13.01.2014r.

LEWIATAN

Stanowisko Konfederacji Lewiatan w sprawie stanu prac nad Projektem rozporządzenia o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz o swobodnym przepływie tych danych (COM 2012/0011)

I. Wstęp

Skumulowane, analizowane i odpowiednio zestawiane dane są w dobie gospodarki cyfrowej źródłem rzetelnej i łatwo dostępnej wiedzy o zachodzących zjawiskach, procesach i tendencjach. Jej umiejętne wykorzystanie przez organy publiczne, przedsiębiorców i obywateli przyczynia się do postępu społeczno-gospodarczego oraz będzie jednym z głównych kryteriów rozstrzygających o pozycji konkurencyjnej Polski i Unii Europejskiej na świecie.

Przedsiębiorcy zrzeszeni w Konfederacji Lewiatan są świadomi, że nieumiejętne i lekkomyślne wykorzystanie danych, szczególnie danych osobowych, może rodzić negatywne skutki i naruszać prawa i wolności obywateli. We wspólnym interesie jest zminimalizowanie takich ryzyk i wyeliminowanie nadużyć.

Europa potrzebuje ram prawnych, które skutecznie zabezpieczą interesy obywateli. Jednocześnie, muszą one umożliwić wykorzystanie danych bez generowania niepotrzebnych kosztów i utrudnień w prowadzeniu działalności gospodarczej i wykonywaniu zadań publicznych. W ocenie Konfederacji Lewiatan obecny stan prac nad projektem rozporządzenia o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz o swobodnym przepływie tych danych (COM(2012) 11 final) rodzi obawę, że szansa na stworzenie przepisów odpowiadających na te wyzwania zostanie zaprzepaszczona.

Po blisko dwóch latach prac nad rozporządzeniem, Parlament Europejski i Rada Unii Europejskiej, zaprezentowały swoje spojrzenie na kształt unijnych ram prawnych dotyczących ochrony danych[1]. Konfederacja Lewiatan popiera oparte o logikę *risk based approach* podejście Rady. Znajduje ono odzwierciedlenie w uzależnieniu zakresu obowiązków informacyjnych i dokumentacyjnych nałożonych na administratora danych od specyfiki przetwarzania danych oraz od ryzyka, jakie może się wiązać z ewentualnym naruszeniem bezpieczeństwa danych. Za właściwe uważamy odejście od wymogu zgody wyraźnej na przetwarzanie danych oraz zwolnienie administratora danych z obowiązku notyfikacji naruszeń bezpieczeństwa danych organowi nadzorczemu i podmiotowi danych, jeśli zastosował on środki techniczne ograniczające możliwość ich wykorzystania przez osoby nieuprawnione. Pozytywnie oceniamy zgodne z obecnym brzmieniem polskiej ustawy, ograniczenie definicji odbiorcy, jako ważną dla codziennego funkcjonowania firm zmianę.

Znaczących zmian wymaga tekst rozporządzenia zaproponowany w sprawozdaniu Parlamentu Europejskiego. Wiele jego postanowień nakłada na administratorów danych nieproporcjonalne i generujące koszty obowiązki. Paradoksalnie, przyjęte rozwiązania będą często niekorzystne również dla podmiotów danych. Za najbardziej problematyczne należy uznać przepisy dotyczące uzasadnionego interesu administratora, całokształt przepisów odnoszących się do obowiązków informacyjnych i

[1] Wyrażone odpowiednio w sprawozdaniu Komisji LIBE z dnia 21.10.2013r. oraz w raporcie Prezydencji Irlandzkiej z 18 maja 2013r., podsumowującym rezultaty prac Rady nad rozdziałami I-IV projektu.

LEWIATAN

dokumentacyjnych, obowiązek notyfikacji naruszenia wobec podmiotu danych i bezwarunkowe prawo sprzeciwu wobec przetwarzania opartego o uzasadniony interes administratora.

Mimo powyższej pozytywnej oceny, także w tekście Rady znalazły się postanowienia, które nadal uważamy za problematyczne (uprzednia konsultacja, przenoszalność danych, prawo do bycia zapomnianym). Jednocześnie, za lepsze uważamy podejście Parlamentu w odniesieniu do danych spseudonimizowanych (art. 10), do uprzedniej konsultacji (z organem nadzorczym lub inspektorem ochrony danych) oraz do możliwości nałożenia opłaty administracyjnej w razie przesadnych wniosków podmiotów danych.

