Edukacja przede wszystkim

WYWIAD | Czy adres IP jest daną osobową? Jak chronić dane osobowe petentów? Kto powinien pełnić w urzędzie funkcję ABI? Rozmawiamy z **Michałem Serzyckim**, Generalnym Inspektorem Ochrony Danych Osobowych.

FOT. M. KAŁUŻYNSKA-JASAK

IT w Administracji: ***Praktycznie każdy urząd przetwarza dane osobowe. Czy polskie urzędy dobrze chronią dane osobowe?***

Michał Serzycki: Sytuacja nie jest jeszcze idealna. Ogólnie można powiedzieć, że sektor prywatny lepiej chroni dane osobowe. Sektor publiczny cały czas stara się mu dorównać, a my próbujemy mu w tym pomóc, przeprowadzając bardzo dużo szkoleń w urzędach centralnych i samorządowych. Na pewno jest lepiej niż dawniej i warto pochwalić urzędników za chęć pogłębiania wiedzy na temat ochrony danych osobowych, ale nie osiągnęliśmy jeszcze stanu, który mógłby w pełni zadowalać.

Informatyzacja działalności urzędów jest procesem, który będzie nieuchronnie postępował. W jaki sposób zastosowanie technologii informatycznych wpłynęło na zagrożenia związane z przetwarzaniem danych osobowych?

M.S.: Informatyzacja jest wyzwaniem: z jednej strony pomaga w codziennym życiu, zarówno petentom, jak i urzędnikom, ale z drugiej powoduje także zagrożenia w dziedzinie ochrony danych osobowych i prywatności. Doświadczenia innych krajów pokazują już od jakiegoś czasu, że informatyzacja znacząco zwiększa zagrożenia dla bezpieczeństwa danych osobowych. Skalę zagrożeń doskonale obrazuje przypadek brytyjski, w którym urzędnik na zewnętrznym nośniku pamięci miał całą bazę danych wszystkich rekrutów Zjednoczonego Królestwa i… po prostu zostawił ją w pubie.

Sieci komputerowe wielu jednostek administracji są wprost kopalnią danych osobowych, dostępnych dla każdego za pośrednictwem popularnych wyszukiwarek internetowych. W jaki sposób GIODO stara się zapobiegać takim zjawiskom?

M.S.: Najważniejsza jest edukacja. Same przepisy, jeśli nie będziemy ich znali, nic nie dadzą, będą po prostu martwe. Stawiamy więc na edukację, na szerzenie informacji o ochronie danych osobowych. Dotyczy to obu stron: zawsze powtarzam, że jako osoba obsługiwana w urzędzie mam prawo pytać się o ochronę danych osobowych, a z drugiej strony jako urzędnik muszę wiedzieć, jak ważne są to kwestie i jak postępować, by dane należycie zabezpieczać. Na szczęście, jak pokazują badania, świadomość wagi zagadnień związanych z ochroną danych osobowych rośnie. W badaniach Eurobarometru z 2006 roku świadomość polskiego społeczeństwa plasowała się w okolicach 20. miejsca w Unii Europejskiej, ale już w 2008 roku znaleźliśmy się na pierwszym miejscu.

Podejmując decyzję o kontroli konkretnej placówki, GIODO kieruje się własną inicjatywą lub planem czy korzysta z informacji o nieprawidłowościach nadsyłanych do biura GIODO?

M.S.: Mamy system mieszany. Z jednej strony są tzw. kontrole doraźne, czyli te, które wynikają z otrzymania konkretnych informacji – od osób fizycznych czy na przykład z prasy. Mamy także plan kontroli, według którego sprawdzamy poszczególne sektory – w zeszłym roku kontrolowaliśmy na przykład szkoły i firmy turystyczne.

W jaki sposób urzędowy informatyk, zauważywszy błędy w przetwarzaniu danych osobowych w swojej placówce, powinien zareagować? Na drodze służbowej, wewnątrz swojej jednostki, czy też może zwrócić się bezpośrednio do GIODO?

M.S.: Najszybciej by było, gdyby taka osoba zwróciła się do swojego przełożonego, wskazała mu, gdzie są nieprawidłowości, i zasugerowała, że powinny zostać usunięte. Ale może się np. zdarzyć, że przełożeni nie widzą problemu, są głusi na takie wskazówki – wtedy oczywiście można złożyć skargę bezpośrednio do GIODO.

Warto w tym miejscu podkreślić, że moim celem jako Generalnego Inspektora Ochrony Danych Osobowych nie jest łapanie kogokolwiek i udowadnianie, że naruszył prawo. Zależy mi na tym, żeby prawo było przestrzegane. M.in. dlatego najczęściej uprzedzamy o kontroli i jej zakresie. Jeśli więc firma lub urząd w ciągu dwóch tygodni od zawiadomienia o kontroli usunie wszystkie nieprawidłowości, to i tak najważniejszy cel został osiągnięty: dane zaczną być przetwarzane zgodnie z prawem. Choć naturalnie zdarzają się też sytuacje, w których przeprowadzamy niezapowiedziane kontrole, ale dotyczą one spraw doraźnych lub ewidentnych przypadków naruszenia prawa.

Administratorzy witryn urzędowych stają przed problemem: czy adres IP jest daną osobową? Czy wszystkie zbiory danych osobowych, zbierane w wyniku działalności internetowej, wymagają rejestracji? Czy np. wpisy w logu systemowym serwera WWW są bazą danych osobowych?

