FUNDACJA PANOPTYKON

REFORMA EUROPEJSKIEGO PRAWA O OCHRONIE DANYCH OSOBOWYCH

CZYM JEST – DLACZEGO JEST WAŻNA – JAKIE BUDZI REAKCJE

CO SIĘ DZIEJE?

Viviane Reding, komisarz ds. sprawiedliwości, wymiaru sprawiedliwości i obywatelstwa w Komisji Europejskiej, na początku 2012 roku opublikowała projekt rozporządzenia o ochronie danych osobowych, który gruntownie przebudowuje europejskie prawo w tym obszarze. Tym samym rozpoczęła międzynarodową batalię o to, jak chronić prywatność i autonomię informacyjną w cyfrowej rzeczywistości. Spór o projekt rozporządzenia to w istocie spór o hierarchię wartości w społeczeństwie opartym na przetwarzaniu informacji – o to, czy ważniejsza jest nasza wolność decydowania o sposobach korzystania z naszych danych, czy zysk i obietnica rozwoju ekonomicznego.

Rozporządzenie o ochronie danych osobowych ma obowiązywać bezpośrednio w całej Unii Europejskiej, czyli automatycznie zastąpi istniejące przepisy (w Polsce – ustawę o ochronie danych osobowych). Co istotne, będzie dotyczyło wszystkich firm, które oferują swoje usługi na europejskim rynku, także tych największych, które do tej pory podlegały regulacji prawnej np. w Stanach Zjednoczonych, jak Google czy Facebook.

Obecnie nad projektem rozporządzenia o ochronie danych osobowych pracuje Parlament Europejski, przy czym największą rolę odgrywa Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE). To jej opinia na temat przygotowanego przez komisarz Reding projektu wyznaczy granice, w których będzie głosował cały Parlament. Rozstrzygające głosowanie w Komisji LIBE zostało zaplanowane na 29 maja tego roku. W kolejnym kroku Parlament Europejski (reprezentowany przez posła sprawozdawcę z Komisji LIBE), Komisja Europejska i Rada UE zasiądą do negocjacji w ramach tzw. trialogu. Dopiero na bazie wypracowanego kompromisu Parlament, w głosowaniu plenarnym, przyjmie bądź odrzuci projekt rozporządzenia.

Wszystkie instytucje działają pełną parą, aby zakończyć prace jeszcze przed wakacjami (tempo jest tak wykańczające, że niektóre rządy protestują: na ostatnim spotkaniu Rady UE Belgowie rozbili namiot po środku sali spotkań). Poziom skomplikowania projektu i liczba aktorów uczestniczących w pracach nie pozwala jeszcze przewidzieć, jaki będzie ostateczny kształt rozporządzenia. W tym momencie wszystkie karty są na stole. Rozstrzygające będą najbliższe dwa miesiące i decyzje, jakie podejmą m.in. polski rząd i polscy eurodeputowani. Polski rząd ma w tej sprawie wiele do powiedzenia: nie tylko może wpływać na poglądy polskich eurodeputowanych (jak przy okazji ACTA), ale wręcz musi zająć własne stanowisko w Radzie Unii Europejskiej.

DLACZEGO TO JEST WAŻNE?

1. Prawo musi dogonić rzeczywistość

Gdy w 1995 roku uchwalano obowiązującą unijną dyrektywę o ochronie danych (95/46/WE), tylko 1% Europejczyków miał dostęp do Internetu. Przez 18 lat, które minęły od tamtej chwili, rzeczywistość zmieniła się diametralnie. Dostęp do Internetu i cyfrowych technik przetwarzania informacji stał się naprawdę powszechny. Dlatego dziś, dyskutując o reformie ochrony danych osobowych, nie dyskutujemy o ochronie interesów elitarnej grupy, ale o sytuacji każdego. Viviane Reding tak o tym mówi:

„17 lat temu mniej niż jeden procent Europejczyków używał Internetu. Dzisiaj olbrzymia ilość prywatnych danych jest przenoszona i wymieniana pomiędzy kontynentami i na całym świecie w ułamku sekundy. Ochrona danych osobowych jest jednym z podstawowych praw Europejczyków, ale obywatele nie zawsze mają poczucie kontroli nad danymi”[1].