Mimo, że w pełni popieramy konieczność zapewnienia ochrony najmłodszych użytkowników sieci pozytywnie oceniamy wykreślenie definicji dziecka z projektu Rady. Wprowadzenie skutecznych mechanizmów weryfikowania wieku jest w środowisku cyfrowym problematyczne i nie powinno (jak zaznaczono w sprawozdaniu PE) prowadzić do przetwarzania większej ilości danych.

Szczegółowy komentarz do tekstów obu instytucji znajdziecie Państwo poniżej. Mamy nadzieje, że w toku dalszej debaty w Radzie i w Parlamencie pomoże on wyeliminować niekorzystne dla przedsiębiorców postanowienia projektu.

II Uwagi szczegółowe[2]

Nadmierna informacja to brak informacji

Sprawozdanie Parlamentu wprowadziło nieproporcjonalnie szeroki katalog informacji, jakie przed i w trakcie pozyskiwania danych, administrator będzie zobowiązany przekazać podmiotom danych (art. 12-15). W dynamicznej praktyce obrotu konsument nie będzie w stanie ich przeczytać, szczególnie biorąc pod uwagę, że informacje o ochronie danych są tylko częścią przekazywanych mu przed zawarciem umowy treści. Co więcej, wiele z informacji, uprzednio podawanych jedynie organom nadzorczym, będzie dla podmiotów danych niezrozumiała. Zniechęci to konsumentów do zapoznania się z przekazywaną informacją i doprowadzi do jeszcze większego automatyzmu wyrażania zgód. Nie zwiększy też świadomości obywateli co do warunków przekazania danych oraz sposobu ich przetwarzania przez podmioty, którym zostały one przekazane.

W ocenie Konfederacji Lewiatan bardziej korzystny jest w tym zakresie tekst Rady, wprowadzający węższy katalog informacji, w tym informacji obowiązkowych oraz takich, które powinny być przekazane, jeśli jest to w konkretnym przypadku konieczne dla zapewnienia uczciwego i przejrzystego przetwarzania danych. Istotne jest także dopuszczenie podania **kategorii odbiorców, którym dane będą przekazywane (ust. 1a pkt c), a nie konkretnych odbiorców, którym dane będą**

[2] Poniższe stanowisko zawiera uwagi Konfederacji do stanowisk Parlamentu Europejskiego i Rady, wyrażonych odpowiednio w sprawozdania Komisji LIBE z dnia 21.10.2013r. oraz w raporcie Prezydencji Irlandzkiej z 18 maja 2013r., podsumowującym rezultaty prac Rady nad rozdziałami I-IV projektu.

LEWIATAN

przekazywane. Administrator często nie jest w stanie podać informacji o konkretnym odbiorcy na przyszłość i możliwe jest jedynie określenie kategorii podmiotów, którym dane będą udostępniane.

Pozytywnym, z punktu widzenia przedsiębiorców, rozwiązaniem wprowadzonym w sprawozdaniu PE (art. 12 ust. 4) jest **możliwość pobrania przez administratora rozsądnej opłaty**, w wysokości uzasadnionej kosztami obsługi wniosków podmiotów danych, w razie ich przesadnego charakteru. Wątpliwości budzi jednak to, że ustęp 4 odsyła do praw wymienionych w ust. 1, z którego zdanie dotyczące artykułów zostało wykreślone. O ile zrozumiałe jest, że realizacja prawa dostępu do danych, prawa do ich poprawienia i sprzeciwu powinna być wolna od opłat (z zastrzeżeniem jak wyżej w razie przesadnego charakteru), **należy sprzeciwić się zakazowi pobierania opłat za realizację prawa do przenoszenia danych**. Konsekwentnie podkreślamy, że prawo do przenoszenia danych jest usługą, nie należącą do przepisów o ochronie danych osobowych, a nie prawem podmiotu danych.

Ikony informacyjne (Standardized information policies)

Sprawozdanie LIBE nakłada na administratora danych obowiązki informacyjne, które powinny być spełnione, jeszcze przed rozpoczęciem przetwarzania, przy wykorzystaniu systemu ikon. Zdaniem Konfederacji Lewiatan przekazanie tych informacji w formie graficznej powinno mieć **charakter fakultatywny**. Zastosowanie ikon będzie niemożliwe lub nieefektywne przy wykorzystaniu niektórych środków komunikacji z podmiotem danych. System ikon może okazać się użyteczny w Internecie albo w kanałach charakteryzujących się ograniczonym miejscem na przekazanie treści informacyjnych (np. aplikacje mobilne). Będzie jednak stwarzał problem w przypadku kontaktu telefonicznego z podmiotem danych. Już obecnie konsumenci bywają poirytowani koniecznością wysłuchania długich informacji przed połączeniem z konsultantem.

