowe, do ich anonimizacji lub co najmniej pseudonimizacji. Prowadzenie wielu działań nie wymaga bowiem przetwarzania danych w pełni „osobowych”. Regulacja kwestii związanych z anonimizacją wymaga jednak chociażby przesądzenia, czy tego rodzaju operacja (będąca sama w sobie „przetwarzaniem danych”, zgodnie z niezwykle pojemną aktualnie funkcjonującą definicją) wymaga spełnienia określonych wymogów, np. uzyskania zgody od zainteresowanych osób.

Konieczne jest również zdefiniowanie nowych kategorii danych, w szczególności kategorii danych “pośrednio umożliwiających identyfikację”. Nowe kategorie powinny zostać poddane właściwym, odpowiednio dostosowanym obowiązkom ochronnym. W szczególności w naszej ocenie konieczne jest wyraźne dookreślenie z jakiego (czyjego) punktu widzenia dokonywana ma być ocena „możliwości identyfikacji”, gdyż zdecydowanie inne „możliwości identyfikacji” ma administrator danych osobowych, osoba bliska w relacji do podmiotu, którego dane dotyczą, czy wreszcie statystyczny oceniający, dysponujący przeciętną wiedzą na temat osoby, której dane dotyczą.

Istotne wydaje się zatem uwzględnienie sytuacji gdy identyfikacja przez określony podmiot jest możliwa jedynie teoretycznie, jednakże w praktyce wymagałoby to użycia nadmiernych kosztów, czasu lub działań.

Należy także ostrożnie podchodzić do poszerzania zakresu danych ‘szczególnych’, z którymi związane byłyby dodatkowe restrykcje w zakresie ich ochrony.

Powyższe uwagi mają na celu nie tylko ułatwienie funkcjonowania podmiotów przetwarzających cudze dane, ale także uniknięcie nadmiernych utrudnień w odniesieniu do właścicieli danych, którzy chcieliby świadomie udostępnić swoje dane np. w celu skorzystania z określonej usługi lub otrzymania oczekiwanej informacji dotyczącej usługi lub produktu.

Przyszłe regulacje w zakresie ochrony danych osobowych powinny w większym zakresie chronić prawo użytkowników usług on-line do pozostania anonimowym w związku z ich**uczestniczeniem w debacie publicznej** i tym celu powinny określać ścisłe zasady udostępniania danych osobowych użytkowników. Aktualnie wydawcy serwisów internetowych otrzymują decyzje organu ochrony danych osobowych nakazujące udostępnienie danych użytkowników każdemu podmiotowi, który jedynie sygnalizuje zamiar wszczęcia postępowania przeciwko takim użytkownikom w związku z ich wypowiedziami zamieszczonymi na stronach internetowych. W naszej ocenie, taka praktyka przeczy celom regulacji w zakresie ochrony danych osobowych i prowadzi do niekontrolowanego wypływu danych dotyczących użytkowników. W sytuacji, w której każdy podmiot może skutecznie wystąpić o udostępnienie danych dowolnego użytkownika pod pretekstem wszczęcia przeciwko niemu postępowania sądowego, ochrona danych osobowych staje się pozorna, a prawo użytkowników do prywatności i tajemnicy komunikowania naruszane. Nietrudno dostrzec możliwość wykorzystania udostępnionych danych osobowych nie tylko w celu niezgodnym z tym, dla którego były udostępnione (tj. w celu wszczęcia postępowania), ale wręcz do podejmowania działań niezgodnych z prawem, co jest niepokojące zwłaszcza w aspekcie często występujących zależności pomiędzy osobami żądającymi udostępnienia danych, a osobami, których te dane dotyczą (np. pracodawca naruszający prawa pracownicze – pracownik, organ administracji samorządowej – osoba zamieszkująca na terenie gminy), i co może w konsekwencji prowadzić do nadużyć w zakresie wykorzystania uzyskanych danych.

Powyższe uwagi dotyczą również problemu decyzji nakazujących udostępnianie danych osobowych dziennikarzy na żądanie osób, których dotyczą treści zamieszczone w materiałach prasowych, pod pretekstem wszczęcia postępowania przeciwko autorom materiałów prasowych. Organ ochrony danych osobowych wydaje decyzje nakazujące wydawcom prasy udostępnianie podmiotom trzecim danych osobowych autorów publikacji prasowych, przy czym dotyczy to również adresu zamieszkania dziennikarzy. Takie decyzje mogą stwarzać realne niebezpieczeństwo dla autorów materiałów prasowych, zwłaszcza tych, którzy podejmują tematy istotne z punktu widzenia interesu społecznego. Tymczasem uzyskanie przez osobę zamierzającą wszcząć postępowanie adresu dziennikarza nie jest warunkiem skutecznego dochodzenia praw na drodze postępowania sądowego.

