DANE OSOBOWE

Czy PUMA pokazuje zbyt wiele? Jeśli tak, samorządy mogą mieć kłopot

PROBLEM: Konwent Powiatów Województwa Świętokrzyskiego alarmuje, że system dziedzinowy PUMA stosowany w urzędach m.in. do obsługi mieszkańców czy prowadzenia spraw pracowniczych nie spełnia wymogów ochrony danych osobowych. A wszystko dlatego, że urzędnikom oprócz informacji o klientach wyświetlają się także dane ich kolegów, w tym numery ich kont bankowych. Według starostów i ekspertów stwarza to ryzyko manipulacji oraz nieuprawnionego pozyskiwania informacji. Co więcej, zmieszanie danych uniemożliwia urzędom zarejestrowanie bazy w Generalnym Inspektoracie Ochrony Danych Osobowych.

©℗ Opracował Paweł Sikora

Starostowie ze świętokrzyskiego chcą szybkiego doprowadzenia do zgodności programu z przepisami. Sytuacja jest rozwojowa i wciąż badana przez lidera projektu, urząd marszałkowski. Sprawie przygląda się też GIODO. Tymczasem niezależni prawnicy podkreślają, że jeśli faktycznie doszło do nieprawidłowości na gruncie ustawy z 29 sierpnia 1997 r. ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922), starostom, jako administratorom danych, mogą grozić sankcje karne oraz ewentualne roszczenia odszkodowawcze. System PUMA jest wykorzystywany przez 400 jednostek samorządowych.

Jeden worek

Jak tłumaczy Mariusz Piskorczyk, administrator bezpieczeństwa informacji w starostwie powiatowym w Jędrzejowie, w systemie PUMA istnieje tylko jedna baza, do której wrzucane są – jak do jednego worka – dane osób prowadzących działalność gospodarczą, osób fizycznych, kontrahentów jednostki oraz pracowników urzędu. Przy czym najszerszy zakres zebranych danych dotyczy urzędników. Obejmuje bowiem nie tylko ich imiona i nazwiska czy adresy, ale także np. PESEL-e, NIP-y, imiona rodziców, numery dowodów osobistych i kont bankowych.

Tymczasem choć PUMA rozróżnia dane mieszkańców od danych pracowników urzędu czy kontrahentów jednostki, to w systemie – jak tłumaczą nam urzędnicy – tworzą one jedną, niepodzielną całość i właśnie stąd bierze się problem. – Przykładowo kasjer w urzędzie przyjmujący opłaty np. za prawo jazdy powinien mieć wgląd tylko do danych klientów urzędu i absolutnie nie powinien mieć możliwości dotarcia do danych osobowych pracowników urzędu. Z kolei kadrowa powinna mieć dostęp wyłącznie do danych pracowników, bo umożliwienie jej wglądu do danych mieszkańców nie da się niczym uzasadnić – tłumaczy Mariusz Piskorczyk.

Dodaje, że zarejestrowanie zbioru danych osobowych zawierającego dane klientów i jednocześnie pracowników traktowanych jak zwykłych klientów jest po prostu niemożliwe. Wynika to z różnego zakresu zbieranych danych osobowych. – Jest to błąd systemu, oznaczający jego niezgodność z ustawą o ochronie danych osobowych w zakresie rejestracji i nadawania poszczególnym pracownikom upoważnień do przetwarzania konkretnych zbiorów – stwierdza Piskorczyk.

U źródła kłopotów

Przy czym wszystko zaczęło się od zastrzeżeń administratora bezpieczeństwa informacji Starostwa Powiatowego w Skarżysku-Kamiennej. To on jako pierwszy poinformował spółkę Zeto Software, która stworzyła PUMĘ, o wadliwości systemu, co jego zdaniem wynika z jednej zmieszanej bazy. Gdy ta stwierdziła, że system działa poprawnie, ABI postanowił zwrócić się o zajęcie stanowiska do Konwentu Powiatów Województwa Świętokrzyskiego. – Konwent, nie badając zastrzeżeń, co więcej, nie zwracając się do wykonawcy o złożenie stosownych wyjaśnień, wydał stanowisko, w którym wskazał na wadliwość systemu oraz konieczność wprowadzenia zmian w celu przywrócenia jego zgodności z ustawą – mówi oburzony Michał Paprocki, radca prawny kancelarii Chmaj i Wspólnicy Sp. k., który jest pełnomocnikiem spółki Zeto Software.

