Dziennik Gazeta Prawna 13-04-2011

Dane osobowe

Nie wszystkie dane znajdujące się w rejestrach powinny być dostępne w internecie
– mówi dr Wojciech Rafał Wiewiórowski, GIODO | C6

Dziennik Gazeta Prawna 13-04-2011

Nie wszystkie dane znajdujące się w rejestrach powinny być dostępne w internecie

DR WOJCIECH RAFAŁ WIEWIÓROWSKI *Oprócz polityki bezpieczeństwa dokumentu, serwera czy bazy danych potrzebne jest stworzenie w samorządach polityki bezpieczeństwa i zasad zarządzania prywatnością również dla procesu administracyjnego*

Jak jednostki samorządu terytorialnego chronią dane osobowe znajdujące się w rejestrach publicznych?
Sytuacja nie jest zła, choć trudno generalizować, biorąc pod uwagę, że w Polsce działa prawie trzy tysiące jednostek samorządu terytorialnego.
W większości instytucji samorządowych istnieje przekonanie, że ta tematyka jest ważna i zajmuje się nią prawie każdy urzędnik, który wykonując swoją pracę, ma dostęp do zgromadzonych w urzędach danych osobowych. Zawsze oczywiście zdarzają się pewne nieprawidłowości, które wykrywamy w toku naszych inspekcji bądź na podstawie wpływających do generalnego inspektora ochrony danych osobowych skarg. Ogólnie jednak ochrona danych osobowych w samorządach jest zadowalająca.

dr Wojciech Rafał Wiewiórowski
generalny inspektor ochrony danych osobowych

Coraz więcej samorządów stawia na nowoczesne sposoby komunikacji z mieszkańcami, a wiele danych gromadzonych jest również w zbiorach elektronicznych. Na jakie elementy przy takim sposobie gromadzenia i przetwarzania danych osobowych samorządy powinny zwrócić szczególną uwagę?
Jesteśmy w okresie dość istotnej zmiany, jeżeli chodzi o korzystanie z danych osobowych, które pochodzą z różnego rodzaju rejestrów publicznych. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, po pierwsze, wprowadziła bardzo szeroką definicję rejestru publicznego, co jest szczególnie istotne dla właściwego ich zabezpieczenia. Po drugie, zmiany, które zostały wprowadzone do kodeksu postępowania administracyjnego w 2010 r., szczególnie w art. 220, wprowadzają domniemanie, że urząd może skorzystać elektronicznie z dostępnych dla niego rejestrów publicznych. Ta sytuacja zmieniła znacząco podejście instytucji samorządowych do danych rejestrowych. Do tej pory rejestry kojarzyły się nam z papierowymi księgami albo bazami danych, w których gromadzone były dokumenty zawierające różnego rodzaju dane, w tym dane osobowe. Tymczasem dzisiaj, kiedy rejestry prowadzone są w formie relacyjnych baz danych, tak naprawdę są one miejscem przechowywania bardzo różnych rodzajów danych, które niosą informacje przywiązane nie do dokumentu, ale np. do danej osoby, przedmiotu czy nieruchomości. To powoduje, że realizując zadanie publiczne, np. wydając jakąś decyzję, urzędnik korzysta z pojedynczych danych z różnych rejestrów; z rejestru PESEL pobiera jakiś fragment, z ewidencji gruntów i budynków inny, a z rejestru związanego z podatkami lokalnymi jeszcze inny element. Mamy więc do czynienia nie z transportem dokumentu w znaczeniu tradycyjnym, ale z wykorzystaniem danych za pomocą środków elektronicznych. To zaś powoduje, że ochrona danych, w tym danych osobowych, to nie jest tylko ochrona dokumentu, ale również ochrona procesu przetwarzania.

W jaki zatem sposób powinien przebiegać proces ochrony tak gromadzonych danych osobowych?
Jak wspomniałem na początku rozmowy, chociaż ochrona danych osobowych w samorządzie terytorialnym nie wygląda źle, to wciąż dotyczy ona tradycyjnego dokumentu albo ochrony poszczególnego komputera czy serwera, na którym znajdują się dane. Dziś natomiast potrzebne jest inne spojrzenie na ochronę danych osobowych. Przede wszystkim należy zastanowić się nie tylko nad tym, czy komputer jest dobrze chroniony, ale również nad tym, czy w procesie ochrony danych osobowych nie pojawiają się jakiegoś rodzaju zagrożenia, np. czy do przetwarzanych danych dostęp mają tylko ci urzędnicy, którzy zajmują się wykonaniem określonego zadania, czy też osoby trzecie, m.in. administratorzy baz albo informatycy przygotowujący różnego rodzaju oprogramowanie. To często jest konieczne, ale musi odbywać się na określonych zasadach. Osoby te muszą być poinformowane o tym, że przetwarzają dane osobowe na potrzeby poszczególnych procesów i nie mogą tych danych ani wykorzystywać w innych celach, ani dowolnie łączyć. Mogą je łączyć tylko w takim zakresie, w jakim przewiduje to wykonywane przez nich zadanie. Zatem oprócz polityki bezpieczeństwa dokumentu, serwera czy bazy danych potrzebne jest stworzenie w samorządach polityki bezpieczeństwa i zasad zarządzania prywatnością również dla procesu administracyjnego, w czasie którego może być wykorzystanych mnóstwo informacji pochodzących z różnych dokumentów i rejestrów.