Dodatkowo, wyraźnej ingerencji prawodawcy unijnego wymaga jednoznaczne wyłączenie spod zakresu przedmiotowego regulacji Dyrektywy 95/46/WE kwestii przetwarzania **danych biznesowych**, tzn. danych nie dotyczących osób fizycznych, lecz podmiotów gospodarczych (biznesowych). Możliwość swobodnego przetwarzanie danych biznesowych – oczywiście przy uwzględnieniu właściwych dla tego rodzaju danych ograniczeń (np. związanych z ochroną tajemnicy przedsiębiorstwa, ochroną poufności informacji na drodze kontraktowej) – jest kluczowa w perspektywie właściwego rozwoju gospodarczego w ramach Rynku

Wewnętrznego. W tym kontekście niezbędne byłoby również precyzyjne określenie zakresu takiego wyłączenia, z uwzględnieniem różnych form prowadzenia działalności gospodarczej w państwach członkowskich. W szczególności określenia wymagałoby, czy wyłączenie to dotyczyć ma określonych jednostek organizacyjnych (spółki prawa handlowego, osoby prawne), czy również pewnych form indywidualnego prowadzenia działalności gospodarczej przez osoby fizyczne, a także czy odnosi się ono do danych osób reprezentujących ww. jednostki organizacyjne (członków władz spółek prawa handlowego, itp.), czy innych osób działających w ich imieniu (pełnomocnicy, różnego rodzaju reprezentanci, przedstawiciele itd.).

A aspekcie definicyjnym, niezbędne wydaje się również dostosowanie do zmieniających się realiów, w szczególności związanych z powszechnym korzystaniem z internetu (serwisy społecznościowe, itd.), wyłączenia, o którym mowa w art. 3 ust. 2 Dyrektywy 95/46/WE („**czynności o czysto osobistym lub domowym charakterze**"). Zróżnicowane podejście do tego zagadnienia w poszczególnych państwach członkowskich, w szczególności wyznaczanie w odmiennym miejscu granic dla tego rodzaju czynności, z pewnością nie wpływa na skuteczność stosowania prawa i wzmocnienie pewności prowadzenia działalności w sieci, nie służy też wzmocnieniu ochrony uzasadnionych interesów jednostek, których dane osobowe są przetwarzane.

Ad. 2.1.2.

W naszej ocenie, dążąc do poprawy przejrzystości, należy doprowadzić do harmonizacji, która zapewni **minimalny standard zawiadomień** o naruszeniu ochrony danych osobowych dla całej Unii Europejskiej. W sytuacji np. wycieku danych w interesie osób, których dane dotyczą jest aby całość działań skierowana została na powstrzymanie wycieku i ustalenie jego przyczyn a także zaimplementowanie działań prewencyjnych, które uniemożliwią wystąpienie podobnych zdarzeń w przyszłości. Dlatego uważamy, że nakładanie kolejnych obowiązków na administratorów w tym kontekście jest zbyteczne. Niezależnie od powyższego każda sytuacja wycieku danych jest wydarzeniem medialnym a użytkownicy których dane „wypłynęły" otrzymują więc stosowne informacje o tym fakcie niezależnie.

Zgadzamy się z opinią, że niezbędne jest zapewnienie właścicielom danych odpowiedniej informacji dotyczącej przetwarzania ich danych. Należy jednak przy tym zapewnić, aby obowiązki w tym zakresie nie wykraczały poza faktyczne potrzeby w zakresie ochrony prywatności.

Ad. 2.1.3.

Popieramy wzmocnienie kontroli nad własnymi danymi. Odnośnie do **prawa do bycia zapomnianym**, w naszej ocenie prawo to powinno zostać zdefiniowane w taki sposób, który chroni pośredników od nowych obowiązków, które są albo technicznie niemożliwe do

spełnienia, albo które rozszerzałyby odpowiedzialność pośrednika na treść stworzoną poza kontrolą pośrednika.