Dodatkowym problemem jest to, że system ikon w wersji zaproponowanej przez Parlament rozszerza i tak już obszerny katalog informacji. Ich przekazanie, ze względów wskazanych poniżej, często będzie nieuzasadnione. **Ewentualne zastosowanie systemu ikon powinno być formą realizacji obowiązku informacyjnego** nałożonego na administratora w art. 14 projektu LIBE. Postulujemy, aby zgrać załącznik numer 1 z treścią przepisu art. 14 tak, aby umieszczenie ikon było (alternatywną) formą spełnienia obowiązku informacyjnego, a nie jego rozszerzeniem. Obecna propozycja systemu ikon Komisji LIBE budzi następujące zastrzeżenia:

- Dwie pierwsze ikony ("No personal data are collected beyond the minimum necessary for each specific purpose of the processing" i "No personal data are retained beyond the minimum necessary for each specific purpose of the processing") nakazują przekazanie podmiotowi danych informacji, że dane przetwarzane są zgodnie z artykułem 5 projektu rozporządzenia. Wartość tej informacji jest dla podmiotu danych niewielka, bo każdy administrator jest zobowiązany przetwarzać dane zgodnie z tymi zasadami. Ponadto, podmiot danych nie będzie w stanie zweryfikować tych deklaracji. Nawet jeśli administrator danych, niezgodnie z artykułem 5, zbierałby więcej danych niż jest to konieczne do osiągnięcia danego celu, trudno sobie wyobrazić, że otwarcie się do tego przyzna.

- Ikony 3-6 odnoszą się do przetwarzania danych, które przy spełnieniu określonych w rozporządzeniu warunków, są zgodne z przepisami projektu. System ikon nie pozwala na wykazanie, że administrator spełnia te warunki. Taki uproszczony przekaz może w rezultacie stworzyć u podmiotów danych mylne

LEWIATAN

wrażenie, że zachowanie administratora danych, sprzeczne z informacją zawartą w systemie ikon, jest działaniem bezprawnym. Mogłyby to podważyć zaufanie konsumentów do legalnie działających firm i zniechęcać do skorzystania z ich usług.

Przykładowo, udostępnianie danych komercyjnym stronom trzecim np. podmiotom z tej samej grupy kapitałowej na podstawie jednej z przesłanek art. 6, jest legalne i często zgodne z interesem podmiotu danych i administratora. Można się jednak spodziewać, że informacja o przekazywaniu danych stronom trzecim przedstawiona w formie zaproponowanej przez LIBE wywoła przeciwne wrażenie u podmiotu danych.

Z tych względów, jeśli system ikon zostałby wprowadzony **przedsiębiorca powinien mieć możliwość prezentowania jedynie wybranych ikon**, które ze względu na specyfikę prowadzonej działalności i możliwe do przewidzenia sytuacje, administrator jest w stanie spełnić. Byłby to rodzaj zapewnienia, wobec podmiotu danych, że nie będzie wykonywał określonych kategorii przetwarzania.

Ocena skutków przetwarzania, analiza ryzyka, rewizja zgodności z przepisami

Sprawozdanie Parlamentu wprowadza szereg przepisów, które formalizują tryb kontrolowania zgodności przetwarzania z przepisami przez administratora danych. Chodzi tu m.in. o weryfikację poprzedzającą przetwarzanie, o ocenę związanego z tym ryzyka oraz o działania monitorujące zgodność. Relacja między analizą ryzyka (32a) i oceną wpływu przetwarzania (33) nie jest jasna, a przeprowadzenie obu analiz będzie dublowaniem tych samych działań i dokumentacji. Wpływ obu procedur na bezpieczeństwo przetwarzania i ochronę danych osobowych jest wątpliwy, a zwiększy obowiązki firm i związane z tym koszty. **Postulujemy wykreślenie artykułów 32a i 33a.**

Brak elastyczności i koszty

Postanowienia sprawozdania Parlamentu są zbyt preskryptywne. Nie pozostawiają administratorowi możliwości dostosowania standardów przetwarzania (ilości informacji przekazywanych podmiotowi danych, procedur przetwarzania i ich dokumentowania, środków przeznaczonych na zapewnienie zgodności, w tym decyzja o zatrudnieniu ABI) do skali i specyfiki przetwarzania danych. Narzucają one, mający zastosowanie do wszystkich podmiotów, szablon, pomijając ich zaawansowanie technologiczne, skalę i charakter przetwarzania danych.

