http://www.cyberlaw.pl/

BIG DATA i ochrona danych, prywatności

Styczeń 20, 2014 Beata Marek

BIG DATA jest niczym diament dla biznesu. W dobie rozwijających się technologii o globalnym zasięgu interesująca jest coraz bardziej relacja właśnie pomiędzy BIG DATA a ochroną danych, ochroną prywatności.

W dniu 28 stycznia 2014 r. obchodzony jest, w Polsce, **VIII Dzień Ochrony Danych Osobowych.** Razem z Generalnym Inspektorem Ochrony Danych Osobowych, dr Wojciechem Rafałem Wiewiórowskim, zapraszamy do wzięcia udziału w konferencji „Prywatność w cyfrowym świecie". Odbędzie się ona w Warszawie, w siedzibie Centralnej Biblioteki Rolniczej, ul. Krakowskie Przemieście 66. Blog cyberlaw.pl objął patronatem medialnym to wspaniałe wydarzenie.

A co na Ciebie czeka jeszcze w tym dniu?

Będziesz mógł skorzystać z **bezpłatnych porad prawnych** z zakresu ochrony danych osobowych, a także otrzymać publikacje Biura Generalnego Inspektora Ochrony Danych Osobowych oraz inne materiały edukacyjne dotyczące ochrony danych osobowych i prywatności.

Warto się pojawić! Z okazji VIII dnia ochrony danych osobowych porozmawiałam z Generalnym Inspektorem m.in. o tym jak wygląda relacja pomiędzy ochroną danych a Internetem Rzeczy? Co dzieje się z projektem jednolitego rozporządzenia dot. ochrony danych osobowych? Jak wygląda obowiązek notyfikacyjny w Polsce (od czasu nowelizacji prawa telekomunikacyjnego)?

Internet Rzeczy czyli nowe oblicze BIG DATA

W związku z tym, że w serwisie Spider's Web pojawiły się w tym miesiącu liczne relacje z tragów CES, do których przeczytania Ciebie zachęcam, postanowiłam pierwszy fragment mojej rozmowy z dr Wojciechcem Rafałem Wiewiórowskim opublikować właśnie na jego łamach. Dotyczy on relacji pomiędzy ochroną danych osobowych, ochroną prywatności a Internetem Rzeczy.

A o czym przeczytasz u mnie?

Projekt rozporządzenia unijnego

Beata Marek: Projektowane przepisy związane z reformą ochrony danych osobowych w Unii Europejskiej (dalej jako „UE") zapewniają zwiększenie poziomu wiedzy dla użytkowników urządzeń, realizację obowiązków informacyjnych na jednolitym poziomie i przede wszystkim też zmieniają zakres terytorialny ich obowiązywania. Zgodnie z art. 3 tegoż projektu, przepisy rozporządzenia znajdują zastosowanie do przetwarzania danych

osobowych podmiotów danych mających miejsce zamieszkania w EU przez administratora niemającego siedziby w Unii, gdy przetwarzanie wiąże się z:

- a) oferowaniem towarów lub usług takim podmiotom danych w Unii, lub
- b) monitorowaniem ich zachowania.

Na jakim etapie są prowadzone rozmowy nad wdrożeniem nowych przepisów? Czy **do maja 2014 r.** jest jakaś szansa, że możemy spodziewać się ich przyjęcia?

Dr Wojciech Wiewiórowski: Już teraz możemy sobie wyraźnie powiedzieć, że do maja 2014 r. tych przepisów na pewno nie będzie. O ile Parlament Europejski w październiku 2013 r. przyjął swoją propozycję zarówno rozporządzenia, jak i dyrektywy dotyczącej byłego III filaru, o ile Komisja jest do tego przygotowana ze swoim projektem, o tyle nie jest do tego gotowa Rada. Na grudniowym posiedzeniu nie zdołała ona bowiem podjąć konkluzji dotyczącej nawet części rozporządzenia. Doszło tutaj do wyraźnej rozbieżności pomiędzy państwami członkowskimi. Oznacza to, że w tej kadencji Parlamentu Europejskiego do trilogu tych podmiotów nie dojdzie. Trilog, jeżeli się zacznie, to dopiero na początku nowej kadencji Parlamentu Europejskiego. O ile jednak wybory do Europarlamentu stopują w jakimś stopniu działania Parlamentu Europejskiego, to w przypadku Rady są irrelewantne. Obecnie spotkania DAPIXu odbywają się co tydzień. Pozostaje mieć nadzieję, że te następnych kilka miesięcy zostanie wykorzystanych przez Radę do zamknięcia procesu prac nad rozporządzeniem i jesienią czy też późnym latem będziemy w stanie powrócić do prac nad reformą. Z tym że wtedy pojawi się pytanie, czy przyjęty projekt będzie obowiązujący dla nowej ekipy parlamentarnej, czy prace zaczną się od początku. Jeżeli w grę wchodziłaby ta pierwsza opcja, to możliwe jest przyjęcie rozporządzenia jeszcze w 2014 r. Jeżeli jednak nie, to oznacza rozpoczęcie prac od nowa i odsunięcie reformy ochrony danych osobowych o kolejnych kilka lat.

