

# Legislacja do przodu

**WYWIAD** | O dobrych zmianach związanych z ochroną danych osobowych w minionym roku, ale i niewłaściwych praktykach w tym zakresie, rozmawiamy z **Wojciechem Rafałem Wiewiórowskim**, Generalnym Inspektorem Ochrony Danych Osobowych.

**Dr Wojciech Rafał Wiewiórowski** pełni funkcję Generalnego Inspektora Ochrony Danych Osobowych IV kadencji, został powołany na to stanowisko 25 czerwca 2010 r. Od 2002 r. pracował jako wykładowca w Gdańskiej Wyższej Szkole Administracji, a od 2003 r. sprawował funkcję adiunkta i kierownika Pracowni Informatyki Prawniczej na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego, z którym związany jest od 1995 r. Od 2006 r. pracuje na rzecz administracji publicznej. Pełnił m.in. funkcję doradcy ds. informatyzacji w gabinecie politycznym Ministra Spraw Wewnętrznych i Administracji, a także współprowadzącego Komisji Regulacyjnej ds. Polskiego Autofalicznego Kościoła Prawosławnego. W październiku 2008 r. objął stanowisko dyrektora Departamentu Informatyzacji w Ministerstwie Spraw Wewnętrznych i Administracji. Jest autorem wielu opracowań, publikacji i wykładów z dziedziny ochrony danych osobowych, prawa nowych technologii, informatyzacji oraz informatyki prawniczej. Prywatnie interesuje się historią stosunków politycznych, historią sportu, muzyką (od muzyki średniowiecznej do punk rocka) oraz prekolumbijskimi kulturami Mezoameryki.

*IT w Administracji: Podjęliśmy ostatnio na naszych łamach (IT w Administracji 2010, nr 12) temat nowelizacji ustawy o ochronie danych osobowych (dalej: uodo), która uchyla przepis normujący udostępnianie danych osobowych. Czy zgadza się Pan z obawą autorów artykułu, że brak tego unormowania w systemie prawa utrudni postępowanie administracyjne?*

**Wojciech Rafał Wiewiórowski:** Proszę pamiętać, że projekt ten powstał jeszcze przed objęciem przeze mnie stanowiska Generalnego Inspektora. Oceniając go wówczas zastanawiałem się nad sensownością wyeliminowania przepisu, który przez wiele lat się sprawdzał. Jednak po dokładnej analizie całkowicie zgodziłem się z projektodawcami, że ten przepis jest rozwiązaniem nadmiarowym, które istnieje tylko w Polsce. W innych krajach UE stosuje się podstawowe zasady, które w polskiej ustawie o ochronie danych osobowych są wyrażone przez artykuły 23 i 27 dotyczące dopuszczalności przetwarzania poszczególnych kategorii danych osobowych. Natomiast wprowadzenie rozwiązań zawartych w art. 29 ustawy było swego rodzaju kompromisem politycznym pomiędzy autorami obecnej ustawy, czyli posłami, a twórcami konkurencyjnego projektu przygotowanego w MSWiA. Wydaje mi się, że obowiązujące w Polsce przepisy szczególne i unormowania zawarte w art. 23 i art. 27 uodo są wystarczającą podstawą umożliwiającą uzyskanie dostępu do danych osobowych. Uważam, że wspomniana zmiana nie wprowadza zamieszania, a raczej usuwa nadmiarowe rozwiązanie prawne.

*Wiele emocji wywołuje obecnie kwestia rozwiązań informatycznych wykorzystujących technologie chmury obliczeniowej (tzw. cloud computing), które są już stosowane w sektorze prywatnym. W przypadku przetwarzania danych w chmurze mamy niewątpliwie do czynienia z powierzeniem przetwarzania danych osobowych na podstawie art. 31 uodo. Czy uważa Pan, że powierzenie przetwarzania danych wrażliwych jest dopuszczalne?*

**W.R.W.:** Trzeba przede wszystkim pamiętać o tym, że sam cloud computing jest jedynie swoistym modelem biznesowym czy też zbiorem technik, który



FOR: GIODO

nie modyfikuje generalnych zasad przetwarzania danych osobowych, a co najwyżej skłania do postawienia nowych pytań dotyczących interpretacji przepisów, które już istnieją. Przetwarzanie danych w chmurze jest, oczywiście, dopuszczalne. Istotne przy tym jest jednak to, jakie działania trzeba podjąć, żeby zachować wszystkie zasady ochrony danych osobowych, które wynikają z ustawy.

Oczywiście, usługa ta umożliwia także przetwarzanie danych wrażliwych, o ile spełnione będą wszystkie warunki niezbędne do tego, aby przetwarzanie tego rodzaju danych było zgodne z prawem. Jednym z nich jest wcześniejsze zarejestrowanie zbioru zawierającego dane szczególnie chronione u Generalnego Inspektora Ochrony Danych Osobowych.

Administrator danych, który zamierza przetwarzać dane osobowe w chmurze, musi zawrzeć z jej dostawcą umowę powierzenia przetwarzania danych osobowych w rozumieniu art. 31 uodo. Zgodnie bowiem z tym przepisem administrator danych może powierzyć innemu podmiotowi przetwarzanie danych, ale muszą być spełnione

określone w ustawie warunki. Umowa musi być zawarta na piśmie, określać zakres powierzonych danych i cel ich przetwarzania. Podmiot, któremu administrator powierzył w ten sposób przetwarzanie danych osobowych, może je wykorzystywać wyłącznie w zakresie i celu wskazanym w tej umowie. Oczywiście, skonstruowanie takiej umowy z dostawcą chmury może być skomplikowane z tego powodu, że powinna ona przewidywać, przy użyciu jakich środków dane będą zabezpieczone. Musimy więc uzyskać bardzo dokładną informację na ten temat, a to w przypadku klasycznej chmury publicznej – niemającej ograniczeń co do terytorium ani co do podmiotu podmiotów, w których władaniu pozostają środki techniczne (serwery służące przetwarzaniu danych), może być bardzo trudne. Natomiast w przypadku chmur w ten czy inny sposób dedykowanych danemu użytkownikowi – jak najbardziej możliwe, ale zapewne znacznie droższe.

