

# Interwencja: PUMA już pod lupą GIODO

**Paweł Sikora**  
pawel.sikora@infor.pl

Generalny inspektorat ochrony danych osobowych postanowił przeprowadzić wyrywkowy audyt w samorządach. To efekt naszej publikacji na temat zbyt szerokiego dostępu do zbiorów osobowych w systemie PUMA. GIODO podejrzewa, że fakt, iż urzędnicy mają wgląd w internetowy system do informacji nie tylko o petentach, ale o wszystkich zatrudnionych w urzędzie, może wynikać z tego, że nie został wdrożony system zarządzania kontrolą dostępu lub PUMA po prostu zawiera błędy.

Jak twierdzi Agnieszka Świątek-Druś, rzecznik prasowy GIODO, sytuacja wzbudziła zaniepokojenie urzędu. Dlatego w najbliższym czasie do administratorów bezpieczeństwa informacji kilku wybranych świętokrzyskich samorządów zostaną skierowane wystąpienia. – W ten sposób chcemy sprawdzić zgod-

ność przetwarzania danych osobowych w systemie informatycznym PUMA z przepisami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z z 2016 r. poz. 195 ze zm.). Z tego aktu wynika, że każdy administrator danych musi zadbać nie tylko o należyte zabezpieczenie gromadzonych danych, ale przede wszystkim o wdrożenie wszelkich rozwiązań prawno-organizacyjnych, by przestrzegać przepisów, i to w szczególności, gdy dane przetwarzane są w systemach informatycznych – mówi Świątek-Druś.

A za to „głową” odpowiadają administratorzy samorządów. W tym przypadku wójtowie oraz starostwie. To właśnie ci ostatni zaalarmowali, że systemy dziedziczone PUMA może nie spełniać wymogów ochrony danych osobowych. W sprawę zaangażowany jest również Urząd Marszałkowski Województwa Świętokrzyskiego, który przy wdrożeniu systemu w samo-

radach pełnił rolę pośrednika. Sprawa jest o tyle poważna, że za błędy w polityce bezpieczeństwa grożą poważne kary, włącznie z pozbawieniem wolności do lat dwóch.

Pełnomocnik wykonawcy PUMY twierdzi jednak, że sam system działa prawidłowo, a problemy mogą wynikać z błędnego nadawania uprawnień.

Tymczasem GIODO wyraźnie podkreśla, że podmioty, które wykorzystują systemy IT służące do przetwarzania danych, powinny z należytą starannością weryfikować osoby uprawnione do korzystania z systemu oraz zakres nadawanych im uprawnień dostępu do danych. Sam system musi też posiadać mechanizmy kontroli dostępu, rejestr użytkowników z przypisanymi im identyfikatorami. Bardzo ważne jest też opracowanie i wdrożenie procedur nadawania uprawnień do przetwarzania danych i rejestrowania ich w systemie. Podmiot posiadający

bazę z danymi osobowymi musi też dysponować odpowiednimi metodami i środkami uwierzytelnienia związanymi z zarządzaniem nią i użytkowaniem. GIODO od lat też podkreśla, że prawidłowa realizacja procedury zamówień publicznych nie oznacza, że zamówiony program został poddany analizie ze strony przepisów o ochronie danych osobowych i jest z nimi zgodny. Tak więc najważniejszą zasadą, jaką należy się kierować w odniesieniu do kontroli dostępu, jest minimalizacja uprawnień. Oznacza to, że zakres nadanych uprawnień nie powinien przekraczać zakresu obowiązków poszczególnych osób. Biorąc to pod uwagę, już na etapie projektowania i zakupu systemu, nabywca powinien przeprowadzić analizę i precyzyjnie zdefiniować obowiązki i uprawnienia poszczególnych pracowników w danym systemie oraz upewnić się, że będzie możliwa ich realizacja. Powinien także wyznaczyć osoby,

które będą odpowiedzialne za wdrożenie i zarządzanie uprawnieniami oraz przeprowadzanie regularnych przeglądów nadanych uprawnień. ©P

Więcej na temat systemu dziedziczonego PUMA pisaaliśmy w artykule z 22 lutego br. (tygodnik SiA, nr 37) pt. „Czy PUMA pokazuje zbyt wiele? Jeśli tak, samorządy mogą mieć kłopot”.

