WSKAZANIA ZAWARTE W ROZPORZĄDZENIU Z 2004 R. SĄ PRZESTARZAŁE

WYWIAD Z DR. WOJCIECHEM RAFAŁEM WIEWIÓROWSKIM, GENERALNYM INSPEKTOREM OCHRONY DANYCH OSOBOWYCH

Data wywiadu: 21 grudnia 2012 r.

ROZMÓWCA:
dr Wojciech Rafał Wiewiórowski,
Generalny Inspektor Ochrony Danych Osobowych

Redakcja: Czy sklepy internetowe mają świadomość, że istnieje ustawa o ochronie danych osobowych? To pytanie nasuwa się, gdy weźmie się pod uwagę fakt, że liczba sklepów internetowych jest znacznie większa niż liczba zbiorów danych osobowych zgłoszonych do rejestracji GIODO?

Dr Wojciech Wiewiórowski: Wbrew pozorom wniosków o rejestrację zbiorów danych osobowych składanych przez różnego rodzaju serwisy internetowe, w tym sklepy internetowe, jest całkiem sporo. Niekiedy trudno jest rozróżnić, co jest sklepem internetowym, a co serwisem internetowym, ponieważ działalność handlowa jest niekiedy jedynie częścią działalności serwisu internetowego. Każdy najprostszy poradnik, nawet internetowy, dotyczący tego, jak prowadzić sklep internetowy, zawiera informacje odnoszące się do obowiązków e-sklepów wynikających z ustawy o ochronie danych osobowych. Główny problem, który pojawia się u prowadzących sklepy internetowe, to ustalenie, w jakich sytuacjach należy dokonywać rejestracji zbiorów danych osobowych, a w jakich istnieją w tym zakresie pewne zwolnienia. O ile dane, które pozyskujemy od klienta, wykorzystujemy wyłącznie celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, to zawierającego je zbioru danych nie musimy zgłaszać do rejestracji GIODO. Jednak gdybyśmy dane klienta zamierzali wykorzystywać w innych celach, np. marketingowych, albo udostępniać je współpracującym z nami firmom bądź po prostu nimi handlować, wówczas z obowiązku zgłoszenia zbioru danych osobowych do rejestracji nie bylibyśmy zwolnieni. Przy okazji warto dodać, że ustawa o ochronie danych osobowych nie zabrania handlu tymi danymi. Jest on dopuszczalny, ale wówczas trzeba spełnić obowiązki, które wynikają z jej przepisów. Uważam, że ze świadomością istnienia przepisów o ochronie danych osobowych nie jest tak źle. Dużo większe zastrzeżenia miałbym co do sposobu zabezpieczania danych osobowych w sklepach internetowych niż np. do spełniania przez nie obowiązków związanych z rejestracją zbiorów czy dopełnianiem tzw. obowiązku informacyjnego.

Redakcja: Zarówno przepisy ustawy o ochronie danych osobowych, jak i wydane na jej podstawie rozporządzenie z 2004 r. określają wymogi dotyczące zabezpieczenia danych osobowych. Czy jednak sklepom internetowym można zarekomendować jakieś standardowe rozwiązania w tym zakresie?

Dr Wojciech Wiewiórowski: Przede wszystkim trzeba pamiętać, że same sklepy inter-