Warto zauważyć, że istota prawa do bycia zapomnianym jest już uregulowana w prawie europejskim w postaci ograniczeń retencji danych. Ponadto, jest ono realizowane przez możliwość przenoszenia danych, czyli możliwość opuszczenia przez podmiot danych osobowych opuszczenia danego serwisu i przeniesienia jego danych do innego serwisu. Taki mechanizm zapewnia podmiotom danych efektywną kontrolę nad ich danymi osobowymi. Podmiot danych może zadecydować, jak długo oraz gdzie chce, żeby przechowywane były jego dane. Może również zadecydować o opuszczeniu danej platformy i usunięciu z niej swoich danych. W ten sposób platformy hostingowe i inni pośrednicy zapewniają efektywny mechanizm realizujący prawo do bycia zapomnianym.

Pragniemy podkreślić, że nie byłoby właściwym sposobem zaadresowanie wszelkich wyzwań społecznych związanych z funkcjonowaniem internetu poprzez nakładanie nowych obowiązków na administratorów danych, podmioty przetwarzające dane oraz pośredników. Uważamy, że najwłaściwszym instrumentem jest tu rozwój mechanizmów kontroli użytkowników nad swoimi danymi i popieramy działania w tym zakresie.

Naszym zdaniem konieczne jest uwzględnienie poniższych kwestii:

1. uniknięcie sytuacji gdy nadmiernie restrykcyjne stosowanie „zasady minimalizacji danych” spowodowałoby w praktyce zbędne utrudnienia co do możliwości przetwarzania danych (także wtedy gdy przetwarzanie danych leżałoby w interesie ich właściciela);
2. jasnego określenia ograniczeń w przypadku „zasady minimalizacji danych”, w celu uniknięcia wątpliwości czy w określonych przypadkach dopuszczalne jest przetwarzanie danych;
3. w przypadku obowiązków w zakresie zapewnienia kontroli danych, „prawa do bycia zapomnianym” i „przenoszalności danych” – wprowadzania rozwiązań uwzględniających także realne możliwości techniczne, organizacyjne i finansowe zobowiązanych podmiotów;

Ad. 2.1.4.

Działania mające na celu pogłębianie świadomości społeczeństwa w zakresie ochrony danych osobowych leży w interesie wszystkich zainteresowanych stron. Wskazane byłoby jednak w tym wypadku przede wszystkim zachęcanie do współpracy i skorzystanie z mechanizmów samoregulacyjnych. Nie wydaje się natomiast, aby była to sfera wymagająca nakładania obowiązków w drodze kolejnych regulacji prawnych.

Ad 2.1.5.

IAB Polska popiera inicjatywę związaną z udoskonaleniem przepisów dotyczących **zgody**, w szczególności w aspekcie jej świadomości i dobrowolności. Jednocześnie pragniemy zauważyć, iż zwłaszcza w środowisku internetowym kluczowe jest, aby na obszarze UE/EOG stosowane były te same wymogi w odniesieniu do „zgody", a także aby pojęcie to było jednolicie rozumiane. Dlatego też przyjęte w tym kontekście rozwiązania na szczeblu unijnym nie powinny stwarzać pola do różnicowania pojęcia zgody w poszczególnych państwach członkowskich, jak również nie powinny dopuszczać wprowadzania w ustawodawstwach krajowych bardziej restrykcyjnych wymogów w zakresie zgody, utrudniających w istotnym zakresie działalność w internecie (np. wymóg zgody pisemnej w zakresie przetwarzania określonych kategorii danych lub dla określonych operacji na danych, nie przystający w żadnej mierze do realiów „elektronicznej" gospodarki).

Postulujemy rozszerzenie przesłanek dopuszczalności przetwarzania danych osobowych o sytuację w której przetwarzanie danych jest konieczne dla **powszechnie akceptowanych społecznie praktyk**.

Uzasadnieniem wprowadzenia opisanej przesłanki może być np. powszechnie występująca konieczność przetwarzania danych w celu realizacji zamówienia (przekazanie danych osobowych firmie kurierskiej), czy rozstrzygnięcia i przekazanie nagród w ramach prowadzonych konkursów (przekazanie danych firmie kurierskiej czy przekazanie danych osobowych do często zewnętrznego Jury), jak również ochrona użytkowników usługi przed np. wyłudzeniami.