Kto ze strony samorządowej powinien koordynować te zadania?
To jest zdanie dla szefa jednostki samorządowej. W praktyce jednak prawidłowa realizacja tych obowiązków spoczywa na sekretarzu gminy czy powiatu, choć z pewnością jest to praca zespołowa i wymaga zaangażowania wielu osób. Ważną kwestią, na którą warto zwrócić uwagę, jest możliwość przetwarzania danych osobowych znajdujących się w zasobach urzędu przez podmiot zewnętrzny, czyli tzw. outsourcing. Uważam, że jednostki samorządu terytorialnego mogą korzystać z tego rozwiązania, ale pod jednym podstawowym warunkiem, jakim jest zawarcie z podmiotem zewnętrznym tzw. umowy powierzenia przetwarzania danych osobowych. Należy w niej określić zakres powierzonych do przetwarzania danych oraz cel, w jakim podmiot, któremu je powierzono, może je przetwarzać. Podmiot ten może bowiem przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Jest też odpowiedzialny za właściwe ich zabezpieczenie, co wprost wynika z przepisów ustawy o ochronie danych osobowych.
W tym kontekście bardzo istotne jest zidentyfikowanie, w jakich przypadkach samorząd powinien zawrzeć z podmiotem zewnętrznym tzw. umowę powierzenia przetwarzania danych osobowych lub uwzględnić niezbędne jej elementy w innej podpisywanej umowie zawieranej z takim podmiotem.

W praktyce bowiem gminom często wydaje się, że zawierają tylko umowę serwisową. Tak naprawdę jednak instytucja, która świadczy usługę serwisową, ma dostęp do danych osobowych, a więc je przetwarza. Oznacza to, że powinna być ona przeszkolona, aby zapewnić odpowiednią ochronę danych osobowych. Takim klasycznym przykładem błędnego zabezpieczenia danych, a w konsekwencji ich wycieku, była sytuacja, która zdarzyła się podczas ostatnich wyborów samorządowych we Wrocławiu. W tym przypadku dane z karty miejskiej zostały wykorzystane na potrzeby marketingu politycznego. Samorządowcom zabrakło świadomości celu, w jakim były gromadzone te dane osobowe. Należy zatem pamiętać, że przetwarzanie danych osobowych dla innego celu nie jest możliwe, jeżeli administracja nie ma do tego podstawy prawnej. Innym słowy, administracja publiczna może działać tylko w takim zakresie, jaki wyraźnie określają przepisy prawa.

Co zatem z jawnością danych zgromadzonych w rejestrach publicznych?
Dzisiaj, kiedy dane gromadzone są w połączonych ze sobą rejestrach umożliwiających równocześnie automatyczne przesyłanie danych, istnieje konieczność udzielenia odpowiedzi na pytanie, czy zawsze jawność rejestru oznacza to, że jest on dostępny dla każdego. Przy części rejestrów na tak postawione pytanie należy udzielić odpowiedzi twierdzącej. Tak jest np. przy Krajowym Rejestrze Sądowym i nawet gdy zawiera on dane osobowe członków zarządu, to osoby te, decydując się na objęcie takich stanowisk w organach spółek, muszą mieć świadomość tego, że ich dane osobowe będą upublicznione, bo tak przewidują przepisy prawa jest tylko w postaci papierowej i tylko w urzędach gmin. Oczywiście każdy ma do niej dostęp i może zapoznać się z jej treścią, ale już nie może ich sam pobierać z systemu i przetwarzać.
W innych samorządach z kolei całość ewidencji została umieszczona w internecie, a podstawą wprowadzenia takich rozwiązań było uznanie, że skoro ewidencja ta jest jawna, to każdy powinien mieć do niej dostęp.
Nie upieram się co do tego, że ta jawność powinna być zawsze ograniczana. Przede wszystkim nie wszystkie rejestry zawierają dane osobowe, część jednak je zawiera i wówczas ten otwarty dostęp powinien być ograniczony. Problemem jest to, że w Polsce jest około 180 rodzajów rejestrów. Nie widzę jednak możliwości jego rozwiązania przez wprowadzenie jednej wspólnej zasady odnoszącej się do wszystkich rejestrów, bo bardzo się one między sobą różnią. Niezbędne jest zatem przeanalizowanie każdego przypadku osobno i zadecydowanie, czy dane zawarte w konkretnym rejestrze powinny być dostępne online.
Jeżeli natomiast nie zmienią się regulacje prawne, to pojęcia jawności formalnej i otwartego dostępu w internecie nie zostaną rozróżnione. W praktyce będzie to zaś oznaczało, że każdy rejestr publiczny, którego jawności nie wyłączono wprost w ustawie, będzie dostępny w internecie. Tego typu rozwiązania mogą zaś wywołać pewien niepokój społeczny. Nie sądzę, żeby takie było oczekiwanie zarówno urzędników, jak i obywateli.

W instytucjach samorządowych przetwarzane są też dane wrażliwe. Na jakie elementy w tym zakresie urzędnicy powinni zwrócić szczególną uwagę?
W pierwszej kolejności należy sprawdzić, czy gmina, powiat bądź województwo mają prawo do przetwarzania takich informacji. Jeżeli uprawnienie nie wynika wprost z aktu prawnego, co powinno być generalną zasadą przy przetwarzaniu danych osobowych przez jednostki samorządu, to musi zostać spełniona inna z przesłanek zezwalająca na przetwarzanie danych wrażliwych. Gdy jest nią tylko zgoda osoby, której danych dotyczą, to trzeba się zastanowić, czy zgoda ta została wyrażona dobrowolnie, czy też osoba, która jej udzieliła, została do tego przymuszona.
W praktyce często się bowiem zdarza, że samorządy niezgodnie z przepisami wymuszają na mieszkańcach wyrażanie zgody na przetwarzanie danych wrażliwych. Klasycznym przykładem takiej sytuacji jest zbieranie danych na potrzeby weryfikacji spełniania kryteriów, na podstawie których prowadzona jest rekrutacja do przedszkoli. W tym przypadku zdecydowanie protestowaliśmy przeciwko traktowaniu zgody jako podstawy przetwarzania danych dotyczących np. stanu zdrowia dziecka, informacji o orzeczeniach sądowych dotyczących rodziców, sytuacji rodzinnej, wyroku rozwodowego, alimentów itp. Oczywiście, samorządy twierdziły, że tych danych nie wymagają, a rodzice godzą się na ich przekazywanie. To absolutnie niedopuszczalne, aby pozyskiwać takie dane na podstawie przesłanki zgody, bo jej udzielenie nie jest dobrowolne. Niewyrażenie przez rodzica zgody na przekazanie tych danych w rzeczywistości skutkuje bowiem pominięciem w procesie rekrutacji do przedszkola. Jednak w tym przypadku zarzutów nie stawiam jednostkom samorządu terytorialnego, lecz ministrowi edukacji narodowej, który mimo sygnalizacji problemu przez GIODO, nie zmienił przepisów prawnych i nie określił wprost w ustawie, jakie dane można pozyskiwać na potrzeby przeprowadzania naboru do przedszkoli.

Ostatnia nowelizacja przepisów ustawy o ochronie danych osobowych przyznała nowe kompetencje generalnemu inspektorowi. Jedną z nich jest możliwość nałożenia grzywny za niewykonanie decyzji i jej egzekucja w trybie administracyjnym. Czy zmiana przepisów zmieni podejście samorządów?
Trzeba pamiętać, że cała działalność egzekucyjna dotyczy wykonania decyzji nałożonych przez generalnego inspektora ochrony danych osobowych. Kolejność działań będzie wyglądała w ten sposób, że w przypadkach szczególnie rażących będziemy wydawali decyzje np. zakazujące samorządom lub ich jednostkom organizacyjnym przetwarzania pewnego rodzaju danych osobowych. W przypadku niedostosowania się do nich GIODO będzie miał możliwość podjęcia działań egzekucyjnych, czyli nałożenia na organ, który decyzji nie wykonuje, grzywny nawet do 50. tysięcy złotych.

ROZMAWIAŁ ŁUKASZ SOBIECH

> Do 50 tys. zł zapłaci gmina za niewykonanie decyzji generalnego inspektora ochrony danych