Jest to widoczne zwłaszcza w:

- wymogu przygotowania obszernej dokumentacji (polityki przetwarzania danych, dokumentacja realizacji obowiązków wynikających z postanowień rozporządzenia, dokumentacja analizy ryzyka, oceny skutków przetwarzania)
- szerokim (i otwartym) katalogu informacji przekazywanych podmiotowi danych
- wymogu powołania ABI w przypadku przetwarzania danych więcej niż 5 000 osób w skali roku (jest to niewiele w przypadku zbierania danych na stronie internetowej, np. na potrzeby wysyłania newslettera). Obowiązek ten obejmie też każdy podmiot, który chcąc reklamować swoje produkty i

LEWIATAN

usługi kupi (legalnie zbudowaną) bazę danych, która będzie zawierać dane więcej niż 5000 osób (kupowanie mniejszej bazy jest praktyce nieopłacalne).
- zakresie informacji notyfikowanych w razie naruszenia bezpieczeństwa,
- wymogu przeprowadzenia i aktualizowania oceny ryzyka oraz przeglądów zgodności przetwarzania,
- określeniu obowiązkowych postanowień (nawet najprostszej) umowy powierzenia danych.

Wszystkie te obowiązki spowodują, że nawet najmniejsze podmioty przetwarzające dane będą zmuszone do skorzystania z profesjonalnej obsługi prawnej lub podmiotów świadczących usługi dotyczące obsługi procesu przetwarzania danych osobowych. Biorąc pod uwagę niewielką liczbę dostępnych w Polsce osób lub podmiotów posiadających wiedzę w tym zakresie, może to spowodować sytuację, w której koszty usług w zakresie obsługi procesu przetwarzania danych bardzo istotnie wzrosną, a podmioty świadczące takie usługi będą przedsiębiorcom dyktować warunki finansowe – przynajmniej w początkowym okresie obowiązywania Rozporządzenia. Tak czy inaczej, zwiększy to koszty rozpoczynania i prowadzenia działalności gospodarczej i utrudni funkcjonowanie firm.

Uzasadniony interes administratora

Bardzo niebezpieczne dla prowadzenia działalności gospodarczej jest zagwarantowanie podmiotowi danych prawa bezwarunkowego sprzeciwu w sytuacji, gdy podstawą przetwarzania jest uzasadniony interes administratora (art. 19 ust 2 LIBE). Przepis nie przewiduje możliwości oceny czy realizowany przez administratora uzasadniony interes nie przeważa nad interesem podmiotu danych. Takie ujęcie zagraża możliwości dochodzenia roszczeń, zapobiegania nadużyciom finansowym, zapewnienia bezpieczeństwa w miejscu pracy i ochrony wielu innych słusznych interesów administratora.

Krytycznie oceniamy też ograniczenie możliwości przetwarzania danych w oparciu o uzasadniony interes administratora tylko, jeśli będzie to zgodne z „rozsądnymi oczekiwaniami" podmiotu danych. Administrator danych nie może przewidzieć, jakiego rodzaju przetwarzania spodziewa się podmiot danych. Ponadto, jak zaznaczono powyżej, nawet jeśli przetwarzanie w konkretnym celu wykraczałoby poza oczekiwania podmiotu danych, może ono być w pełni uzasadnione.

Zgoda

W kontekście zgody zwracamy uwagę na ostatnie zdanie art. 7 ustęp 4 (LIBE), zakazującego uzależniania świadczenia usługi od zgody na przetwarzanie większej ilości danych, niż to konieczne do wykonania umowy. Naszym zdaniem taki zakaz zamknie podmiotom danych dostęp do bezpłatnych usług, takich jak skrzynka mailowa, portale społecznościowe, serwisy prasowe, muzyczne itp. Usługi te funkcjonują w modelu biznesowym opartym o finansowanie pochodzące od reklamodawców. Aby przestrzeń reklamowa dostępna na stronach tych serwisów była dla nich atrakcyjna, konieczne jest przetwarzanie pewnych (spseudonimizowanych) danych użytkowników. Jeśli dostawca treści nie będzie mógł sfinansować swojej działalności środkami uzyskiwanymi (w zamian za dane o użytkownikach) od innych przedsiębiorców, taki model biznesowy straci rację bytu. Podkreślamy, że obecnie zdecydowana