Jego zdaniem system działa poprawnie, a zarzuty są bezpodstawne. Nie jest także prawdą, że firma przyznała się do błędu i zgodziła się na wykonanie poprawek. Dodaje, że wprowadzenie jednolitej bazy kontrahentów w jednym zbiorze wynikało z wymagań zamówionego przez świętokrzyski Urząd Marszałkowski systemu. – Program spełnia ponadto wszystkie wymogi określone w specyfikacji projektu, w tym wymaganie dotyczące uprawnień użytkowników, co zostało potwierdzone stosownymi protokołami odbioru – twierdzi mecenas Paprocki. – Sugerowane rozbijanie bazy kontrahentów na dwie oddzielne jest rozwiązaniem archaicznym i nie jest stosowane w nowoczesnych, zintegrowanych systemach informatycznych. PUMA nie dopuszcza osób nieupoważnionych do przeglądu czy edycji danych kadrowych. Do nich uprawnienia dostępu posiadają tylko upoważnieni pracownicy jednostki zajmujący się obsługą kadrowo-płacową. Osoba z dostępem do kartoteki klientów, np. kasjer przyjmujący opłaty za prawo jazdy, nie ma wglądu do danych stricte kadrowych, a tym bardziej nie ma możliwości ich edycji – zapewnia radca.

Z kolei Ewelina Gładki, dyrektor departamentu społeczeństwa informacyjnego Urzędu Marszałkowskiego Województwa Świętokrzyskiego, twierdzi, że zaletą systemu jednokrotnego miejsca wprowadzania informacji jest zmniejszenie czasochłonności i niepowielanie pracy. Eliminuje to konieczność wielokrotnego wprowadzania danych, a zmiana raz wprowadzona jest widoczna w całym systemie.

– Do tej pory nie spotkaliśmy się z informacjami o braku możliwości nadania prawidłowych uprawnień do właściwych obszarów sytemu – mówi Ewelina Gładki. Zwraca uwagę, że obecnie za eksploatację, utrzymanie produktów i rezultaty projektu odpowiada indywidualnie każdy z partnerów (poszczególne urzędy gmin i powiatów - red.). – Jednak w przypadku zaistnienia problematycznej sytuacji na styku partner/wykonawca – urząd marszałkowski uczestniczy w procesie wyjaśniania. W związku z tym podjęliśmy stosowne działania. Przy czym zidentyfikowaniem problemu i jego miejsca zajmie się wykonawca, natomiast my możemy jedynie zastosować odpowiednie instrumenty zapobiegawcze w przypadku potwierdzenia wystąpienia nieprawidłowości. To wykonawca w ramach gwarancji ma obowiązek nieodpłatnie wprowadzić właściwe zmiany w przypadku niezgodności systemu z obowiązującymi przepisami i specyfikacją zamówienia – zapewnia Gładki.

Problemami z PUMĄ zaskoczony jest Tomasz Zembrzuski, informatyk Starostwa Powiatowego w Sandomierzu. Twierdzi, że w jego urzędzie problemy z programem nie mają miejsca. – Być może kłopoty są związane z błędną konfiguracją użytkowników – zastanawia się Zembrzuski.

Żadnych problemów nie ma także np. Urząd Gminy w Czarnocinie czy starostwo w Busku-Zdroju.