Transfer danych, safe harbour

BM: Komisja Europejska zaproponowała **13 zaleceń** w celu usprawnienia funkcjonowania systemu bezpiecznego transferu danych osobowych. Czy są one dobre?

WW: Z pewnością idą w dobrym kierunku. Wiele jednak zależy od tego, jak zostaną odebrane po drugiej stronie Oceanu. Można powiedzieć, że to są warunki, które postawiła Europa, natomiast USA wciąż jeszcze nie odniosły się do nich wprost. Znamy stanowisko Prezydenta Obamy w sprawie reformy działania służb specjalnych Stanów Zjednoczonych przedstawione w wypowiedzi z 17 stycznia 2014 r. Niemniej z punktu widzenia użytkownika z Europy ta wypowiedź nie wniosła nic nowego. Można powiedzieć, że jeśli nie jestem obywatelem USA lub przywódcą jego kraju sojuszniczego, prezydent Obama nie zapowiedział żadnej zmiany nastawienia USA do mnie.

BM: Wymiana danych osobowych między UE i USA do celów komercyjnych została uregulowana w decyzji w sprawie ochrony prywatności w ramach **safe harbour** (pol. bezpieczna przystań). Czy dokument ten wymaga zmiany?

WW: Kiedy w 2010 r. rozpoczynałem pracę na stanowisku Generalnego Inspektora, byłem bardzo sceptyczyny do programu safe harbour i publicznie określałem go jako świnkę morską. Ani to świnka, ani morska. Ani to safe, ani to harbour. Krytycznie wypowiadłem się

na temat tej decyzji i tego, że stanowi podstawę transferu danych. Natomiast przyznaję, że w ciągu pierwszych trzech lat pełnienia swojej funkcji zmieniłem zdanie przede wszystkim na temat sposobu wykonywania nadzoru w USA. Federalna Komisja Handlu (FTC) w ciągu kilku lat nadzorowania tego rozwiązania wykonała ogromną pracę. To doprowadziło do sytuacji, że na przełomie 2012 i 2013 r. Biuro Generalnego Inspektora zmieniło nieco swoją praktykę w zakresie zezwoleń na transfer danych do państw trzecich, w dużo większym stopniu otwierając się na transfer poprzez USA do kolejnych państw trzecich dokonywany właśnie na podstawie safe harbour. Mieliśmy poprostu dobre doświadczenia w pracy z Federalną Komisją Handlu. Kiedy jednak już zmieniliśmy te zasady, wybuchła sprawa PRISM i problem safe harbour powrócił.

Powiedziałbym, że to, co wyglądało na dobry nadzór, dobry enforcement ze strony Federalnej Komisji Handlu, niestety, w sposób wyraźny dotyczy najwyżej komerycyjnego użycia tych danych. Jest natomiast problem z safe harbour w kontekście dostępu do danych, jaki mają instytucje administracji amerykańskiej.

Bardzo ważne są również kwestie możliwości dostępu do swoich danych oraz zakwestionowania sposobu ich przetwarzania. Pragnę przypomnieć, że ten system rozstrzygania skarg indywidualnych w safe harbor jest bardzo rzadko wykorzystywany. Pytanie Tylko, czy dlatego że Europejczycy tak naprawdę nie interesują się tym, jak ich dane są przetwarzane w USA, czy jednak system ten jest na tyle skomplikowany i na tyle amerykański, że Europejczykowi trudno z niego poprostu skorzystać?

Zgłoszeń kwestionujących to, w jaki sposób dane przekazane w ramach safe harbour są przetwarzane od początku istnienia tego programu było zaledwie 4, przy czym 2 złożyła ta sama osoba. W związku z tym z możliwości złożenia skargi do Grupy UE ds. ochrony danych skorzystało najwyżej 3 Europejczyków.