Zdjęcia: Prevent Magazine

netowe i konstrukcja oferowanych przez nie usług bardzo różnią się między poszczególnymi sklepami. W związku z tym trudno jest wydać jeden rodzaj zaleceń, które skierowane byłyby do wszystkich podmiotów będących e-sklepami bądź wykonującymi „sklepopodobne" działania. Przecież serwis aukcyjny to też pewnego rodzaju sklep. Serwis, który nastawia się na promocję muzyki danego zespołu, też może być sklepem, o ile prowadzi sprzedaż nagrań zespołu lub związanych z nim gadżetów. Zatem e-sklepy mogą bardzo się od siebie różnić, podobnie jak zestaw zbieranych przez nie danych. Jeżeli weźmiemy pod uwagę, że sklepy internetowe sprzedają czasem sprzęt medyczny, może się okazać, że część danych, które na te potrzeby pozyskują od swoich klientów, ma charakter danych wrażliwych, podlegających szczególnej ochronie.
To utrudnia operowanie danymi i wymaga stosowania dodatkowych zabezpieczeń. Wskazania, które zostały zawarte w rozporządzeniu z 2004 r., zdaniem zarówno rynku, jak i Generalnego Inspektora są przestarzałe. Dlatego mamy zamiar dokonać zmiany tego aktu prawnego. W tej chwili zespół utworzony na zewnątrz Biura Generalnego Inspektora Ochrony Danych Osobowych opracowuje stosowną propozycję. Przy czym nie będzie to odświeżenie przepisów z 2004 r., lecz nowe spojrzenie na kwestie stosowania właściwych zabezpieczeń. Warto bowiem przeanalizować, czy rzeczywiście powinny one przesądzać, że hasło służące do uwierzytelniania użytkowników w systemie informatycznym powinno mieć minimum 6 znaków i być zmieniane nie rzadziej niż co 30 dni, czy też może powinny odwoływać się do pewnego rodzaju norm, standardów czy formalnych specyfikacji, które na rynku istnieją. Przecież wiele instytucji dokonuje oceny ryzyka choćby według pewnego rodzaju schematów przyjętych przez międzynarodowe organizacje zajmujące się audytem systemów teleinformatycznych lub stosuje się do ustaleń zawartych w Polskich Normach albo w normach przyjętych przez inne organizacje standaryzacyjne. Chodzi więc raczej o ponowne przemyślenie, na czym polega bezpieczeństwo informacji Anno Domini 2013, a nie odświeżenie rozporządzenia Anno Domini 2004.

Redakcja: Kiedy można się spodziewać wyników tych prac?
Dr Wojciech Wiewiórowski: Chciałbym, żeby w styczniu bądź lutym 2013 roku propozycja takiego rozwiązania została poddana konsultacjom środowiskowym. Proszę pamiętać, że Generalny Inspektor Ochrony Danych Osobowych nie ma inicjatywy ustawodawczej. W jego kompetencjach nie leży też wydawanie rozporządzeń. Z pewnością takie rozporządzenie powinno być wydane przez ministra właściwego do spraw administracji, bo to on jest w tej chwili za nie odpowiedzialny. Jednak zanim Ministerstwo Administracji i Cyfryzacji zacznie je przygotowywać, chcemy przeprowadzić dyskusję środowiskową w tej sprawie. Niemniej wiemy, że samo Ministerstwo zdaje sobie sprawę, że wypracowanie tego typu rozwiązania w 2013 r. jest konieczne.

Redakcja: Optymistycznie patrząc – czy koniec 2013 roku jest terminem realnym?
Dr Wojciech Wiewiórowski: Bardzo trudno jest przewidywać tempo procesu legislacyjnego, zwłaszcza gdy przygotowywane zmiany nie są wymuszone np. stanowiskiem Komisji Europejskiej czy jakimś skandalem. Bardzo dobrze kwestię tę obrazuje tempo prac nad zmianą ustawy o świadczeniu usług drogą elektroniczną. Zostały one rozpoczęte w roku 2009, gdy jeszcze pracowałem w Ministerstwie Spraw Wewnętrznych i Administracji. Wiedzieliśmy, że dokonanie zmian jest potrzebne, ale ich przygotowywanie rozpoczęliśmy właśnie od konsultacji społecznych. Jednocześnie byliśmy ciekawi, jak długo będą trwały te prace. Jak wspomniałem, gdy je rozpoczynaliśmy, była wiosna 2009 r. Obecnie mamy początek roku 2013 i, według mojej wiedzy, rząd jest w tej chwili przygotowany, żeby przyjąć ostateczną wersję projektu ustawy.

Redakcja: Czy rok 2013 będzie rokiem wiążącym?

Dr Wojciech Wiewiórowski: Myślę że tak, bowiem powszechne jest przekonanie, iż obecne rozwiązania są przestarzałe. Poza tym fakt, że eksperci na zewnątrz Biura GIODO wykonali pewną pracę, pozwoli nam w 2013 roku rzeczywiście ruszyć z pracami w sposób zorganizowany i szybki.