Niezależnie zwracamy uwagę, że zmienione brzmienie Dyrektywy powinno jednoznacznie potwierdzać wartość i znaczenie zgody na przetwarzanie danych osobowych w kontekście relacji osoby, której dane dotyczą do administratora danych osobowych. Z obowiązującego prawa jednoznacznie powinna wynikać możliwość traktowania zgody na przetwarzanie danych osobowych, jako świadczenia wzajemnego za możliwość korzystania z bezpłatnych usług oferowanych przez przedsiębiorcę. Logiczną konsekwencją jest potwierdzenie możliwości zaprzestania świadczenia (braku obowiązku świadczenia) bezpłatnej usługi przez przedsiębiorcę w sytuacji nieudzielenia lub cofnięcia zgody przez użytkownika tej usługi.

Ponownie należy wskazać, że nasze stanowisko uwzględnia także interes osób których dane dotyczą – nie znajduje uzasadnienia nadmierne utrudnianie lub wręcz uniemożliwianie tym osobom udostępniania ich danych, w szczególności jeśli ma to związek z korzystaniem z zamawianych usług.

Ad. 2.1.7.

Nie uchylając się przed odpowiedzialnością w przypadku naruszenia przepisów w zakresie ochrony danych osobowych, chcielibyśmy zwrócić uwagę, że w praktyce skupienie się na nadmiernej penalizacji przynosi często mniejsze efekty niż inne działania, takie jak

stworzenie jasnych regulacji, edukacja czy zachęcanie do działań o charakterze samoregulacyjnym.

Ad. 2.2.1.

Zgadzamy się, że konieczne jest podejmowanie dalszych działań mających na celu ułatwienie swobodnego przepływu danych osobowych w obrębie rynku wewnętrznego UE. Niewątpliwie przyczyniłoby się do tego ujednolicenie regulacji we wszystkich Państwach Członkowskich.

Ad. 2.2.2.

Zmniejszenie obciążeń administracyjnych obciążających administratorów danych, w szczególności w zakresie **uproszenia aktualnego systemu notyfikacji / rejestracji**, powinno stanowić w naszej ocenie jeden z podstawowych zadań w zakresie rewizji przepisów Dyrektywy 95/46/WE. Zgodzić w pełni należy się ze stanowiskiem, iż obowiązek notyfikacyjny nie stanowi sam w sobie żadnej wartości dodanej, zasadne wydaje się zatem jego znacznie uproszczenie (bez pozostawiania swobody decyzyjnej dla poszczególnych państw członkowskich) lub nawet zniesienie, przy spełnieniu określonych obowiązków (w związku tym rozważyć można przykładowo powszechne wprowadzenie w państwach UE/EOG wyłączenia obowiązku notyfikacji w sytuacji powołania przez administratora danych urzędnika do spraw ochrony danych osobowych).

Ad 2.2.3

Wyrażamy poparcie dla stanowiska Komisji Europejskiej, pragnącej ostatecznie zapewnić unijnym osobom, których dane dotyczą ten sam stopień ochrony, niezależnie od lokalizacji geograficznej administratora danych.

Stoimy na stanowisku, że konieczne jest doprecyzowanie przepisów Dyrektywy dotyczących **prawa właściwego**. Zgadzamy się z oceną Komisji, że aktualne przepisy dotyczące prawa właściwego są pod wieloma względami wadliwe i nie dają ani użytkownikom, ani przedsiębiorcom wystarczającej pewności prawnej. W szczególności, w przypadkach, w których przetwarzanie danych przez określony podmiot odbywa się w kilku państwach członkowskich, właściwe powinno być prawo państwa członkowskiego, w którym znajduje się główna siedziba danego podmiotu. Określenia wymagają kryteria definiujące „główną siedzibę", w tym kryterium miejsca przetwarzania danych osobowych oraz miejsca, w którym podejmowane są decyzje dotyczące przetwarzania tych danych. Jasna definicja zniechęciłaby przedsiębiorców do „forum shoppingu". Zwracamy uwagę, że dla pewności prawa dla użytkowników oraz podmiotów gospodarczych konieczne jest doprowadzenie do wyższego poziomu harmonizacji w Unii Europejskiej w zakresie regulacji ochrony danych osobowych.