Wydaje mi się, że cała praca jeżeli chodzi o safe harbour jest jeszcze przed nami. Poza tym czekamy na reakcję ze strony USA. Wiemy, że jednocześnie trwają prace nad tym, jak będzie wyglądał dalszy nadzór nad NSA.

BM: Co mogłoby **nakłonić USA do** przystąpienia do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych („Konwencja 108")?

WW: Trudno mi powiedzieć. Może uderzenie meteorytu? A mówiąc już zupełnie poważnie, o ile zdarzają się sytuacje, że USA przystępują do konwencji, której nie negocjowały i w pracach nad którą nie uczestniczyły, jak np. konwencja butapesztańska o cyberprzestępczości, której notabene nie ratyfikowała jeszcze Polska, to co do Konwencji 108 byłbym sceptyczny. Statuuje ona bowiem europejskie spojrzenie na ochronę danych osobowych oraz na podstawowe pojęcia w tym zakresie i jest z zasady różna od tego, w jaki sposób chroniona jest prywatność w konstytucji amerykańskiej.

Mam nadzieję, że Konwencja 108 będzie atrakcyjna dla innych krajów świata i pokaże, że jest pewnym słownikiem, którym posługują się nie tylko Europejczycy. Na razie spoza Europy przystąpił do niej jedynie Urugwaj, ale planuje przystąpić Maroko.

Ratyfikowanie Konwencji nie rozwiązuje oczywiście wszystkich problemów. Od 1 września 2013 r. stroną Konwencji jest Rosja, a nie oznacza to jednak, że jesteśmy przekonani, że

wszystkie dane, które są przetwarzane przez instytucje prywatne oraz służby publiczne tego państwa są w 100% bezpieczne.

BM: Jednak przystąpienie do Konwencji to już jakiś krok. Okazanie dobrej woli.

WW: Oczywiście. To jest krok dobry. Zresztą współpracujemy z kolegami z Rosji, np. w grudniu 2013 r. miałem okazję być na odbywającej się w Moskwie konferencji poświęconej ochronie danych osobowych. Z drugiej strony wprost mówimy, że mamy jednak wątpliwości co do niezależności organu nadzorczego w Rosji i co do pewnych praktycznych rozwiązań, które istnieją w ustawie rosyjskiej. Ale prawdą jest, że Rosja ratyfikowała Konwencję.

Obowiązek notyfikacyjny

BM: W 2013 r. w Polsce zaczęło obowiązywać znowelizowane Prawo telekomunikacyjne. Jak realizowany jest obowiązek notyfikacyjny, o którym mowa m.in. w art. 174a ustawy? Ile zgłoszeń zostało dokonanych w 2013 r.? **Jakie przeważają incydenty**?

WW: W 2013 r. zgłoszono ponad 170 zderzeń bezpieczeństwa danych u przediąbiorców telekomunikacyjnych. Zgłoszenia dokonywane są z dnia na dzień. Dzisiaj już widziałem dwa nowe. Z reguły są to drobne sprawy. Przykładowo błędnie zostały wysłane faktury i np. Pan Kowalski mógł przeczytać dane z faktury, a czasem też z bilingu, Pana Nowaka i odwrotnie. Co ciekawe i ważne, konieczność ujawniania nawet drobnych wycieków doprowadziła do tego, że operatorzy telekomunikacyjni poprawili procedury związane z zabezpieczaniem danych.

Zdarzyło się kilka większych zgłoszeń. Prawo przewiduje zaś, że w przypadku, gdy naruszenie danych osobowych może mieć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, operator o tym, że zdarzenie miało miejsce, powinien powiadomić również abonenta. Jeśli tego nie robi, to Generalny Inspektor może w drodze decyzji nakazać wykonanie tego obowiązku. Mogę powiedzieć, że we wszystkich poważniejszych sytuacjach, operatorzy telekomunikacyjni sami podejmowali decyzje o informowaniu swoich abonanetów o wyciekach i sprawnie informowali Generalnego Inspektora o tym, jakie środki bezpieczeństwa podjęli, by zapobiec podobnym incydentom w przyszłości.