Globalny rynek napędzany nową cyfrową walutą – danymi osobowymi – domaga się regulacji, tak jak kiedyś spekulacja w sektorze finansowym czy eksploatacja środowiska naturalnego. Potrzebne są mocne ramy prawne na następne 20 lat (bo mniej więcej co tyle lat udaje się gruntownie przebudować przepisy prawa). To właśnie próbuje zrobić komisarz Reding: jej projekt ma ambicję dostosować standardy ochrony prywatności

[1] Komunikat Komisji Europejskiej, http://europa.eu/rapid/press-release_IP-12-46_pl.htm?locale=en.

do warunków, jakie panują w świecie zdominowanym przez cyfrowe technologie. Oczywiście, projekt z takimi ambicjami musi też uwzględniać przyszłe trendy w zakresie przetwarzania danych. Między innymi dlatego Reding zdecydowała się na poszerzenie definicji samych danych osobowych i uregulowanie decyzji opartych o profilowanie (por. punkt (ii)). Właśnie na te propozycje bardzo źle reaguje szeroko pojęta branża internetowa, obawiając się „stłumienia innowacji".

Rozwiązania europejskie w zakresie ochrony danych mają też znaczenie w skali globalnej. Wiele krajów (m.in. Brazylia, Korea Południowa, Kanada, Filipiny, Izrael czy Argentyna) tworzyły swoje przepisy w oparciu o unijną dyrektywę o ochronie danych. W taki sam sposób nowe przepisy będą wpływały na standardy ochrony danych poza Unią Europejską.

2. Potrzeba jednolitych standardów prawnych dla ponadnarodowego rynku

Dziś europejskie standardy ochrony danych osobowych obowiązują tylko te firmy, które mają swoją siedzibę lub przetwarzają dane na terytorium Unii Europejskiej. To daje ogromną przewagę np. firmom amerykańskim, które konkurują na tym samym rynku, ale nie podlegają tej samej regulacji. Na ten problem nakładają się istotne różnice w sposobie, w jaki poszczególne państwa członkowskie wdrożyły dyrektywę o ochronie danych osobowych z 1995 roku. W efekcie powstał bardzo skomplikowany prawny kolaż, który nie sprzyja ani biznesowi, ani obywatelom-konsumentom.

Między innymi dlatego Viviane Reding podkreśla, że jej inicjatywa nie jest próbą ataku na istniejące modele biznesowe. Wręcz przeciwnie. Na stworzeniu jednolitych, przejrzystych zasad ochrony danych osobowych dla całej Unii Europejskiej mają skorzystać zarówno obywatele jak i biznes:

„Propozycja reformy ochrony danych otworzy rynek cyfrowy Unii Europejskiej. Spełnia to oczekiwania biznesu dotyczące prawdziwego, jednolitego rynku cyfrowego, z jednym prawem w zakresie ochrony danych osobowych. Implementacja obecnej Dyrektywy jest rozdrobniona i skomplikowana. Dyrektywa z 1995 roku ma 34 artykuły, ale jest implementowana w 27 państwach. Na przykład w Niemczech obecna ustawa o ochronie danych składa się z 63 sekcji. Pomnóżmy je przez 27 państw członkowskich i otrzymamy obraz tego, co w praktyce oznacza »złożoność regulacyjna«. Zastąpimy to morze biurokracji jednym prawem – 91 artykułami, które będą obowiązywać w całej Europie"[2].

O korzyściach wynikających z rozciągnięcia europejskich standardów na wszystkie firmy działające na europejskim rynku mówił też minister Michał Boni:

„Ułatwimy sobie egzekwowanie przepisów unijnych, dlatego że teraz część tych firm, gdy nie chce przestrzegać prawa europejskiego, może uciekać do innego kraju. Chcemy również uprościć reagowanie na wszystkie sygnały o łamaniu tych zasad. Obywatel będzie mógł zgłaszać problem do swojego krajowego [Inspektora Ochrony Danych Osobowych, a konsekwencje prawne działań [przez niego] podjętych [będą wiążące] nie tylko na terenie danego kraju, ale już na terenie całej UE"[3].