Redakcja: Wracając do obowiązków sklepów internetowych, czy mógłby Pan Minister wskazać, które z prowadzonych przez siebie zbiorów danych powinny one rejestrować, a które nie?

Dr Wojciech Wiewiórowski: Z pewnością do rejestracji należy zgłaszać zbiory, które zawierają dane osobowe wykorzystywane w celach marketingowych, na potrzeby prowadzenia różnego rodzaju akcji lojalnościowych albo do utrzymywania kontaktów z klientami. Przy okazji warto wspomnieć, o czym właściciele sklepów internetowych nie zawsze wiedzą, że niekiedy adres mailowy może mieć charakter danych osobowych. Jeśli jego częścią jest np. imię i nazwisko, już wówczas może być uznany za dane osobowe, a już tym bardziej, gdy w dalszej jego części pojawia się np. nazwa konkretnej firmy czy instytucji. Jeżeli w adresie mailowym pojawia się fraza „Wojciech Wiewiórowski" powiązana choćby z nazwą Uniwersytetu Gdańskiego, którego jestem pracownikiem naukowym, to wiadomo, że jest to informacja dotycząca konkretnej osoby, możliwej do zidentyfikowania bez większego problemu.

Redakcja: Jeśli już jesteśmy przy temacie marketingu, to kontrowersje budzi łączenie zgody na przetwarzanie danych osobowych w celach marketingowych ze zgodą na otrzymywanie informacji handlowych drogą elektroniczną.

Dr Wojciech Wiewiórowski: Są to dwie różne zgody, których pozyskiwanie wynika z dwóch różnych podstaw prawnych. Konieczność pozyskiwania zgody na otrzymywanie informacji handlowych drogą elektroniczną wynika z ustawy o świadczeniu usług drogą elektroniczną. Z kolei w określonych sytuacjach, kiedy dane osobowe naszych klientów chcemy wykorzystywać w celach marketingowych, to na takie działanie musimy pozyskać ich zgodę wyrażoną na podstawie ustawy o ochronie danych osobowych. I choć obie wymienione ustawy przewidują, że zgody nie można domniemywać z oświadczenia woli o innej treści, to jednak przesyłanie informacji handlowych drogą elektroniczną jest innym działaniem niż wykorzystywanie danych osobowych w celach marketingowych. Proszę pamiętać, że możemy przesyłać informację handlową do osób, które nie są zidentyfikowane jako osoby fizyczne i odwrotnie, możemy identyfikować osoby fizyczne i nie chcieć przekazywać im informacji handlowych drogą elektroniczną. Należy więc odróżniać przepisy antyspamowe od przepisów związanych z ochroną danych osobowych. Przy okazji chciałbym podkreślić, że rejestracja zbiorów danych osobowych przestała być czynnością trudną. Dowodzi tego m.in. liczba zbiorów zgłaszanych w tej chwili do rejestracji GIODO, która wzrosła szczególnie od czasu, gdy wprowadzona została możliwość dokonywanie tej czynności drogą elektroniczną. Wkrótce nie będzie nawet konieczne wysyłanie wersji papierowej zgłoszenia, jeżeli korzystać będziemy z podpisu weryfikowanego za pomocą profilu w ePUAP. Jednocześnie dzięki udostępnieniu na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych odpowiednich formularzy, zawierających system podpowiedzi i wymuszających podanie określonych informacji, coraz rzadziej mamy do czynienia z sytuacją, gdy trzeba prowadzić postępowanie polegające na uzupełnieniu braków formalnych zgłoszeń. To, oczywiście, cieszy, ale

Niekiedy adres mailowy może mieć charakter danych osobowych – jeśli jego częścią jest np. imię i nazwisko, a tym bardziej gdy dodatkowo pojawia się nazwa konkretnej firmy.

bez wątpienia spowodowało znaczący wzrost liczby zgłaszanych do rejestracji zbiorów - jeszcze dwa-trzy lata temu wpływało ich rocznie 8-9 tys., a w roku 2012 liczba ta wzrosła do prawie 20 tys. Wzrost jest zatem prawie dwukrotny.
To dowodzi m.in. tego, jak wiele zbiorów nie było do tej pory zgłaszanych do rejestracji. Podejmujemy działania edukacyjne w tym zakresie, biorąc pod uwagę m.in. fakt, że dopełnianie obowiązku zgłoszenia zbioru danych do rejestracji wymaga jednocześnie dokonania przemyśleń dotyczących bezpieczeństwa systemu teleinformatycznego, który jest przez nas wykorzystywany.

Redakcja: Sklepy internetowe bardzo często korzystają z Allegro. Mają tam swoje profile. Robiąc zakupy w sklepie internetowym dostępnym za pośrednictwem Allegro, spotkaliśmy się z praktyką, że sklep, wykorzystując dane z Allegro, zakłada konto bezpośrednio w swoim sklepie, który jest odrębną stroną internetową od Allegro. Czy taka praktyka jest zgodna z prawem?
Dr Wojciech Wiewiórowski:
Musiałbym przeanalizować konkretny przypadek, by powiedzieć, czy określona praktyka stosowana przez dany podmiot jest zgodna z prawem, czy nie. Proszę pamiętać, że inaczej sytuacja będzie wyglądała w przypadku, w którym rzeczywiście przetwarzamy dane osobowe, czyli dane konkretnej osoby, która tworzy swoje konto indywidualne, a inaczej, gdy tworzone jest konto firmowe, a przetwarzane dane nie dotyczą konkretnej osoby fizycznej, lecz firmy. Również nie do końca wiem, na czym polega wykorzystywanie danych z Allegro i jakie są to dane. To, że ktoś wykorzystuje możliwości logowania się za pomocą dostarczonego z zewnątrz urządzenia, tak jak logujemy się czasem za pomocą narzędzi pochodzących z różnych serwisów społecznościowych, nie oznacza jeszcze, że mamy do czynienia z przenikaniem danych pomiędzy serwisami. Raczej wykorzystujemy usługę jednego podmiotu do zrealizowania jakiegoś innego działania. Nie jestem w stanie udzielić odpowiedzi wspólnej dla wszystkich przypadków, które mogą mieć miejsce.

Redakcja: Jak traktować dane, które uzyskują sprzedawcy na Allegro? Czy są to dane sklepów, czy też dane Allegro? Ludzie zakładają konto na Allegro, wśród tych kont mamy również konta sklepowe i użytkownik kupuje bezpośrednio w sklepie, czyli sklep za pośrednictwem Allegro ma dostęp do danych. Czy ten stan można traktować jako powierzenie przetwarzania danych?
Dr Wojciech Wiewiórowski:
Kluczowa w tym przypadku jest odpowiedź na pytanie, kto decyduje o celach i środkach przetwarzania danych. Jeżeli o celach przetwarzania danych decyduje sklep, który znajduje się poza Allegro, to nie ma najmniejszej wątpliwości, że powstał odrębny zbiór danych. To, że te dane są pozyskiwane z miejsca publicznie dostępnego, nie oznacza, że tracą one charakter danych osobowych. Możemy mieć najwyżej podstawę uprawniającą nas do ich przetwarzania. Jednak jeśli stworzyliśmy odrębny zbiór danych, musimy dopełnić m.in. tzw. obowiązku informacyjnego wobec osoby, której dane zebraliśmy i przetwarzamy.

Redakcja: Częstą praktyką jest logowanie się przez Facebook i problemem jest dopełnienie tego obowiązku. Czy mógłby Pan coś zalecić w tym zakresie firmom, które stosują tego typu rozwiązania?
Dr Wojciech Wiewiórowski:
Przede wszystkim powiem, że obowiązek informacyjny jest obowiązkiem wynikającym z polskiego prawa i jeżeli ktoś ma kłopoty z jego spełnieniem, nie oznacza, że się go pozbył. Dlatego nie podejmujmy działań, które spowodują, że nie będziemy w stanie spełnić obowiązku wynikającego z ustawy.