Bezwzględnie konieczne jest przy tym uniknięcie sytuacji, w której administratorzy danych z Państw Członkowskich są dyskryminowani ze względu na fakt, iż podlegają określonej jurysdykcji – chodzi tu o nadmiernie restrykcyjne regulacje zarówno w poszczególnych państwach UE, jak i w porównaniu z państwami spoza UE (w szczególności poprzez nałożenia nadmiernych obowiązków, które nie muszą być stosowane przez administratorów z państw trzecich). Komisja powinna rozważyć, by przy wyborze oraz implementacji środków prawnych gwarantujących obywatelom Państw Członkowskich równe standardy ochrony niezależnie od siedziby dostawcy usługi zostały wzięte pod uwagę następujące kryteria: chociażby częściowe prowadzenie działania komercyjnego lub zawodowego w relacji do obywateli któregokolwiek z krajów członkowskich (pomocniczo decydujące w tym zakresie mogłyby być: język prezentowanych treści, rozszerzenie domeny, treść kierowanych komunikatów, treść komunikatów reklamowych – zwłaszcza geolokalizowanych) lub znaczna liczba użytkowników pochodzących z Państwa Członkowskiego, korzystających z usług oferowanych przez dostawców spoza Unii Europejskiej.

Ad. 2.2.4.

Nie uchylając się od odpowiedzialności w przypadku naruszenia przepisów w zakresie ochrony danych osobowych należy zwrócić uwagę, że już na gruncie obecnie obowiązujących przepisów nie można mówić o bezkarności administratorów danych osobowych. Zatem wprowadzanie dodatkowych obowiązków obciążających administratorów danych należy rozważać mając na względzie ich adekwatność do zamierzonych celów i faktycznych potrzeb w tym zakresie.

Ad 2.2.5

Ponadto jako ważny punkt zmian w Dyrektywie wskazujemy **zwiększenie roli kodeksów dobrych praktyk** w których przedsiębiorcy samodzielnie nakładają na siebie obowiązki z jednoczesnym zapewnieniem, że obowiązki te będą respektowane.

Z uwagi bowiem na dużo szybszy rozwój technologii aniżeli prawa, nie będzie możliwe prowadzenie ciągłej rewizji Dyrektywy jako podstawowego aktu prawnego. Dlatego też postulujemy rozszerzenie rozdziału V Dyrektywy o zapisy odnośnie regulacji wewnętrznych w szczególności nadania znaczenia prawnego uchwalonym samoregulacjom (na przykład możliwość określania w samoregulacjach „powszechnie akceptowanych społecznie praktyk"). Chodzi o ustanowienie efektywnego, praktycznego i powszechnie dostępnego (podanego do publicznej wiadomości) narzędzia do elastycznego dopasowywania obowiązujących regulacji (zwłaszcza w zakresie klauzul generalnych poprzez podanie przesłanek ocennych etc.) do dynamicznie rozwijającego się rynku usług teleinformatycznych.

Kwestia **unijnego systemu certyfikacji** ochrony prywatności wymagałaby szczegółowej analizy pod kątem kosztów tego rodzaju rozwiązań, kwestii organizacyjnych, itd. Aby system

certyfikacji spełnił swoją rolę, nie może być nadmiernie czasochłonny ani wiązać się z nadmiernym kosztem dla administratorów danych. Ważne jest także ustalenie przejrzystych kryteriów jakie należy spełnić w celu uzyskania certyfikatu.

Ad 2.5

IAB Polska z zadowoleniem przyjmuje zwrócenie uwagi na rolę jaką może i powinna odegrać **Grupa Robocza Art. 29** w ramach zaktualizowanego stanu prawnego w zakresie ochrony danych osobowych. Wzmocnienie uprawnień Grupy Roboczej Art. 29, a także określenie jasnych (transparentnych) zasad w zakresie prowadzenia konsultacji z zainteresowanymi uczestnikami rynku (w niektórych przypadkach konsultacji o charakterze obligatoryjnym), przyczynić może się do zwiększenia jakości prawa (lepiej odzwierciedlających stosunki społeczne czy uwarunkowania technologiczne, co ma szczególne znaczenie dla branży internetowej), czy też wzmocnienia poziomu harmonizacji regulacji w poszczególnych państwach członkowskich.

W tym aspekcie zasadne wydaje się również zwrócenie uwagi na wzmocnienie uprawnień (ale i obowiązków) doradczych krajowych organów nadzorczych, które to uprawnienia (obowiązki) nie są aktualnie właściwie realizowane.