3. Nie wszyscy czują się bezpiecznie w cyfrowym świecie

Zmiana reguł gry na globalnym rynku danych jest potrzebna przede wszystkim obywatelom-konsumentom. Jeśli wierzyć badaniom, coraz więcej osób przyznaje, że nie czuje się bezpiecznie w warunkach ciągłego przepływu danych poza ich kontrolą i nie ma w tym zakresie zaufania do firm, z usług których korzysta. Według badania Eurobarometru na temat ochrony danych w Internecie i tożsamości elektronicznej (opublikowane 16 czerwca 2011 roku):

- trzech na czterech Europejczyków akceptuje to, że ujawnianie danych osobowych jest częścią codzienności, niepokoi ich jednak, w jaki sposób firmy (w tym właściciele wyszukiwarek i serwisów społecznościowych) korzystają z tych informacji,
- tylko 26% użytkowników serwisów społecznościowych i 18% klientów sklepów internetowych ma poczucie pełnej kontroli nad swoimi danymi osobowymi,
- 43% badanych twierdzi, że proszono ich o podanie większej ilości danych osobowych niż było to konieczne,
- 70% badanych obawia się, że ich dane osobowe mogą zostać wykorzystane w innym celu niż ten, w którym je zgromadzono,

[2] Komisja Europejska, "EU Data Protection rules: Better for business, better for citizens", http://europa.eu/rapid/press-release_SPEECH-13-269_en.htm.
[3] Radio TOK FM, rozmowa z 12 kwietnia 2013 r., http://bi.gazeta.pl/im/1/13729/m13729031.mp3.

- najczęściej wyrażane przez badanych obawy dotyczyły: tego, że dane przekazywane w trakcie dokonywania zakupów internetowych trafią w ręce oszustów (55% badanych); wykorzystywania dotyczących ich informacji w serwisach społecznościowych bez ich wiedzy (44%); wymieniania się danymi przez firmy bez ich zgody (43%)[4].

Na problem braku zaufania do firm przetwarzających dane osobowych wielokrotnie zwracała uwagę Neelie Kroes, wiceprzewodnicząca Komisji Europejskiej odpowiedzialna za agendę cyfrową:

„Wiele osób nieufnie podchodzi do zakupów w Internecie, obawiając się o swoją prywatność. Blokuje to rozwój europejskiego jednolitego rynku cyfrowego oraz ożywienie gospodarcze. Obywatele mają także bardzo poważne obawy, czy ich tożsamość będzie bezpieczna w Internecie. W odpowiedzi na nie przedstawię już wkrótce odpowiedni projekt legislacyjny" – zapowiadała już w 2011 r. Neelie Kroes[5].

Również Viviane Reding w swoich wystąpieniach podkreśla ten problem:

„Większość osób jest przyzwyczajona do podawania danych osobowych w celu dokonywania zakupów internetowych lub korzystania z sieci społecznościowych. Niepokoi ich jednak to, jak dane te zostaną wykorzystane – nie zawsze mają poczucie kontroli nad tym procesem. (...) Moja propozycja pozwoli zbudować zaufanie do usług świadczonych online zapewniając ludziom lepszą informację o ich prawach i większą kontrolę nad przepływem informacji" – mówiła podczas prezentacji cytowanych badań[6].

4. Coraz więcej osób ma potrzebę kontrolowania przepływu swoich danych

Promowana przez niektóre środowiska biznesowe teza, że konsumentom usług opartych na przetwarzaniu danych już nie zależy na ochronie prywatności i że nie oczekują interwencji regulacyjnych w tym obszarze, nie znajduje potwierdzenia w badaniach. Według cytowanego już Eurobarometru:

- 74% badanych uważa ujawnianie danych osobowych za coraz bardziej znaczący aspekt współczesnego życia,
- 74% badanych chce, żeby gromadzenie i przetwarzanie ich danych w Internecie wymagało ich wyraźnej zgody,
- 90% uważa również, że w całej Europie powinny obowiązywać te same uregulowania prawne[7].

To, że świadomość ludzi zmienia się raczej w kierunku większej troski o kontrolę nad swoimi danymi, pokazują nie tylko badania, ale również konkretne, oddolne inicjatywy. Przykładem jednej z nich jest Europe versus Facebook[8] – akcja zainicjowana przez austriackich studentów, którzy chcą wymusić na Facebooku dostosowanie się do europejskich przepisów dotyczących ochrony danych osobowych.

Aktywiści zorganizowani w tej grupie żądają większej kontroli nad danymi osobowymi, które udostępniają na swoich profilach społecznościowych. Sprzeciwiają się np. praktyce przechowywania danych na serwerach Facebooka mimo ich usunięcia przez samego użytkownika. Oczekują jasnej informacji na temat tego, w jaki sposób ich dane są wykorzystywane. Uważają, że polityka prywatności Facebooka jest sformułowana zbyt ogólnie i zawiera wiele potencjalnie niebezpiecznych luk.

CO KONKRETNIE MOŻE (LUB POWINNO) SIĘ ZMIENIĆ?

Projekt rozporządzenia zaprezentowany przez Reding na początku ubiegłego roku zawierał wiele propozycji zmierzających do wzmocnienia standardów ochrony danych osobowych i ich dopasowania do obecnych praktyk rynkowych. Projekt podlega jednak dalszym przekształceniom w Parlamencie Europejskim i Radzie Unii Europejskiej, skąd wychodzą różne propozycje – czasem zmierzające w dokładnie przeciwnym kierunku. Poniżej przedstawiamy najważniejsze „punkty sporne", wokół których kręci się dyskusja w ramach europejskich instytucji:

[4] Ankieta Eurobarometru dotycząca ochrony danych i tożsamości elektronicznej w Unii Europejskiej, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_pl_en.pdf.
[5] Komisja Europejska, „Ile prywatności w sieci", http://ec.europa.eu/polska/news/110617_dane_pl.htm.
[6] Tamże.
[7] Ankieta Eurobarometru dotycząca ochrony danych i tożsamości elektronicznej w Unii Europejskiej, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_pl_en.pdf.
[8] Strona akcji Europe vs Facebook: http://www.europe-v-facebook.org/.

Definicja danych osobowych i podmiotu danych
Definicja danych osobowych i podmiotu danych to fundamenty całego projektu. Od tego, jak szeroko zostaną zakrojone, zależy zakres obowiązywania nowego prawa. Zgodnie z projektem Reding, „dane osobowe" oznaczają każdą informację dotyczącą podmiotu danych, natomiast sam „podmiot danych" – każdą osobę, którą można (czyli: którą ktokolwiek na świecie może) zidentyfikować pośrednio lub bezpośrednio. To dobra, szeroka definicja, choć na kolejne 20 lat może się okazać niewystarczająca.

Z perspektywy organizacji walczących o wyższe standardy ochrony prywatności (m.in. Fundacji Panoptykon), ważne jest, żeby dane były traktowane jako „osobowe" nie tylko wtedy, gdy dotyczą możliwej do zidentyfikowania osoby. W wielu przypadkach, szczególnie w Internecie, identyfikacja wcale nie jest konieczna do naruszenia prywatności – coraz częściej wystarcza np. tymczasowy identyfikator, który może zdradzać nasz internetowy profil. Dlatego definicja „danych osobowych" powinna obejmować wszelkie identyfikatory, także te wykorzystywane do śledzenia w sieci, a to, czy konkretna osoba jest możliwa do zidentyfikowania, musi być oceniane w odniesieniu do aktualnych możliwości technicznych.

Ograniczenia dla decyzji opartych na profilowaniu
Profilowanie, czyli zbieranie i automatyczne przetwarzanie informacji na nasz temat po to, żeby zbudować pewne założenia na temat naszej osobowości i przyszłych zachowań, wiąże się z wieloma ryzykami. Najważniejsze to ryzyko dyskryminacji i utrwalenia społecznych stereotypów. Poważnym problemem jest też „margines błędu", który zawsze występuje w przypadku korelacji statystycznych, a dla konkretnej osoby może oznaczać wykluczenie z ważnej społeczności lub odmowę istotnych usług.

Przepisy zaproponowane przez komisarz Reding nie zawierają definicji samego profilowania, ale za to poświęcają sporo miejsca środkom (np. decyzjom) opartym na profilowaniu, wobec których formułują szereg ograniczeń. Np. przyznają osobie, która jest poddawana takim środkom, prawo do uzyskania „ludzkiej interwencji", jeśli nie zgadza się z podjętą decyzją.

