Wywiad z Generalnym Inspektorem z okazji Dnia Ochrony Danych Osobowych - rozmawia Jarosław Malec, Memex.pl (Warszawa, 2 luty 2007 r.)

Witam serdecznie Pana Generalnego Inspektora. Na początku chciałbym zapytać o Dzień Ochrony Danych Osobowych (28 stycznia). Trudno ukryć, że w Polsce jest to mało znana data. Z czym wiąże się ta data, jaki jest jej rodowód?

O ustanowieniu dnia 28 stycznia świętem ochrony danych osobowych zdecydował Komitet Ministrów Rady Europy. W tym dniu obchodzona jest rocznica otwarcia do podpisu konwencji 108 Rady Europy z dnia 28 stycznia 1981r. w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych. Konwencja ta jest najstarszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych. Celem konwencji jest zapewnienie, na obszarze państw członkowskich, każdemu - niezależnie od obywatelstwa i zamieszkania - ochrony jego praw i wolności, a w szczególności prawa do poszanowania sfery osobistej, w związku z automatycznym przetwarzaniem danych osobowych. Jednocześnie konwencja nałożyła na kraje członkowskie zobowiązanie do stworzenia ustawodawstwa w zakresie ochrony danych osobowych i wyznaczyła kierunki, w jakich ustawodawstwo to ma zmierzać. Niejednolitość tych ustawodawstw spowodowała, że Unia Europejska, która postulowała początkowo jedynie ratyfikowanie konwencji przez państwa członkowskie, rozpoczęła prace nad dyrektywą 95/46/WE Parlamentu Europejskiego i Rady, która stała się z kolei wzorem wszystkich ustawodastw o ochronie danych w państwach należących do UE.

Wiele mówi się o polskiej ustawie o ochronie danych osobowych, jako ustawie dosyć restrykcyjnej w porównaniu z ustawami w innych krajach europejskich np. niemieckiej. Jak Pan sądzi, czy rzeczywiście nasza ustawa na taką opinię zasługuje?

Jak już wspomniałem, wszystkie europejskie ustawy są wzorowane na tej samej dyrektywie 95/46/WE Parlamentu Europejskiego i Rady. Jej zadaniem było zapewnienie minimalnego, a zarazem jednolitego dla państw członkowskich poziomu ochrony danym osobowym gromadzonym w zbiorach oraz zapewnienie swobodnego przepływu danych osobowych pomiędzy krajami członkowskimi. Zrealizowanie tego drugiego zadania było koniecznym warunkiem zapewnienia swobodnego przepływu towarów, usług i osób pomiędzy krajami Wspólnoty, co każdorazowo łączy się z koniecznością przekazania danych osobowych. Na pewno zasady ochrony danych i te minimalne gwarancje są podobne w krajach Unii, a przyjmowanie bardziej restrykcyjnych rozwiązań nie byłoby racjonalne, chociażby dlatego, że korzystając ze swobodnego przepływu danych na terytorium UE, zbyt łatwo byłoby te restrykcyjne przepisy omijać. Natomiast, co do porównania z innymi krajami, to generalnie nie uważam, aby polska ustawa była bardziej restrykcyjna od innych, np. niemieckiej. Ale na to pytanie nie ma tak naprawdę ogólnej odpowiedzi, bo trudno byłoby przyjąć jakieś ogólne kryterium takiej oceny. Spotykamy się z różnymi modelami ochrony danych więc trzeba byłoby analizować poszczególne elementy rozwiązań wprowadzonych w różnych krajach i tylko tym sposobem dokonać jakichkolwiek porównań. Na przykład w niektórych krajach ochroną objęte są dane o podmiotach prowadzących działalność gospodarczą (np. Dania, Austria). W Polsce, podobnie jak w Belgii czy Wielkiej Brytanii - nie. Każdy taki czynnik należałoby analizować odrębnie, nie zapominając o ustawodastwach krajowych, do których przepisy o ochronie danych odsyłają.

Jak ocenia Pan praktyczne przygotowanie urzędów państwowych w zakresie ochrony danych osobowych? Czy polskie urzędy dysponują odpowiednimi środkami do zabezpieczenia naszych danych osobowych?

Zadaniem każdego administratora danych jest, zgodnie z art. 36 ustawy o ochronie danych osobowych, zastosowanie takich środków organizacyjnych i technicznych, aby zapewnić ochronę danych osobowych, w zależności od zagrożeń oraz kategorii danych objętych ochroną. Dobór tych środków to kwestia zależna od administratora. Kontrole wykazują, że ciągle jest jeszcze problem z doborem tych środków lub niektóre z wymaganych zabezpieczeń nie są w ogóle stosowane. Z ustaleń kontroli wynika, że błędami najczęściej popełnianymi przez podmioty publiczne jest brak wymaganej dokumentacji np. polityki bezpieczeństwa; brak mechanizmów kontroli dostępu do

danych; nie zapewnianie przez systemy informatyczne odnotowania daty wprowadzenia danych do systemu, brak identyfikatora użytkownika; nieprawidłowe prowadzenie ewidencji osób upoważnionych. Kontrole wykazują też, że wbrew takiemu obowiązkowi nie są zgłaszane zbiory danych do rejestracji.

Wiemy, jak duże znaczenie odgrywa dzisiaj informacja i dostęp do niej w sferze biznesu. Dla wielu firm fakt posiadania bazy danych, jej przetwarzania to podstawa uzyskania przewagi konkurencyjnej, często to nawet sprawa "być albo nie być" na rynku. W wyścigu rynkowym firm pojawiają się zapewne zagrożenia związane z uchybieniami w sferze odpowiedniego zabezpieczenia baz danych. Na co przede wszystkim szczególnie powinny zwrócić uwagę firmy posiadające dane osobowe?

Myślę, że w zakresie zabezpieczenia nie ma normy, której trzeba szczególnie przestrzegać. Należy rzetelnie spełnić wszystkie wymagania określone w art. 36 - 39 ustawy o ochronie danych osobowych oraz w przepisach rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
Administrator musi zastosować środki techniczne i organizacyjne zapewniające ochronę danym osobowym. Te środki powinny być adekwatne do stopnia zagrożenia oraz kategorii danych, aby zabezpieczały dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem, zmianą, utratą, uszkodzeniem lub zniszczeniem. Musi też opisać zastosowane środki w dokumentacji, na którą składa się w szczególności polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym. Obowiązkiem jest również wyznaczenie administratora bezpieczeństwa informacji, który powinien czuwać nad całokształtem spraw związanych z bezpieczeństwem danych nadzorować systematycznie proces przetwarzania danych. Z przepisów ustawy wynika także konieczność zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Kolejnym obowiązkiem jest wydanie wszystkim osobom uczestniczącym w procesie przetwarzania danych upoważnień, w których należy wskazać: komu i na jaki okres zostało wydane, a przede wszystkim do jakiego zbioru dana osoba ma dostęp i w jakim zakresie z danych może korzystać. Te upoważnienia powinny zostać ewidencjonowane.

W Polsce istnieje ponad 400.000 podmiotów gospodarczych, z których zdecydowana większość przetwarza dane osobowe, natomiast oficjalnie zarejestrowanych zbiorów i zgłoszonych do rejestracji jest ok. 92.000. Czy w Polsce istnieje "szara strefa" przetwarzania danych osobowych?

Należy pamiętać o tym, że znaczna ilość zbiorów z obowiązku rejestracji jest zwolniona. Przypadki zwolnienia wymienia art. 43 ustawy o ochronie danych osobowych i jest ich, aż 11. Natomiast, gdybym posiadł wiedzę o "szarej strefie" natychmiast bym zainterweniował, chociażby poprzez kontrolę.

Jaki był rok 2006 dla Generalnego Inspektora Ochrony Danych Osobowych - "cienie i blaski" minionego roku?

Początkowy okres mojego urzędowania to był przede wszystkim okres poznawania instytucji, problemów oraz wypracowywania koncepcji na przyszłość.
A jakie wnioski? Wydaje mi się, że największym problemem jest w chwili obecnej mała świadomość społeczeństwa o ochronie danych osobowych, mała wiedza osób o ich prawach. Lepiej jest na poziomie urzędów centralnych, dużych korporacji czy dużych firm. Mam wrażenie, że wpływa mniej skarg na działalność firm marketingowych oraz sygnałów o niewłaściwym zabezpieczeniu danych, niż przed laty.
Postanowiłem postawić na edukację. Bardzo dobrą okazją, ku temu był Dzień Ochrony Danych Osobowych. Mam nadzieję, że w ramach imprez zorganizowanych przy okazji obchodów Dnia z informacją udało się dotrzeć do szerokich kręgów społeczeństwa, zarówno w Polsce, jak i za granicą. Informacje na temat ochrony danych osobowych pojawiły się w prasie papierowej, radiu oraz telewizji. We współpracy z Wyższą Szkołą Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego zorganizowaliśmy z okazji Dnia Ochrony Danych Konferencję, która ma być początkiem naszej współpracy z uczelnią. Brakuje bowiem edukacji o ochronie danych osobowych

na poziomie uczelni wyższych, szkół. Problemem wydaje mi się też to, że często urzędnicy samorządowi używają określenia "ustawa o ochronie danych osobowych" do odmówienia dostępu do informacji. Działanie takie jest niezgodne z prawem i trzeba z nim walczyć. Opracowaliśmy publikację na temat ochrony danych "ABC ochrony danych" skierowaną przede wszystkim do podmiotów publicznych. Planuję też podobne publikacje w przyszłości.
Uważam też, że Generalny Inspektor, wskutek umarzania przez prokuratury postępowań w sprawach o naruszenie prawa do ochrony danych osobowych, nie dysponuje wystarczającymi instrumentami służącymi egzekwowaniu przestrzegania ustawy. Ten problem mam nadzieje rozwiązać przy najbliższej nowelizacji ustawy o ochronie danych osobowych.

Czy czekają nas zatem w 2007 roku jakieś zmiany w zakresie ochrony danych osobowych?

Obecnie rozpoczynamy prace nad nowelizacją, ale dopiero na poziomie Biura. To jeszcze długa droga do wprowadzenia zmian, nie sądzę zatem, aby udało się znowelizować przepisy w 2007 r.