LEWIATAN

większość stron internetowych finansowanych jest z reklamy. Korzystają na tym obywatele, prasa, fundacje i inne podmioty prowadzące działalność w Internecie.
Pozostawienie takiego przepisu w finalnej wersji tekstu uniemożliwiłby również organizację konkursów z nagrodami i promocji, których pośrednim celem jest pozyskanie danych potencjalnych klientów. Postulujmy wykreślenie tego zdania. Promowanie swoich produktów i usług jest nieodłącznym i słusznym elementem działalności gospodarczej, a taki przepis znacznie ograniczałby taką możliwość. Stałby on też w sprzeczności z prawem decydowania przez podmioty danych o tym, na jakich zasadach chcą udostępniać swoje dane i korzystać z oferowanych usług.

Ponadto, konsekwentnie podkreślamy, że wymóg wyraźnej zgody w wielu sytuacjach utrudni funkcjonowanie firm i może być niekorzystny dla podmiotów danych. Sposób wyrażenia zgody powinien być adekwatny do sytuacji (kontekstu), w jakim jest wyrażana. Przykładowo, jeśli konsument zwróci się do przedsiębiorcy z wnioskiem o odroczenie spłaty lub zwolnienie z długu, w uzasadnieniu podając dane o stanie zdrowia, taki wniosek powinien być uznany za zgodę na przetworzenie danych niezbędnych do tego celu. Podobnie - otrzymując wizytówkę lub adres e-mail od innej osoby przedsiębiorca nie powinien poprosić o dodatkowe wyrażenie zgody wyraźnej. Przypominamy, że ciężar udowodnienia uzyskania zgody spoczywa na administratorze. W jego interesie będzie wiec zadbanie o to, by sposób uzyskania zgody był adekwatny do warunków, w jakich ją wyrażono.

Naruszenie bezpieczeństwa danych i definicja naruszenia.

Popieramy wersję Rady, zarówno w odniesieniu do definicji naruszenia jak i sytuacji, w których notyfikacja będzie przekazywana organom nadzorczym i podmiotom danych. W naszej ocenie bardziej korzystna byłaby jednak rezygnacja z wyznaczania konkretnego terminu notyfikacji (jak w wersji PE), na rzecz obecnie funkcjonującego w dyrektywie 2002/58 o prywatności i łączności elektronicznej obowiązku przekazania takiej informacji bez zbędnej zwłoki.

Zwracamy także uwagę na rozszerzenie definicji naruszenia danych w wersji LIBE. Obejmuje ona wszelkie niezgodności z rozporządzeniem, a nie tylko naruszenie bezpieczeństwa. Obowiązek notyfikowania tak szeroko rozumianych naruszeń byłby niezwykle uciążliwy i doprowadziłby do zalewu organów nadzorczych nieistotnymi z punktu widzenia bezpieczeństwa danych notyfikacjami. Należy powrócić do definicji KE i Rady.

Profilowanie

Opowiadamy się za podejściem przyjętym w tekście Rady. Naszym zdaniem zabezpiecza ono interesy podmiotów danych, pozwalając na wykorzystanie profilowania, które nie wpływa znacząco na podmiot danych i nie rodzi skutków prawnych, do usprawiedliwionych celów administratora. Zwracamy uwagę na konieczność wykreślenia ustępu 1 (z tekstu LIBE) , umożliwiającego bezwarunkowy sprzeciw wobec profilowania, niezależnie od tego czy interes administratora danych nie przeważa nad interesem podmiotu danych. Może to podważyć możliwość profilowania w celu oceny zdolności kredytowej, zapobiegania nadużyciom finansowym i innym usprawiedliwionym celom. W naszej ocenie „sprzeciw" rozumiany, jako możliwość zakwestionowania wyniku profilowania, powinien przysługiwać wobec