Zdaniem organizacji walczących o wyższe standardy ochrony prywatności potrzebne jest ograniczenie możliwości wykorzystywania danych wrażliwych w procesie profilowania (ponieważ znacząco zwiększa ryzyko dyskryminacji). Projekt powinien przewidywać również prawo do informacji o tym, według jakich reguł i w jakim celu tworzony jest nasz profil.

***Privacy by default* – maksymalna ochrona prywatności w opcji „domyślnej"**
Komisarz Reding proponuje zmianę paradygmatu w relacji klient – usługodawca z „domyślnego śledzenia" na „domyślne gwarancje prywatności" (*privacy by default*). Zgodnie z tym modelem już w momencie, w którym zaczynamy korzystać z danego serwisu czy usługi, powinniśmy mieć zapewnioną maksymalną ochronę prywatności. Do nas – klientów – będzie należała decyzja czy i jakimi danymi chcemy się dzielić.

Dotychczas ten wybór należał do dostawców usług, a więc często „opcją domyślną" było udostępnianie wszystkich danych – czego nie każdy użytkownik był świadomy. Model *privacy by default* zabezpiecza dane osobowe przed eksploatacją przez samego usługodawcę. Nie chodzi przy tym o zakaz przetwarzania danych, ale o uszanowanie podstawowych zasad, takich jak celowość, proporcjonalność czy adekwatność (tego, co jest na nasz temat zbierane do tego, co jest nam oferowane).

Takie same standardy dla firm i instytucji spoza Unii Europejskiej
Nawet najlepsza regulacja na poziomie unijnym niewiele zmieni bez gwarancji, że te same standardy prawne będą obowiązywały firmy działające na europejskim rynku, ale zarejestrowane poza granicami Unii Europejskiej. Zgodnie z projektem rozporządzenia o ochronie danych wszystkie firmy, które kierują swoje usługi do obywateli Unii Europejskiej lub przynajmniej monitorują ich zachowanie w sieci, mają stosować się do takich samych zasad. Wprowadzenie takiego wymogu nie tylko pomoże ujednolicić standardy obowiązujące na europejskim rynku, ale przede wszystkim powstrzyma „wyścig do dna". Obecnie wiele firm (także polskich) rejestruje swoje siedziby poza Unią Europejską – w kraju, którego prawo dotyczące ochrony danych osobowych jest mniej rygorystyczne.

Informacja podana ludzkim językiem
Dziś ani dostarczenie rzetelnych informacji o przetwarzaniu danych, ani ich przystępne podanie nie mieści się w rynkowym standardzie. Za największe kłamstwo Internetu uważana jest formułka „przeczytałem i zgadzam się", bo mało kto jest w stanie przebrnąć przez kilometrowe i hermetyczne warunki umów. Zgodnie z projektem Reding informacje o przetwarzaniu danych osobowych muszą być sformułowane w sposób prosty, zwięzły i zrozumiały.

Definicja zgody na przetwarzanie danych
Jedną z podstaw przetwarzania danych jest zgoda osoby, której one dotyczą. Projekt Reding mówi, że taka zgoda musi być wyraźna – nie można jej domniemywać z naszego zachowania, bo w praktyce otwierałoby to drogę do oczywistych nadużyć. Potwierdzają to badania Eurobarometru, zgodnie z którymi aż 74% obywateli Unii Europejskiej chciałoby udzielać wyraźnej zgody przed rozpoczęciem gromadzenia i przetwarzania ich danych w Internecie.

Uzasadniony interes administratora – „koń trojański" projektu rozporządzenia
Najbardziej kontrowersyjną podstawą przetwarzania naszych danych, którą w swoim projekcie utrzymuje Reding, jest tzw. uzasadniony interes administratora. To pojęcie bardzo niejasne, zakładające uznaniowość, a faktycznie dobrą wolę, administratora, który sam ma decydować o tym, czy dane mogą być przetwarzane (bez zgody osoby, której dotyczą). Administrator danych nie powinien być sędzią we własnej sprawie.

Zdaniem organizacji walczących o wyższe standardy ochrony prywatności ta podstawa powinna całkowicie zniknąć z rozporządzenia, a przynajmniej zostać lepiej zdefiniowana i obudowana dodatkowymi gwarancjami.

JAKA JEST REAKCJA NA TE POMYSŁY?