Redakcja: Przejdźmy do tematu nowelizacji ustawy o ochronie danych osobowych w kontekście funkcji ABI. Czy te działania są już bardziej zaawansowane? Różne informacje można znaleźć na ten temat w Internecie…

Dr Wojciech Wiewiórowski: Wedle mojej wiedzy, z dużego pakietu deregulacyjnego, który został przygotowany w Ministerstwie Gospodarki, do dalszego procedowania wybrano jedynie część przepisów. Wśród nich nie znalazły się te dotyczące administratora bezpieczeństwa informacji (ABI). Po części ze względu na to, że zaczęły być torpedowane przez niektóre środowiska biznesowe. W tej chwili są przedmiotem dalszych rozważań w Ministerstwie Gospodarki i mają być uwzględnione w kolejnym pakiecie deregulacyjnym. Trudno mi zrozumieć argumenty tej grupy, która nie chce wprowadzenia tych przepisów do ustawy, zważywszy że są one alternatywne, a więc można zostać przy dzisiejszym systemie albo wprowadzić rozwiązania, które są proponowane w pakiecie deregulacyjnym. Jeśli jednak biznes nie jest w stanie porozumieć się w tej kwestii, pewnie na razie obowiązywać będą dotychczasowe unormowania.

Redakcja: Ponadto jest też cień rozporządzenia europejskiego, które gdzieś się czai.

Dr Wojciech Wiewiórowski: Co do unijnego rozporządzenia to faktycznie należy przypuszczać, że w roku 2014, w tej czy innej formie, jednak się pojawi. Znajdą się w nim również przepisy dotyczące inspektorów ochrony danych, czyli odpowiedników naszych administratorów bezpieczeństwa informacji.

Redakcja: Czy są szanse na to, że za jakiś czas informacje o osobach fizycznych prowadzących działalność gospodarczą zostaną wyłączone spod reżimu ustawy o ochronie danych osobowych, tak jak to miało miejsce przed 1 stycznia 2012 r., a więc gdy funkcjonowała ustawa Prawo działalności gospodarczej? Słyszałem informację, może plotkę, że trwają prace mające na celu przywrócenie stanu poprzedniego.

Dr Wojciech Wiewiórowski: Ja również ze strony Ministerstwa Gospodarki słyszałem informację, że taka zmiana jest planowana. My przeciwko niej nie oponujemy, bo stanowisko GIODO od początku istnienia urzędu było takie, że dane osobowe przedsiębiorców mogą podlegać innej regulacji niż klasyczne dane osobowe. Z drugiej strony mogę powiedzieć, że od 1 stycznia 2012 r. przedsiębiorcy przestali być traktowani jako obywatele drugiej kategorii i traktowani są tak jak każdy obywatel w tym kraju. Niemniej jeśli Ministerstwo Gospodarki uważa, że dobrym rozwiązaniem jest przywrócenie poprzedniego rozwiązania, nie będziemy tego utrudniać.

Redakcja: Czy takie rozwiązania zostały przyjęte w innych państwach Unii Europejskiej – że jednoosobowa działalność gospodarcza jest chroniona tamtejszymi przepisami o ochronie danych osobowych. Czy Pan Minister ma taką wiedzę?

Dr Wojciech Wiewiórowski: Są kraje, w których dane osób prowadzących działalność gospodarczą podlegają ochronie jak dane osobowe. Niemniej są też kraje, w których zakres swobody przetwarzania danych, które znajdują się w obrocie gospodarczym, jest jeszcze większy niż w Polsce. Na przykład w niektórych państwach dane dotyczące rozliczeń podatkowych, nawet osób fizycznych, są danymi, które są powszechnie możliwe do przetwarzania. W tym zakresie wciąż istnieją bardzo duże różnice między krajami członkowskimi UE.

Redakcja: Dlaczego w ogóle warto interesować się tematem Dnia Ochrony Danych Osobowych? Czy warto przyjść na takie spotkanie?