OPINIE EKSPERTÓW

TOMASZ LEWANDOWSKI
associate w kancelarii SMM Legal

Starosta, jako administrator danych osobowych, odpowiada za ich bezpieczeństwo na gruncie ustawy o ochronie danych osobowych. Przy każdym upublicznieniu tego typu incydentu można spodziewać się kontroli ze strony generalnego inspektora ochrony danych osobowych. Niezależnie od ryzyka takiej kontroli starostowie powinni natychmiast zaprzestać przetwarzania danych w ramach systemu PUMA i przystąpić do oceny skutków jego funkcjonowania dla systemu ochrony danych w kierowanych przez nich urzędach. Ponowne przetwarzanie będzie dopuszczalne wyłącznie w przypadku usunięcia wad i przywrócenia funkcjonalności systemu odpowiadającej wymaganiom prawa. Kazus jest istotny z punktu widzenia zmian przepisów z zakresu ochrony danych osobowych związanych z wejściem w życie nowego rozporządzenia ogólnego o ochronie danych osobowych, które zacznie być stosowane od 25 maja 2018 r. Zgodnie z nim przed wdrożeniem podobnego systemu na administratorach danych osobowych spoczywa obowiązek przeprowadzenia rzetelnej oceny ryzyka związanego z przetwarzaniem danych. W rozporządzeniu przewidziano możliwość nakładania wysokich kar na podmioty, które dopuszczają się naruszeń (do 20 mln euro). Starostowie, dokonując ewaluacji ryzyka związanego z przetwarzaniem danych w systemie PUMA, powinni brać zmiany pod uwagę, w tym obowiązkowo powołać inspektora ochrony danych osobowych, który w porę może zapobiec kłopotom.

MICHAŁ KUŹNIAK
radca prawny z Kancelarii Radców Prawnych Klatka i Partnerzy

Odpowiedzialność karna za przetwarzanie w zbiorze danych osobowych spoczywa na każdym, kto nielegalnie przetwarza dane, a więc na administratorze, a także na pracowniku administratora, który udostępnia lub zmienia dane, chociaż nie jest do tego upoważniony. Wgląd do bazy danych nie stanowi jeszcze ich przetwarzania, tak więc zapoznanie się z danymi osobowymi nielegalnie udostępnionymi nie jest czynem, za który można ponosić odpowiedzialność na podstawie ustawy o ochronie danych osobowych. Jednak do przetwarzania mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych (czyli starostwo). Inną możliwością legalnego poszerzenia przez administratora danych możliwości dostępu do danych osobowych jest powierzenie przetwarzania danych innemu podmiotowi na mocy umowy pisemnej zawieranej z administratorem. Odpowiedzialność spoczywa wówczas nadal na administratorze danych, jak również dodatkowo na podmiocie, któremu powierzono przetwarzanie danych.

MACIEJ HAWLICZEK
radca prawny Omega Kancelarie Prawne Sp. z o.o.

Jeżeli chodzi o odpowiedzialność cywilną pracownika, to kwestie związane z ochroną danych osobowych stanowią część prawa do prywatności, które z kolei jest dobrem osobistym podlegającym ochronie na podstawie art. 24 k.c. W związku z tym, jeżeli pracownik swoim działaniem naruszy kwestie związane z ochroną danych osobowych, to może narazić się na to, że osoba poszkodowana jej działaniem wytoczy powództwo w sądzie cywilnym. Powództwo takie może zostać wytoczone przeciwko jednostce samorządu terytorialnego, która odpowiada za niezgodne z prawem działania pracownika, chronione prawem dobra, takie jak dane osobowe. Takiemu poszkodowanemu przysługują następujące roszczenia: o zaniechanie naruszeń, o odszkodowanie lub zadośćuczynienie.

DAWID SKRZYPCZYK
prawnik w Omega Kancelarie Prawne Sp. z o.o.

Wzgłoszeniu zbioru danych należy wskazać między innymi cel przetwarzania danych osobowych oraz opis zastosowanych środków technicznych i organizacyjnych. Dane pracowników oraz dane interesantów przetwarzane są w innych celach i w oparciu o inne przepisy uprawniające do ich przetwarzania. Można zatem uznać, że stanowią oddzielne zbiory danych i powinny być odrębnie zarejestrowane. Przetwarzanie danych w zbiorze przed jego zgłoszeniem lub rejestracją wydaje się sprzeczne z przepisami. W świetle powyższego należałoby rozważyć zgodność z prawem przetwarzania danych interesantów, skoro zbiór tych danych mógł nie zostać zgłoszony czy zarejestrowany.