Projekt reformy europejskiego prawa o ochronie danych osobowych wzbudza wielkie emocje. Reakcje na zmiany proponowane przez komisarz Reding bywają skrajnie różne, czemu trudno się dziwić, biorąc pod uwagę zróżnicowanie interesów, które trzeba w tej regulacji pogodzić. Ponieważ stawka, także ekonomiczna, jest naprawdę wysoka, instytucje europejskie od ponad roku muszą się mierzyć z bezprecedensowym zainteresowaniem i ogromnym naciskiem ze strony wszystkich zainteresowanych środowisk.

Viviane Reding przyznaje, że propozycja Komisji Europejskiej stała się przedmiotem najbardziej agresywnego lobbingu jaki do tej pory widziała. Świadczyć o tym może również liczba opinii, które zostały do tej pory przesłane do europosłów pracujących nad reformą. Tylko jedna eurodeputowana, Amelia Andersdotter opublikowała ponad 100 dokumentów, które zostały jej przesłane przez biznes i inne organizacje[9].

Większość międzynarodowych korporacji podejmuje działania lobbingowe „dwutorowo": pod własnym szyldem i poprzez zrzeszenia przedsiębiorców. Niektóre firmy idą jeszcze krok dalej i w celach lobbingowych zakładają stowarzyszenia o mylnie brzmiących nazwach jak np. „Industry Coalition for Data Protection" czy „European Privacy Association". Takie działanie może wprowadzać w błąd decydentów politycznych, a na pewno podważa zasady transparentności.

Najbardziej intensywną kampanię lobbingową prowadzą firmy i władze amerykańskie, na czele z Departamentem Handlu USA oraz Amerykańską Izbą Handlową. Rząd USA oficjalnie argumentuje, że Europa, ze swoimi restrykcyjnymi przepisami chroniącymi prywatność, pozostanie osamotniona i znacznie osłabi swój potencjał rozwojowy w stosunku do reszty świata. Pod wpływem amerykańskich nacisków wielu eurodeputowanych, szczególnie w gronie Europejskiej Partii Ludowej, przyjęło retorykę podważającą sens i wartość prawa do prywatności, jak gdyby zapominając, że z Karty Praw Podstawowych Unii Europejskiej nadal wynika obowiązek ochrony tego prawa.

Po przeciwnej stronie w kampanię wokół reformy europejskiego prawa o ochronie danych osobowych zaangażowali się aktywiści z całej Europy, wspierani przez środowiska akademickie i równie stanowcze opinie narodowych rzeczników ochrony danych skupionych w Grupie Roboczej Artykułu 29[10]. Eurodeputowani dostają w tej sprawie maile z Wielkiej Brytanii, Holandii, Danii, Niemiec, Francji, Belgii, Polski, Austrii, Rumunii. Oficjalna strona kampanii: http://www.privacycampaign.eu/.

W styczniu tego roku, rok po ogłoszeniu przez Komisję Europejską projektu rozporządzenia, grupa organizacji pozarządowych i niezależnych ekspertów z zakresu ochrony danych osobowych przyjęła deklarację o potrzebie zwiększenia standardów ochrony prywatności w cyfrowym świecie (*The Brussels Privacy Declaration*). „Prywatność jest jednym z fundamentalnych praw człowieka, a mimo to jest powszechnie ignorowana. Jesteśmy wkurzeni" – pod tym stwierdzeniem podpisało się ponad 50 organizacji i kilkaset nieprzypadkowych osób[11].

[9] Por. https://dataskydd.net/lobbydokument-i-parlamentet-om-dataskydd/.
[10] Por. http://ec.europa.eu/justice/data-protection/article-29/.
[11] Tekst deklaracji: http://brusselsdeclaration.net/.