LEWIATAN

decyzji opartej wyłącznie na profilowaniu(tak, jak w tekście Rady), a nie wobec profilowania jako takiego, tj. wobec samego procesu.
- ust. 2 lit b – opowiadamy się za tekstem Rady. Proponujemy aby w wersji Parlamentu w art. 20 ust.2 lit. b, wykreślić słowo: „expressly". Zwracamy bowiem uwagę, że obowiązek korzystania z profilowania nie zawsze będzie wyraźnie („expressly") wskazany w przepisach prawa powszechnie obowiązującego, często obowiązek ten wynika z przepisów branżowych lub wydawanych przez organy nadzorcze. Przepisy np. w sektorze bankowym, finansowym, ubezpieczeniowym często nakładają na te podmioty ogólny obowiązek zapewnienia odpowiedzialnego kredytowania lub zapobieżenia nadużyciom finansowym. Środki realizacji tego obowiązku, np. stosowanie metod ratingowych, czy scoringowych opartych na automatycznym przetwarzaniu dookreślane są w regulacjach wydawanych przez instytucje nadzorcze, np. Komisja Nadzoru Finansowego czy zrzeszenia, izby branżowe, itp. Takie akty często nie mają statusu przepisów powszechnie obowiązujących i stanowią raczej zasady dobrych praktyk (np. w Anglii „Information Sharing Priciples of Reciprocity") lub są rekomendacjami. Ten postulat mógłby zostać również spełniony poprzez nastepujacą zmianę w ust.2 lit.b "Is expressly authorized by a Union or Member State law, in particular, codes of conduct or the requirements of supervisory authorities".

- ust. 5 –zamiast fragmentu zobowiązującego do wyjaśnienia decyzji opartej o profilowanie lub interwencje człowieka proponujemy dodanie „shall provide suitable measures to safeguard data subject interests".

Przenoszalność danych

Opowiadamy się za wykreśleniem tego prawa z projektu. W ocenie Konfederacji Lewiatan instytucję uregulowaną w tym przepisie należy postrzegać jako nałożenie na administratora obowiązku świadczenia specjalnej usługi podmiotowi danych, a nie instytucję chroniącą dane osobowe tego podmiotu. Żądanie przeniesienia danych osobowych do innego podmiotu nie jest w żaden sposób związane z prawem do ochrony danych osobowych. Nałożenie na przedsiębiorcę obowiązku świadczenia usługi przeczy zasadzie swobody działalności gospodarczej i prawom wolnego rynku. Obawy rodzi zwłaszcza konieczność stosowania interoperacyjnych rozwiązań. Konieczność zapewnienia możliwości przenoszenie danych pomiędzy systemami może negatywnie wpłynąć na innowacyjność, ponieważ nowe rozwiązania będą musiały współgrać z już istniejącymi. Należy również zawrócić uwagę na koszty związane z dostosowaniem obecnie stosowanych systemów do tego wymogu. Jeśli prawo do przenoszenia danych miałoby pozostać w treści rozporządzenia, powinno ono przybrać formę bliższą wersji Parlamentu, a nie Rady.

Prawo do bycia zapomnianym

W naszej ocenie wersja Rady lepiej opisuje sytuacje, w których podmiot danych będzie mógł skorzystać z „prawa do bycia zapomnianym" (ust. 1-3). **Jeśli takie uprawnienie podmiotów danych miałoby pozostać w projekcie rozporządzenia, jego realizacja powinna być możliwa w ściśle określonych przypadkach**. Istotne jest jednak doprecyzowanie, że przysługuje ono tylko, jeśli złożony przez podmiot danych sprzeciw był skuteczny (c). W ustępie 1 (d) należy wyjaśnić, że „prawo do bycia zapomnianym" będzie mogło być zrealizowane tylko w przypadku przetwarzania danych bez podstawy prawnej z artykułu 6 (Lawfulness of processing), a nie w razie zaistnienia jakiejkolwiek

LEWIATAN

niezgodności z przepisami rozporządzenia. Sugerujemy w związku z tym dodanie w punkcie d odniesienia do art. 6.
Nadal konieczne jest wyraźne wskazanie, że prawo do bycia zapomnianym nie powinno mieć zastosowania, jeśli dane zostały zgromadzone i są przetwarzane w oparciu o przepisy ustawowe. Ma to szczególne znaczenie w przypadku danych zbieranych przez instytucje powołane do oceny zdolności kredytowej lub gospodarczej wiarygodności płatniczej. Przetwarzanie i dostęp do takich danych leży w interesie wszystkich podmiotów gospodarczych i jest częścią podejmowanych przez Komisje Europejską działań. Sprawnie działający system informacji o wiarygodności finansowej (creditworthiness), a w szczególności dostęp do samej informacji jest kluczowy dla rozwoju działalności i wzrostu w sektorze SME i ułatwienia dostępu podmiotów z tego sektora do finansowania. Jeżeli prawo do bycia zapomnianym będzie miało zastosowanie także do dostawców informacji oraz do danych przetwarzanych w celu oceny zdolności kredytowej (czy też szerzej wiarygodności kredytowej) będzie ono ograniczało realizacje celów funkcjonowania takich instytucji, ale przede wszystkim może stać w sprzeczności ze strategią Komisji co do tej branży[3].