Dr Wojciech Wiewiórowski: W czasie Dnia Ochrony Danych Osobowych zawsze organizujemy dużą konferencję, która jest poświęcona jakiemuś zagadnieniu, które będzie bardzo ważne w danym roku kalendarzowym. Tak było z retencją danych telekomunikacyjnych dwa lata temu. Tak było w zeszłym roku, jeśli chodzi o rejestry publiczne. W tym roku jako temat wybraliśmy dane osobowe w ochronie zdrowia i w badaniach klinicznych, uznając, że choć większość rozwiązań prawnych w tym zakresie przyjęto w roku 2011 i 2012, to jednak w roku 2013 i 2014 zaczną one obowiązywać w praktyce. W 2013 roku zostaną bowiem zbudowane systemy teleinfor-

matyczne, które będą wykorzystywane do przetwarzania danych medycznych. Wydaje mi się, że zarówno z punktu widzenia pacjenta, jak i z punktu widzenia tego, który udziela świadczeń medycznych, a więc lekarza, pielęgniarki, położnej czy w końcu placówki ochrony zdrowia, to, jak będą przetwarzane dane medyczne i do jakich danych medycznych będziemy mieli dostęp, jest kluczowe. Kwestia ta jest też kluczowa dla biznesu. Zarówno ze względu na konieczność stworzenia systemów teleinformatycznych dla sektora ochrony zdrowia, jak i ze względu na możliwość wtórnego wykorzystywania danych. W tym kontekście istotne jest pytanie, czy nowe przepisy w tym zakresie są wystarczającą gwarancją, że nasze dane osobowe nie dostaną się w ręce osób niepowołanych lub nieupoważnionych, np. ubezpieczycieli, pracodawców albo banków, a więc podmiotów, które niejednokrotnie chciałyby uzyskać dane o stanie zdrowia konkretnych osób. Prawo, niestety, nie zawsze jest ono doskonałe. Dla przykładu – mamy w tej chwili dwa rozwiązania prawne dotyczące przechowywania dokumentacji medycznej wytworzonej przez podmioty, które kończą praktykę lekarską, i trzecie, które jest stosowane w praktyce. Z jednego aktu wynika, że podmiot rozpoczynający działalność ma określić, gdzie będą przechowywane dokumenty po zakończeniu jego działalności, podczas gdy z innego aktu wynika, że mają one trafiać do systemu informacji medycznej. Z kolei w praktyce dokumenty te są po prostu przekazywane izbie lekarskiej, co może zresztą jest rozsądnym rozwiązaniem, tyle że działanie takie odbywa się bez podstawy prawnej. Jest zatem wiele pytań, na które musimy obecnie odpowiedzieć, pamiętając, że przyjęte rozwiązania będą obowiązywać zapewne przez kolejnych kilkanaście lat.

Redakcja: Jakie wyzwania stoją przed GIODO na najbliższe lata? Czy jest wśród nich coś szczególnego?

Dr Wojciech Wiewiórowski: Oczywiście wyzwań jest mnóstwo. Część z nich już wymieniliśmy, ale do tej listy dodałbym konieczność stworzenia ustawy o wideomonitoringu, o co zabiegam od dawna, deklarując aktywne uczestnictwo w jej przygotowaniu. Wciąż brak jest uregulowań prawnych jeśli chodzi o dane biometryczne i biobankowanie. Wyzwaniem jest stworzenie właściwych przepisów regulujących zasady funkcjonowania tzw. inteligentnych sieci energetycznych i inteligentnych liczników. To są wszystko wyzwania prawne, które przed nami stoją, ale dołóżmy do tego również fakt, że zwiększa się świadomość społeczna, jeśli chodzi o kwestie związane z ochroną danych osobowych, co powoduje, że nie tylko wzrasta liczba zbiorów zgłaszanych do rejestracji, o czym już wspominałem, ale znacząco rośnie również liczba skarg kierowanych do GIODO – w ciągu ostatnich dwóch lat zwiększyła się prawie dwukrotnie. To świadczy o tym, że coraz więcej osób zdaje sobie sprawę, jakie niebezpieczeństwa są związane z brakiem właściwej ochrony danych osobowych. Truizmem będzie wspominanie, że rozwój serwisów społecznościowych czy innych serwisów informatycznych wywołuje nie tylko konieczność nowego podejścia do ochrony danych w Internecie, ale również konieczność zastanowienia się nad tym, jakie niebezpieczeństwa na przyszłość rodzą zdarzenia, które dziś wydają nam się tylko drobnymi zmianami w oprogramowaniu czy w kształcie serwisu. ■

Rozmawiał: Michał Sztąberek