W jednym przypadku chodziło o znaczący wyciek danych. Lokalny operator telekomunikacyjny zgubił dane kilkuset tysięcy użytkowników. Sprawa ta jest jeszcze wciąż badana zarowno przez organa ścigania, jak przez Generalnego Inspektora.

W najbliższym czasie mamy zamiar przeanalizować zgłoszenia i wstępnie podsumować pierwszy okres obowiązywania nowych przepisów. Niewątpliwie jedną z zauważanych przez nas tendencji jest to, że spośród dużych operatorów od tylko jednego nie spływają żadne zawiadomienia. Powody mogą być dwa – albo rzadne wycieki się tam nie zdarzają, albo operator ma pewien problem z raportowaniem.

W 2013 r., w marcu oraz we wrześniu, GIODO spotkał się przedstawicielami operatorów telekomunikacyjnych, by przeanalizować i wyjaśnić praktyczne aspekty dotyczące informowania GIODO o naruszeniach, w tym różne kwestie administracyjnoprawne, jak m.in. pełnomocnictwa do składania zawiadomień. Z reguły zgłoszenia o incydentach dokonywane są elektronicznie. Przygotowaliśmy na te potrzeby osobny system teleinformatyczny.

Sądzę, że do wykonywania nowych obowiązków dobrze przygotowały się obie strony, zarówno GIODO, jak i operatorzy telekomunikacyjni. W lipcu 2013 r. pojawiło się co prawda rozporządzenie wykonawcze UE, które minimalnie zmieniło zasady w stosunku do tych przyjętych dla rynku polskiego, ale poradziliśmy sobie z tym dość sprawnie. We wrześniu 2013 r. odbyło się w Brukseli spotkanie podmiotów, które zajmują się zbieraniem właśnie tych informacji w UE i okazało się, że tylko w 5 krajach wdrożono to rozwiązanie na czas, z czego w 4 przygotowano w tym celu rozwiązanie teleinformatyczne.

BM: Czyli Polska znalazła się w czołówce, co cieszy. Nawiązując jeszcze do proponowanego rozporządzenia dot. ochrony danych osobowych i propozycji objęcia obowiązkiem notyfikacyjnym szerszej grupy podmiotów, jestem ciekawa zdania Generalnego Inspektora na ten temat.

WW: Rozporządzenie przewiduje, że obowiązek notyfikacyjny zostanie rozciągnięty na wszystkie podmioty przetwarzające dane. Jestem bardzo ostrożny co do tego rozwiązania, biorąc pod uwagę konsekwencje, z jakimi mamy do czynienia w krajach, które je wprowadziły. Przy okazji warto wskazać, że data breach notfication, przeciwko któremu protestują przedstawiciele biznesu w Polsce, to nie jest europejski tylko amerykański pomysł. Co więcej, w USA, w każdym stanie jego realizacja wygląda inaczej. Wspólne rozwiązanie dla Europy miałoby sens, ale zwracam jednak uwagę, że np. w Irlandii – gdzie przedsiębiorców obowiązuje kodeks dobrych praktyk w zakresie zgłaszania takich zdarzeń – doszło do tego, że organ ochrony danych stał się podmiotem prowadzącym rejestrem zgubionych pendrive'ów. Każdy, kto zgubił pendrive, na wszelki wypadek zgłaszał to irlandzkiemu organowi ochrony danych osobowych.

Jeżeli nośnik jest zaszyfrowany, to jego utratę powinno traktować się jako zdarzenie małej wagi nieobjęte obowiązkiem notyfikacyjnym. swoją drogą może to powodować upowszechnienie szyfrowania danych jako dobrego sposobu nie tylko na zmniejszenie swojej odpowiedzialności, ale przede wszystkim zabezpieczenie swoich danych.

BM: Dziękuję bardzo za rozmowę.

WW: Dziękuję i zapraszam do uczestnictwa w VIII Dniu Ochrony Danych Osobowych. Kulminacyjnym punktem będzie konferencja „Prywatność w cyfrowym świecie", podczas której poruszane będą takie kwestie, jak big data, zagrożenia związane z korzystaniem z aplikacji mobilnych oraz konieczność edukacji cyfrowej. Jednocześnie w tym dniu w Centralnej Bibliotece Rolniczej w Warszawie, gdzie będzie się odbywała konferencja GIODO, dyżurować będą pracownicy Biura, od którzy udzielać będą porad i wyjaśnień z zakresu ochrony danych osobowych i prywatności.

Autor grafiki promującej wpis: Haydn Woods