25 stycznia 2012	Komisja Europejska przedstawia projekt rozporządzenia w sprawie ochrony danych osobowych[12]. Projekt trafia jednocześnie do Parlamentu Europejskiego oraz pod obrady grupy roboczej Rady UE (DAPIX), w której spotykają się przedstawiciele rządów. Polskę w tej grupie reprezentują urzędnicy Ministerstwa Administracji i Cyfryzacji. Prace grupy powinny zakończyć się na początku czerwca.
2 marca 2012	Ministerstwo Administracji i Cyfryzacji rozpoczyna konsultacje projektu rozporządzenia w sprawie ochrony danych osobowych. W toku konsultacji swoje stanowiska zgłosiły: Allegro, Biuro Informacji Kredytowej S.A., Fundacja Dzieci Niczyje, Fundacja Panoptykon[13], IAB Polska, Izba Wydawców Prasy, Związek Banków Polskich, Telekomunikacja Polska, Polska Izba Komunikacji Elektronicznej[14].
Lipiec 2012	Polski rząd publikuje projekt swojego stanowiska w sprawie projektu rozporządzenia[15].
8 stycznia 2013	Jan Philipp Albrecht, poseł-sprawozdawca dla tego projektu, publikuje swoje propozycje poprawek do rozporządzenia o ochronie danych osobowych[16]. Jan Philipp Albrecht jest członkiem Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE).
13 lutego 2013	Drugi Kongres Wolności w Internecie, zorganizowany przez Ministerstwo Administracji i Cyfryzacji. Pierwsza publiczna dyskusja na temat reformy ochrony prywatności z udziałem premiera, ministra Michała Boniego, Generalnego Inspektora Ochrony Danych Osobowych, eurodeputowanych i organizacji pozarządowych[17].
1 marca 2013	Spotkanie ministra Boniego z komisarz Viviane Reding[18].
13 maja 2013	Planowana wizyta komisarz Viviane Reding w Warszawie.
29 maja 2013	Głosowanie w Komisji ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE).
6-7 czerwca 2013	Posiedzenie Rady UE ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w Luksemburgu. Na tym posiedzeniu ministrowie z poszczególnych państw członkowskich podejmą kluczowe decyzje dotyczące projektu rozporządzenia.

[12] Komunikat prasowy Komisji Europejskiej, http://europa.eu/rapid/press-release_IP-12-46_pl.htm?locale=en.
[13] Stanowisko Fundacji Panoptykon, https://mac.gov.pl/wp-content/uploads/2013/03/opinia-fundacji-Panoptykon.pdf.
[14] Wszystkie opinie dostępne są na stronie Ministerstwa Administracji i Cyfryzacji, https://mac.gov.pl/ochronadanychosobowych/.
[15] Por. https://mac.gov.pl/wp-content/uploads/2013/03/Projekt-stanowiska-RP_COM_2012_011.pdf.
[16] Por. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf. Komentarz Fundacji Panoptykon: http://panoptykon.org/wiadomosc/kompromis-czy-kompromitacja-posel-sprawozdawca-parlamentu-europejskiego-przedstawia-swoja-.
[17] Por. relacja MAC, http://www.kprm.gov.pl/multimedia/wideo/2-kongres-wolnosci-w-internecie.html.
[18] Por. https://mac.gov.pl/wiadomosci/boni-i-reding-rozmawiali-o-ochronie-danych-osobowych/.

POLECANE ŹRÓDŁA

1. Najważniejsze postulaty Fundacji Panoptykon, http://panoptykon.org/wiadomosc/aby-prywatnosc-byla-lepiej-chroniona-6-postulatow-fundacji-panoptykon.
2. Wszystko na temat reformy europejskich przepisów o ochronie danych osobowych, http://panoptykon.org/category/tagi-tematyczne/reforma%20prywatno%C5%9Bci.
3. Opinia Grupy Roboczej Artykułu 29 na temat projektu rozporządzenia, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.
4. Opinia uzupełniająca Grupy Roboczej Artykułu 29, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.
5. Opinia Europejskiego Inspektora Ochrony Danych Osobowych na temat projektu rozporządzenia, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.
6. Opinia uzupełniająca Europejskiego Inspektora Ochrony Danych Osobowych, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

FUNDACJA PANOPTYKON

O nas

Fundacja Panoptykon powstała w kwietniu 2009 r. Jej celem jest działanie na rzecz ochrony praw człowieka w kontekście rozwoju „społeczeństwa nadzorowanego" – współczesnych form kontroli i nadzoru nad społeczeństwem. W obszarze zainteresowania Fundacji znajdują się takie zagadnienia jak: powstawanie i rozbudowa baz danych, rozwój monitoringu wizyjnego, retencja danych telekomunikacyjnych, wykorzystywanie technologii biometrycznych, uprawnienia służb specjalnych, techniki nadzoru nad pracownikami, praktyki kontroli przepływu informacji w Internecie.