Z tego względu w ocenie Konfederacji Lewiatan należy przywrócić przewidziany wcześniej w wersji Rady ust. 3(f), wyłączający prawo do bycia zapomnianym, jeśli dane są potrzebne dla zapobiegania i wykrywania nadużyć i innych przestępstw finansowych, dla potwierdzenia tożsamości oraz oceny wiarygodności kredytowej podmiotu danych" (prevention, detection of fraud and other financial crimes, confirming identity and/or determining creditworthiness).

Mimo wprowadzonych do tekstu zmian, wersja Parlamentu i Rady nie dają odpowiedzi na pytanie jak chcąc spełnić swój obowiązek administrator miałby ustalić innych administratorów, którzy przetwarzają upublicznione dane. Nawet jeśli w określonym wypadku byłoby to możliwe, administrator nie ma wpływu wymuszenia takich działań na działających niezależnie od niego podmiotach. Sposób uregulowania tej materii w tekście LIBE jest korzystniejszy, bo przewiduje taki obowiązek tylko w sytuacji, gdy dane zostały przez administratora upublicznione bez podstawy prawnej. Zmiany wymaga jednak brzmienie art. 1 (c), w sposób pozwalający na skorzystanie z prawa do bycia zapomnianym tylko w razie gdy interes administratora nie przeważa nad interesem podmiotu danych, a nie - jak obecnie - bezwarunkowo. Postulujemy również wprowadzenie takiego zastrzeżenia w artykule 19 PE.
Popieramy (j.w.) ważne z punktu widzenia administratora uzależnienie wykonania prawa do bycia zapomnianym od możliwości weryfikacji tożsamości podmiotu wnioskującego (art. 17 ust. 1a LIBE).

Ust. 8a i 8b zobowiązują do zapewnienia mechanizmów kontrolowania okresu przetwarzania danych oraz okresowego przeglądu zgodności przetwarzania z przepisami. Zwracamy uwagę, że jeśli miałyby one być realizowane przez dostosowanie systemów przetwarzania danych to wygeneruje to nieuzasadnione koszty. Opowiadamy się za usunięciem tych ustępów.
Konsekwentnie opowiadamy się za usunięciem delegacji dla KE z rozporządzenia (ust. 9).

Dane wrażliwe

[3] Brussels, 24.04.2013, SWD(2013) 156 final, Commission Staff Working Document; European Financial Stability and Integration Report 2012.

LEWIATAN

Zwracamy uwagę na dodanie w wersji LIBE do katalogu danych wrażliwych kategorii gender identity. Jeśli zwroty ten byłby rozumiany jako płeć podmiotu danych, taka zmiana byłaby dużym problemem praktycznym. Samo zaadresowanie listu zwrotem grzecznościowym (Szanowna Pani/Szanowny Panie) lub użycie imienia, z którego można wywnioskować płeć, byłoby przetwarzaniem danych wrażliwych i wiązało by się z właściwymi dla przetwarzania takich danych obostrzeniami. Dla uniknięcia wątpliwości interpretacyjnych ten rodzaj danych powinien zostać usunięty z katalogu art. 9. Jeśli nie zostałby on wykreślony, istotne jest zapewnienie, że termin ten nie zostanie przetłumaczony (i nie będzie rozumiany) jako płeć, ale wąsko - jako tożsamość płciowa.

Do pkt. 1e artykułu 9 pozwalającego na przetwarzanie wrażliwych „danych osobowych, które zostały wyraźnie podane do publicznej wiadomości przez podmiot danych" postulujemy dodanie „lub dobrowolnie i na wniosek podmiotu danych przekazane administratorowi danych w konkretnym, wskazanym przez siebie celu, a przetwarzanie to odbywa się w interesie podmiotu danych". Ma to znaczenie w sytuacjach, gdy konsumenci podają dane wrażliwe „mimo woli" administratora, na przykład zwracając się do przedsiębiorcy z wnioskiem o odroczenie spłaty lub zwolnienie z długu i uzasadniając prośbę swoją trudną sytuacją osobistą (np. chorobą). Chcąc zrealizować wniosek (i w związku z tym przetwarzać te dane) administrator powinien zażądać od podmiotu danych przesłania odrębnej zgody na przetwarzanie danych wrażliwych. Byłoby to niekorzystne i w praktyce uciążliwe zarówno dla administratora jak i podmiotu danych. Ponieważ zgoda na przetwarzanie danych nie może być dorozumiana z treści wniosku podmiotu danych (wymóg zgody wyraźnej) proponowane przez nas rozszerzenie punktu 1e pozwoliło by na realizację takiego wniosku, bez konieczności pozyskiwania odrębnej, zgody na przetwarzanie na cele realizacji wniosku.

Uprzednia konsultacja

Przepis wymaga skonsultowania organów nadzorczych w sytuacji, kiedy planowe przetwarzanie danych może się wiązać z wysokim ryzykiem.

W naszej ocenie konsultacja powinna mieć charakter fakultatywny. Nawet jeśli przetwarzanie danych wiąże się z pewnym ryzykiem, administrator może stwierdzić, że wie w jaki sposób je zminimalizować. Obowiązek konsultacji i czekania na wytyczne (advice) organu zahamuje rozpoczęcie działalności na 6 do 10 tygodni (wersja Rady). Wersja LIBE jest bardziej korzystna, w części, która pozwala na przeprowadzenie konsultacji „wewnętrznej"-z inspektorem ds. ochrony danych. Takie podejście słusznie odzwierciedla zasadę: „risk based approach". Administrator, który w pełni odpowiada za przetwarzanie danych osobowych, powinien móc samodzielnie podjąć decyzję o przetwarzaniu danych, jeśli w oparciu o jego wiedzę jest w stanie zminimalizować ryzyka związane z określanym przetwarzaniem. Jest to szczególnie uzasadnione w przypadku administratorów korzystających z profesjonalnej obsługi prawnej lub zatrudniających administratora bezpieczeństwa informacji.

Relacja z przepisami szczególnymi i regulacjami sektorowymi.

LEWIATAN

Mimo zmian wprowadzonych w propozycjach PE i Rady nadal wątpliwości budzi relacja postanowień rozporządzenia do unijnych i krajowych przepisów sektorowych czy też regulacji organów nadzorczych, np. organów nadzoru finansowego. Realizacja niektórych praw podmiotów danych stałaby w sprzeczności z przepisami sektorowymi i uniemożliwiłaby podmiotom gospodarczym i instytucjom wywiązanie się z celów, do których zostały one powołane. Jest to szczególnie istotne w przypadku baz danych służących bankom w celu oceny zdolności kredytowej mających na celu zapobieganie nadużyciom finansowym, czy oceny wiarygodności finansowej podmiotów gospodarczych.

W ocenie Konfederacji Lewiatan rozporządzenie powinno rozstrzygnąć, że jego postanowienia pozostają bez uszczerbku dla unijnych i krajowych przepisów szczególnych, regulujących przetwarzanie danych w konkretnych sektorach, przez co należy rozumieć również obowiązki prawne wynikające z regulacji sektorowych, które nie mają charakteru przepisów powszechnie obowiązujących. Odnosi się to zwłaszcza do rekomendacji organów nadzorczych, powszechnie stosowanych kodeksów dobrych praktyk czy też układów zbiorowych. Obecne brzmienie np. artykułu 20 pozwalającego na profilowanie tylko jeśli **wyraźnie** (expressly) zezwalają na to przepisy unijne lub krajowe mogłoby wykluczyć taką interpretację, np. w odniesieniu do stosowanych przez banki i rejestry kredytowe metod ratingowych czy scoringowych dla oceny ryzyka kredytowego i zdolności kredytowej , których obowiązek stosowania nie wynika wprost z ustawy, ale z zaleceń krajowych i unijnych instytucji nadzorczych. Celem doprecyzowania proponujemy wprowadzić ogólną regułę (Recital 36), że jeśli podstawą przetwarzania jest realizacja obowiązku prawnego, obowiązek ten może wynikać także z rekomendacji organów nadzorczych (codes of conduct or the requirements of supervisory authorities)".