Jestem sobie w stanie wyobrazić, że mogą istnieć specjalne obwarowania w przypadku powierzenia przetwarzania danych osobowych przez niektóre instytucje publiczne, np. służby specjalne. Natomiast nie ma żadnego generalnego zakazu, który uniemożliwiłby instytucjom publicznym stosowanie wspomnianej technologii.

**Praktyką, która bulwersowała rodziców w całym kraju, było żądanie przez gminy, by ich organom lub dyrektorom przedszkoli – na potrzeby przyjęcia dziecka do placówki – przedkładali oni różnego rodzaju dokumenty, m.in. zaświadczenie ZUS RMUA czy roczne rozliczenie podatkowe PIT. Czy to dopuszczalne?**

**W.R.W.:** Zakres danych, które można zbierać przy rekrutacji do przedszkoli, jest określony w przepisach na poziomie ustawy i rozporządzenia, a okazało się, że jest dość dowolnie rozszerzany w aktach prawnych wydawanych na poziomie gmin. Wśród żądanych dokumentów były m.in. odpisy orzeczeń sądowych w sprawach rodzinnych, rozwodowych czy informacje o wysokości alimentów. Jest to niezgodne z przepisami ustawy o ochronie danych osobowych, które stanowią, że zakres żądanych danych musi być określony na poziomie ustawowym. Nie można tego robić uchwałą rady gminy, a już na pewno nie w zarządzeniach wójta, co się też zdarzało. Szczególnie niedopuszczalna jest sytuacja, w której żąda się przekazywania kopii zaświadczeń zawierających dane medyczne dzieci i rodziców albo dane dotyczące orzeczeń wydanych w postępowaniu sądowym i administracyjnym. Są to dane wrażliwe i jako takie muszą, zgodnie z uodo, podlegać szczególnej ochronie. Oczywiście, wiele gmin próbuje się asekurować, twierdząc, że te informacje zostały pozyskane za zgodą rodziców. Jednak nie mamy tu do czynienia z dobrowolną zgodą,

ponieważ jej brak eliminuje dziecko z procesu rekrutacji. Podsumowując – gminy są postawione w bardzo trudnej sytuacji, ponieważ miejsc w przedszkolach publicznych jest zbyt mało, aby umożliwić dostęp do nich wszystkim dzieciom, muszą więc przeprowadzić „selekcję”. Niestety, robi się to sposobami, które nie są dozwolone przez prawo. Wiedząc, że gminy nie do końca są winne takiemu stanowi rzeczy, postanowiliśmy, poza sytuacjami skrajnymi, nie podejmować działań przeciwko nim. Natomiast w momencie zakończenia procesu przyjmowania do przedszkoli, czyli pod koniec sierpnia 2010 r., nagłośniliśmy problem z nadzieją, że MEN do następnego roku przygotowuje potrzebne rozwiązania prawne. Niestety, jak dotąd ich nie opracowano.

**Poproszę o krótkie podsumowanie 2010 r. Jakiego typu sygnały dotyczące naruszania przepisów o ochronie danych przez urzędy otrzymywał Pan najczęściej? Czego dotyczyły największe naruszenia?**

**W.R.W.:** Podsumowując rok 2010, szczególnie uwagę należałoby zwrócić na kwestie legislacyjne. Po pierwsze, po niemal trzech latach dyskusji zakończono proces nowelizacji uodo. Po drugie, ubiegły rok to również początek kolejnej dyskusji o przepisach dotyczących ochrony danych osobowych i prawa do prywatności. Jest ona bardzo istotna, bo obecna uodo została stworzona jeszcze w czasach przedinternetowych i wymaga dostosowania do nowych wyzwań technologicznych. Po trzecie, jesteśmy też u progu dyskusji o nowelizacji europejskich regulacji dotyczących ochrony danych, zwłaszcza dyrektywy 95/46/WE z 2005 r. o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym ich przepływie. Ta dyskusja dotyczy przede wszystkim ram prawnych, w jakich powinna być osadzona ochrona danych osobowych, tak by zwiększyć ochronę prywatności obywateli przy jednoczesnym poszanowaniu tego, że dane osobowe są towarem swobodnie przepływającym na rynku ogólnoeuropejskim.

Natomiast co do spraw trafiających do GIODO: wzrosła liczba skarg dotyczących przetwarzania danych osobowych za pomocą nowoczesnych technik, przede wszystkim internetowych (przykładem mogą być serwisy społecznościowe). W porównaniu z poprzednimi latami mniej jest skarg dotyczących podmiotów, które zajmują się marketingiem bezpośrednim. Natomiast coraz więcej skarg dotyczy instytucji publicznych, zarówno samorządowych, jak i rządowych, co być może jest związane z większą świadomością obywateli, że również podmioty z tego sektora są zobowiązane do ochrony danych osobowych.

*Rozmawiała Katarzyna Bielińska-Kuniszewska*