M.S.: Trzeba pamiętać, że definicja danych osobowych w ustawie o ochronie danych osobowych jest definicją otwartą. To znaczy, że ona cały czas ewoluuje. Kiedyś adres IP komputera czy pliki cookie nie były uznawane za dane osobowe, ale teraz uważamy, że mogą one stanowić dane osobowe. Jest wiele sytuacji, kiedy adres IP nie jest daną osobową, natomiast rozwój technologii spowodował, że liczba takich przypadków maleje.

Rejestracja zbiorów danych to kolejny problem. Obliczyliśmy, że firm działających w Internecie, które przetwarzają dane osobowe, a co za tym idzie – mają obowiązek rejestracyjny, jest w Polsce 800 tys. Natomiast Generalny Inspektor Ochrony Danych Osobowych rejestruje rocznie od trzech do czterech tysięcy zbiorów danych. Biorąc pod uwagę tę skalę oraz rozwiązania przyjęte przez inne kraje, chcielibyśmy odejść od obowiązku rejestracji danych zwykłych. Zastanawiamy się nad wprowadzeniem takich zmian, zmierzających do poluźnienia obowiązku rejestracji zbiorów danych zwykłych. Powinien on jednak nadal bezwzględnie obowiązywać w przypadku danych szczególnie chronionych (wrażliwych).

Natomiast odnosząc się do Pana pytania o rejestrację zbiorów adresów IP osób, które odwiedzały strony internetowe urzędu, uważam, że nie ma obowiązku zgłaszania ich do rejestracji w GIODO. Zgodnie bowiem z art. 43 ust. 1 pkt 11 ustawy o ochronie danych osobowych z obowiązku rejestracji zbioru danych zwolnieni są administratorzy przetwarzający je w zakresie drobnych, bieżących spraw życia codziennego. Na podstawie tego przepisu nie podlegają obowiązkowi rejestracji zbiory danych mające dla administratora charakter pomocniczy, których zasadniczym celem jest usprawnienie działalności administratora. Można uznać, że taki właśnie charakter ma zbiór adresów IP wszystkich osób, które wchodziły na stronę internetową danego podmiotu, odnotowanych w logu systemowym serwera WWW. Tym samym zbiór ten zwolniony jest z obowiązku rejestracji na podstawie art. 43 ust. 1 pkt 11 ustawy o ochronie danych osobowych.

Wielokrotnie natrafić można było na informacje o nieprawidłowościach przy przetwarzaniu danych osobowych w ZOZ-ach. Czy GIODO współpracuje np. z takimi instytucjami jak Centrum Systemów Informacyjnych Ochrony Zdrowia, wskazując takie kierunki informatyzacji, które pozwolą na jak najlepszą ochronę danych wrażliwych w placówkach służby zdrowia? Na czym taka ewentualna współpraca polega?

M.S.: Niestety, nie mamy takiej współpracy. Przyznaję, przetwarzanie danych osobowych przez sektor medyczny stanowi problem. To sprawa z jednej strony bardzo delikatna, dotycząca danych szczególnie chronionych, czyli danych o stanie zdrowia pacjentów. Ale z drugiej strony trzeba mieć świadomość, że informatyzacja służby zdrowia może przyczynić się do podniesienia jakości usług, np. szybszego niesienia pomocy pacjentom. W tej dziedzinie jest jeszcze wiele do zrobienia.

Z badań dotyczących e-usług realizowanych przez administrację publiczną wynika, że ponad połowa Administratorów Bezpieczeństwa Informacji (ABI) w urzędach to informatycy. Kto modelowo powinien pełnić tę funkcję?

M.S.: Dyskusja na ten temat trwa nie od dzisiaj. Jest to rzeczywiście problem, dlatego że ustawa o ochronie danych osobowych dotyczy sfery zarówno informatycznej, jak i prawnej. Zatem osoba znająca się wyłącznie na prawie, a będąca laikiem, jeśli chodzi o kwestie informatyczne, nie będzie dobrym ABI. I odwrotnie – tylko i wyłącznie informatyk, który nie zna się w ogóle na kwestiach prawnych, również będzie swego rodzaju „niepełnosprawnym" administratorem bezpieczeństwa. Dlatego najlepszym połączeniem byłby ktoś, komu nieobce są i zagadnienia prawne, i informatyczne, ale ze znalezieniem takich fachowców jest rzeczywiście duży problem.

Rozmawiał Marcin Meszczyński

Michał Serzycki jest absolwentem Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego, Policealnego Studium Nauczycielskiego oraz studiów podyplomowych dla kadry kierowniczej administracji w Wyższej Szkole Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego na kierunku zarządzanie w administracji publicznej. Karierę zawodową Michał Serzycki rozpoczął w Państwowym Funduszu Rehabilitacji Osób Niepełnosprawnych. Od grudnia 2002 r. sprawował urząd Zastępcy Burmistrza Dzielnicy Warszawa-Wola. W dniu 13 lipca 2006 r. Michał Serzycki, wybrany przez Sejm RP na stanowisko Generalnego Inspektora Ochrony Danych Osobowych, złożył ślubowanie przed Sejmem i rozpoczął czteroletnią kadencję na tym stanowisku. Od 15 lutego 2010 r. jest wiceprzewodniczącym Grupy Roboczej Art. 29 – niezależnego europejskiego organu doradczego Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności.