Opinie i analizy

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Nr 5, 2016

www.nist.gov.pl

Opinia na temat możliwości gromadzenia przez jednostki samorządu terytorialnego danych o mieszkańcach i ich wykorzystywania dla świadczenia usług publicznych

Krzysztof Król

Ustawa o ochronie danych osobowych z 29 sierpnia 1997 roku (tekst jednolity: Dz. U. 2014 r. poz. 1182, z późn. zm.) nakłada szereg obowiązków na wszystkie podmioty, które w swojej działalności przetwarzają dane osobowe. Jednak w wypadku ich realizacji w jednostkach administracji państwowej oraz w jednostkach samorządu terytorialnego, administratorzy danych osobowych często napotykają na poważne trudności prawne, które uniemożliwiają przetwarzanie danych osobowych zgodnie z przyjętymi wcześniej założeniami wdrażanego przez daną gminą czy powiat projektu samorządowego.

Najczęściej tego typu problemy pojawiają się na poziomie miasta lub gminy przy przetwarzaniu danych osobowych znajdujących się w zasobach administracji publicznej i dotyczą centralnych systemów przetwarzania danych wykorzystywanych np. do celów podatkowych, świadczenia usług komunalnych, prowadzenia ewidencji gruntów czy budowy usług typu call center dla mieszkańców gminy, miasta lub powiatu. Problemy tego typu mogą pojawiać się również przy tworzeniu zinformatyzowanych systemów zarządzania ruchem miejskim, komunikacją miejską, wydawania kart miejskich uprawniających do korzystania z komunikacji, parkomatów czy wreszcie gminnych kart dużej rodziny. W niniejszym raporcie zwracamy uwagę na najważniejsze, a zarazem typowe zagadnienia, które najczęściej stwarzają problemy związane z ochroną danych osobowych i wskażemy możliwe sposoby ich rozwiązywania.

Przepływ informacji

Z punktu widzenia obywatela zgłaszającego się do urzędu chciałby on, aby raz przekazana administracji publicznej informacja nie musiała być ponownie udostępniana przez niego przy kolejnej wizycie w urzędzie. Z drugiej strony obywatele mają prawo do ochrony danych osobowych między innymi dlatego, aby uniknąć sytuacji, w której urząd jest w stanie sprofilować obywatela, a następnie na tej podstawie go w jakiś sposób dyskryminować. Tego typu sytuacje mogą mieć teoretycznie miejsce w wypadku sporu obywatela z urzędem, który poprzez podległe mu organy może go represjonować np. przeprowadzając nieuzasadnione kontrole czy podwyższając opłaty.

Oczywiście, przedstawione powyżej oczekiwania obywateli są ze sobą sprzeczne i dlatego przy realizacji zadań samorządowych należy w jak największym stopniu uwzględnić oba przeciwstawne oczekiwania, ale trzeba przy tym pamiętać, że właśnie dlatego nie uda się stworzyć jednolitego systemu informatycznego przy pomocy którego gmina czy miasto byłyby w stanie zarządzać danymi o obywatelach. Z tego powodu niemożliwe jest też stworzenie jednego okienka, w którym dałoby się załatwić wszystkie sprawy urzędowe, tym bardziej, że część kompetencji może leżeć po stronie administracji państwowej, a część po stronie administracji lokalnej. Zgodnie z ustawą o ochronie danych osobowych, oba typy administracji nie mogą bowiem przekazywać sobie żądnych danych osobowych, z wyjątkiem sytuacji objętych uchwalonymi przepisami ustawowymi.

Właśnie dlatego Generalny Inspektor Ochrony Danych Osobowych powołany został do stania na straży podstawowych zasad ochrony danych osobowych, które określone zostały w aktach prawnych – zarówno w samej ustawie, jak i odnośnych rozporządzeniach. Trudno się też spodziewać zmiany polityki w tej kwestii związanej z tym, że w najbliższych 2-3 latach przepisy krajowe powinny zostać zastąpione odpowiednim rozporządzeniem europejskim. Wspomniane przepisy europejskie będą implementowane

w ten sam sposób we wszystkich krajach członkowskich Unii Europejskiej, ale trudno się tu spodziewać odstępstw od generalnych zasad, które są obecnie obowiązujące dla administracji samorządowej i administracji państwowej.

Zbieranie i przechowywanie danych

Zarówno w przepisach krajowych, jak i w planowanych przepisach europejskich obowiązują dwie podstawowe zasady zbierania i przechowywania danych osobowych. Pierwsza z nich to zasada minimalizacji danych. Oznacza ona, że zbierane i przechowywane są tylko takie dane dotyczące obywatela, które są niezbędne do przeprowadzenia przez jednostkę samorządu terytorialnego danego, konkretnego działania. Drugą podstawową zasadą jest zaś zasada określenia celu. Celu, dla którego konkretne dane mają zostać wykorzystane.

Oznacza to, że zebrane przez jednostkę samorządu terytorialnego dane, które są przez nią przechowywane mogą zostać ponownie przez nią wykorzystane tylko wtedy, gdy cel ich użycia jest albo zgodny z celem pierwotnym, dla którego dane te zostały w ogóle zabrane, albo też prawo przewiduje możliwość ponownego wykorzystania zgromadzonych danych do innego, ściśle określonego w ustawie działania (istnieje wyraźne upoważnienie ustawowe). Tego typu sytuacja miała m.in. miejsce podczas spisu powszechnego, gdzie specjalna ustawa pozwoliła wykorzystać zgromadzone przez administrację publiczną dane do celów statystycznych przy zachowaniu obostrzeń dotyczących procesu anonimizacji tych danych.

Widać tu wyraźnie pewien paradoks związany z kompetencjami poszczególnych szczebli administracji publicznej i prawem obywateli do ochrony danych osobowych. Z jednej strony prawo wspiera samorząd terytorialny w ten sposób, żeby poszczególne jednostki samorządu terytorialnego mogły decydować o tym, co się u nich dzieje, z drugiej wyraźnie oddzielono administrację rządową od samorządowej. Dodatkowo przepisy o ochronie danych osobowych sprawiają, że administracja samorządowa nie może bezpośrednio korzystać z danych, które zostały zebrane zostały na potrzeby administracji rządowej. I odwrotnie, administracja rządowa bez upoważnienia ustawowego nie może korzystać z danych samorządowych.

Innymi słowy administracja publiczna, niezależnie od szczebla, nie może sama decydować o tym, które z dostępnych danych np. zgromadzonych w Urzędzie Stanu Cywilnego, organach podatkowych związanych z podatkami lokalnymi, Urzędach Pracy czy jednostkach samorządowych zajmujących się pomocą społeczną mogą być ze sobą łączone i zestawiane. Oczywiście, stwarza to poważny problem jak nawet w sposób ogólny powiązać zgromadzone dane, które trafiły do administracji publicznej i jak stworzyć profil przetwarzania tych danych, który pomógłby w kompleksowej obsłudze obywatela.

Konstruując system informatyczny przeznaczony do przetwarzania tego typu rozproszonych danych osobowych, w pierwszej kolejności należy dokonać przeglądu poszczególnych regulacji dotyczących działania samorządu i przetwarzania różnych danych zbieranych przez gminę pod kątem nienaruszania zasad ochrony danych osobowych. Najlepiej jeśli tego typu system służy tylko jednemu ściśle określonemu celowi, w związku z którym zebrane zostały przetwarzane dane.

Odnosząc się do problemu wykorzystania danych osobowych przez organy samorządowe do innych celów niż pozwalają na to określone przez przepisy ustawowe, GIODO jasno stwierdza, że gmina nie ma prawa przetwarzać danych osobowych do innych celów niż te, wynikające ściśle z przepisów albo też tworzyć na podstawie zebranych danych innych ewidencji lub wykazów. Tę wykładnię potwierdza m.in. wyrok WSA w Poznaniu z 8 sierpnia 2015 r., sygn. akt IV SA/Po 252/15. Sąd wskazał tu, że Rada Gminy nie może nałożyć obowiązku wyrażenia przez składającego deklarację, zgody na przetwarzanie jego danych osobowych, w celu przeprowadzenia postępowania administracyjnego. Złożona przez obywatela deklaracja uprawnia jedynie organ gminy do ewentualnego wydania decyzji administracyjnej lub wystawienia tytułu wykonawczego. Nie może jednak służyć do tworzenia nowych zbiorów ewidencyjnych.

Przekazywanie danych

Oddzielny problem stanowi zarysowana przed chwilą kwestia powierzenia danych osobowych do przetwarzania przez podmiot administracji publicznej innemu podmiotowi publicznemu. Jeśli chodzi o zasady powierzania danych osobowych do przetwarzania przez firmy i przedsiębiorstwa prywatne, to są one jasno określone w ustawie o danych osobowych. Wątpliwości budzi jednak możliwość zawierania analogicznych porozumień pomiędzy podmiotami publicznymi również w sytuacji wykonywania zadań publicznych przez te jednostki. Nie chodzi tu tylko o wątpliwości dotyczące podstaw prawnych zawierania takich porozumień i na ich podstawie powierzenia przetwarzania danych, ale i samej możliwości zawarcia takiej umowy czy porozumienia. W praktyce ta kwestia sprawia wiele problemów jednostkom samorządowym i ich jednostkom organizacyjnym. Dobrym przykładem tych wątpliwości są zastrzeżenia jakie Biuro GIODO zgłosiło w sprawie Karty Warszawiaka. O sprawie tej głośno było w zeszłym roku.

Nie może być również tak, że gmina czy miasto zarządza danymi, których tak naprawdę nie jest właścicielem.

Z taką sytuacją mamy do czynienia w przypadku różnych platform edukacyjnych i scentralizowanych elektronicznych dzienników. Dane dotyczące uczniów i nauczycieli zbierane są bowiem przez szkoły i tym samym głównym administratorem tych danych jest szkoła reprezentowana przez jej dyrektora. Jednostki samorządowe oferują szkołom platformy edukacyjne, na których te dane mogą być przechowywane i obrabiane. Jednak jednostka samorządu terytorialnego nie może decydować o tym do czego i w jaki sposób dane te zostaną wykorzystywane. Jedyną osobą, która może zarządzać tymi danymi jest wciąż główny administrator tych danych osobowych czyli w tym wypadku dyrektor szkoły. Jednostka samorządowa nie może więc określać własnych celów, do których będzie wykorzystywać dane osobowe zebrane w szkołach, powołując się tylko to, że jest organem założycielskim szkoły. GIODO uznaje takie działanie za niewystarczające do tego, aby uznać, że jednostka administracji samorządowej może przejąć dane osobowe wszystkich osób, które przekazały swoje dane szkole, a ta składuje je w systemie platformy edukacyjnej.

Jeśli chodzi o budowę scentralizowanego systemu informatycznego obejmującego na przykład miasto czy gminę oraz podległe jej jednostki organizacyjne, należy mieć na uwadze, że każdy z podmiotów eksploatujących taki scentralizowany system jest administratorem swoich własnych danych osobowych. Budowa takiego systemu, często bazującego na fizycznej infrastrukturze tylko jednego podmiotu publicznego np. gminy musi uwzględniać rozdzielność i poufność przechowywanych w nim danych. Oczywiście powstaje wówczas szereg pytań dotyczących możliwości i ewentualnej podstawy prawnej wykorzystania i przetwarzania danych wprowadzanych do takiego systemu przez inne jednostki np. przez gminę, ale musi być to dokładnie rozważone pod kontem przestrzegania prawa indywidualnie.

Na szczęście problem ten został zauważony przez ustawodawcę w ustawie wprowadzającej tzw. Centra Usług Wspólnych (CUW) – ustawa z dnia 25 czerwca 2015 r. o zmianie ustawy o samorządzie gminnym oraz niektórych innych ustaw (Dz. U. 2015 r. poz. 1045). W nowowprowadzonym do ustawy o samorządzie gminnym art. 10d wskazano, że: „Jednostka obsługująca jest uprawniona do przetwarzania danych osobowych przetwarzanych przez jednostkę obsługiwaną w zakresie i celu niezbędnych do wykonywania zadań w ramach wspólnej obsługi tej jednostki."

Identyfikacja osób

Oddzielnym problemem jest kwestia identyfikacja osób w gminnych systemach informatycznych. Z punktu widzenia systemu IT, najlepszym rozwiązaniem jest posłużenie się w tym wypadku numerem PESEL. Numer PESEL, to numer Powszechnego Elektronicznego Systemu Ewidencji Ludności. Służy on do jednoznacznej identyfikacji osoby fizycznej, której to numer ten został nadany. Identyfikator PESEL powinien być zatem również jedynym identyfikatorem zewnętrznym dla wszystkich systemów informatycznych, zarówno samorządowych, jak i centralnych.

Warto zauważyć, że w przypadku administracji podatkowej od września 2011 r. numer PESEL jest już jedynym identyfikatorem, którym w kontaktach z tą administracją posługują się osoby nieprowadzące działalności gospodarczej i niezarejestrowane jako podatnicy VAT. Co prawda, numer PESEL w większości wzorów formularzy jakie są kierowane do organów publicznych jest już informacją obligatoryjną, ale warto byłoby nadać wprost organom administracji uprawnienie do żądania od osoby fizycznej podania numeru PESEL każdorazowo w kontaktach z administracją publiczną. Obecnie taki obowiązek jest nałożony wprost w sprawach dotyczących zobowiązań podatkowych oraz niepodatkowych należności budżetowych.

Brak numeru PESEL przy przetwarzaniu danych dotyczących osoby fizycznej uniemożliwia bowiem jednoznaczną identyfikację osoby w systemach informatycznych, co często prowadzi do działań niepożądanych, to jest na przykład do przetwarzania danych całkiem innej osoby lub też zmusza często organ administracji do zbierania danych dodatkowych. Dopiero te dodatkowe dane pozwalają na jednoznaczne zidentyfikowanie osoby. W wypadku osób prawnych i jednostek nie mających osobowości prawnej, takim identyfikatorem powinien być NIP – w każdym rodzaju spraw, nie tylko w sprawach podatkowych lub ewentualnie REGON/KRS w zależności od typu podmiotu.

Rozwiązania biznesowe

Jednostki samorządu terytorialnego takie jak gminy czy miasta, coraz częściej przychylnym okiem sięgają po rozwiązania pomagające w kontaktach urzędu z obywatelami. Jednym z tego typu rozwiązań są centra telefoniczne czy biura obsługi mieszkańca prowadzone w systemie usług Call Center. Niestety pojawiają się tutaj, kolejne problemy związane z ochroną danych osobowych.

Najistotniejszym problemem jest to, że o ile firmy komercyjne, takie jak banki, firmy ubezpieczeniowe czy przedsiębiorstwa zajmujące się marketingiem bezpośrednim mają zagwarantowaną w prawie pewną dowolność w przetwarzaniu danych osobowych (po uzyskaniu odpowiedniej zgody od osoby przekazującej swoje dane), o tyle jednostki administracji nie mogą w dowolny sposób wykorzystywać tego typu danych. W wypadku firm komercyjnych istnieje bowiem prosta zasada wolności gospodarczej mówiąca o tym, że jeżeli jakieś działanie nie jest przez

prawo zabronione, wówczas jest ono dozwolone. Oznacza to, że jeżeli osoba udostępniająca swoje dane wyraziła na to zgodę, wówczas te informacje mogą być przetwarzane przez instytucję biznesową.

Niestety, administracja publiczna nie posługuje się zasadą wolności gospodarczej. Mało tego, obowiązuje tutaj odwrotna zasada wynikająca wprost z artykułu siódmego polskiej konstytucji, mówiąca o tym, że „Organy władzy publicznej działają na podstawie i w granicach prawa". Innymi słowy, jeżeli nie znajdziemy w przepisach prawnych podstaw do danego działania na poziomie ustawy, a ustawa o ochronie danych osobowych mówi, że musi to być wyraźne upoważnienie ustawowe, wówczas nie wolno przetwarzać danych osobowych w innym celu, niż ten, dla którego zostały te dane pierwotnie zebrane.

Oznacza to, że dane wykorzystywane w biurze obsługi mieszkańca muszą być zebrane przez jednostkę samorządu terytorialnego wyłącznie w celu telefonicznych kontaktów z mieszkańcami i nie można do tego wykorzystać danych osobowych pochodzących z innych źródeł dostępnych dla administracji miasta czy gminy. Niestety, jeżeli chcielibyśmy doprowadzić do zmiany takiego systemu i chcielibyśmy dać administracji samorządowej większe uprawnienia do przetwarzania danych niż obecnie wynikają z obowiązującej ustawy o ochronie danych osobowych, należy stworzyć wyjątek na poziomie ustawowym i przy przewidywanym zmianom prawa w tej dziedzinie zgłosić go również do organów Unii Europejskiej.

Big Data

Kolejnym problemem z którym muszą zmierzyć się samorządy jest problem przetwarzania i analizy ogromnych ilości zbieranych automatycznie danych, czyli Big Data. Jak podkreślają analitycy, problemy związane z Big Data stanowić będą jedno z największych wyzwanie dla administracji publicznej, samorządowej i rządowej na całym świecie. Obecnie zaawansowane systemy informatyczne zbierają coraz większa ilość danych nie tylko o zachowaniach użytkowników w Internecie. W wypadków administracji samorządowej i podległych jej jednostek zbierana jest automatycznie ogromna liczba danych m.in. na potrzeby zarządzania ruchem miejskim czy inteligentnego sterowania komunikacją. Zdarza się, że tego typu dane mogą zostać przypisane (w sposób celowy lub nie) do konkretnego obywatela. Taki problem wystąpił między innymi w wypadku wspomnianej przed chwila Karty Warszawiaka czy zintegrowanego systemu inteligentnego sterowania ruchem drogowym w Trójmieście – Tristar. Pytanie czy te dane są zawsze danymi osobowymi?

Zagadnienia te są obecnie analizowane przede wszystkim przez Europejskiego Inspektora Danych Osobowych, który stoi na stanowisku, że wraz ze zbieraniem przez organizację samorządową czy firmę coraz większych ilości danych kwalifikujących się jako dane Big Data, rośnie odpowiedzialność tego podmiotu. Wynika to stąd, że dane, które obecnie nie muszą być danymi osobowymi, mogą takimi stać się w przyszłości dzięki powiązaniu ich z danymi osobowymi, albo przez poprawę algorytmów analizujących te dane, i w ten sposób uzyskania z nich danych osobowych.

Dobrą ilustracją tego problemu jest przetwarzanie danych w systemach GIS czy szerzej w systemach informacji przestrzennej. Przetwarzane tam dane nie są na pierwszy rzut oka danymi osobowymi, ponieważ nie są one połączone wprost z ewidencją gruntów czy budynków. Z drugiej strony analizując w odpowiedni sposób te dane można je mimo wszystko połączyć z danymi, które pozwalają odtworzyć do kogo należy dana posesja identyfikując w ten sposób konkretnego obywatela.

Należy zatem zastanowić się przy tworzeniu systemu przetwarzającego informacje klasy Big Data czy dane, które są przetwarzane mogą stać się w specyficznych sytuacjach danymi osobowymi. Dobrym sposobem na uniknięcie błędu jest przetwarzanie ich przy mniejszym stopniu szczegółowości, takim, na którym nie można ich zindywidualizować, a są one wystarczające do celów statystycznych bądź np. oceny skutków działań. Tak rozwiązano problem który pojawił się w systemie Tristar. W wypadku tego systemu, głównym założeniem było zbieranie bardzo dużej ilości danych dotyczących komunikacji miejskiej, komunikacji prywatnej, miejscach parkingowych, natężenia ruchu oraz tego jak po terenie Trójmiasta poruszają się obywatele. Zrezygnowano jednak z identyfikacji numerów rejestracyjnych, identyfikacji kierowców czy przypisywania miejsc parkingowych do najczęściej pojawiających się samochodów. Zmniejszenie szczegółowości przetwarzanych danych pozwoliło uniknąć problemów związanych z naruszeniem przepisów ustawy o ochronie danych osobowych.

Podsumowanie

Aby było możliwe przetwarzanie w innych celach danych osobowych, które zebrane zostały przez jednostki samorządu terytorialnego przy okazji prowadzenia różnych postępowań administracyjnych czy podatkowych, musi istnieć wyraźne upoważnienie ustawowe. Należy brać jednak pod uwagę, że potencjalne zmiany w prawodawstwie nie mogą naruszać podstawowych zasad ochrony danych osobowych, a więc minimalizacji zebranych informacji oraz jasno zdefiniowanego i określonego celu.

W dotychczasowej praktyce większy nacisk kładziono na zachowanie zasad wynikających z ochrony danych osobowych niż na zwiększoną funkcjonalność działań związa-

nych z możliwością przekazywania danych. Jak się wydaje, jedyne na co mogą liczyć jednostki samorządu terytorialnego w najbliższych latach w kwestii zmian prawnych dotyczących ochrony danych osobowych, to usprawnienie elektronicznego przepływu informacji pomiędzy rejestrami publicznymi. Jednakże pod tym warunkiem, że nie będą one służyły budowaniu profili osób. Nie ma więc obecnie możliwości, a także w dającej się przewidzieć przyszłości, konsolidacji pod względem używanych baz danych systemów informatycznych należących do administracji państwowej i samorządowej, w których są przechowywane i przetwarzane dane osobowe. Na szczęście ustawodawca zauważył potrzebę tworzenia Centrum Usług Wspólnych, dzięki którym istnieje możliwość uwspólnienia pewnych elementów infrastruktury IT przetwarzającej dane osobowe. Biuro GIODO nie widzi również przeszkód w wykorzystywaniu w tym celu usług chmurowych. Opublikowany został nawet „Dekalog Chmuroluba" opisujący dziesięć zasad stosowania usług chmurowych przez administrację publiczną.

Literatura

[1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. Nr 0, poz. 1182, z późń. zm.).
[2] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923, z późn. zm.).
[3] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r. Nr 229, poz. 1536).
[5] Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 225, poz. 1350).
[6] Orzeczenie WSA w Poznaniu z 8 sierpnia 2015 r., sygn. akt IV SA/Po 252/15 (http://orzeczenia.nsa.gov.pl/doc/06055876FF)
[7] Dekalog Chmuroluba (http://www.giodo.gov.pl/259/id_art/6271/j/pl)

Notatki:

Narodowy Instytut Samorządu Terytorialnego powstał w 2015 r.
Jest państwową jednostką budżetową podległą MSWiA.
Działa na rzecz dalszej profesjonalizacji samorządu terytorialnego i administracj publicznej.

Opinie i analizy NIST, ul. Zielona 18, Łódź 90-601
Sekretariat tel. +48 42 633 10 70
e-mail: sekretariat@nist.gov.pl