



RZECZNIK PRAW OBYWATELSKICH

Warszawa,

Adam Bodnar

VII.520.9.2016.AG

**Pan
Mariusz Błaszczak
Minister Spraw Wewnętrznych
i Administracji
ul. Stefana Batorego 5
02-591 Warszawa**

W ostatnich dniach pojawiły się doniesienia prasowe, informujące o tzw. wycieku danych z bazy PESEL. W mediach początkowo informowano, że problem może dotyczyć nawet ok. 1,5 mln Polaków (zob. np. <http://fakty.tvn24.pl/ogladaj-online,60/wyciek-danych-z-bazy-pesel-moze-dotyczyc-nawet-poltora-miliona-polakow,672044.html>). W kolejnych dniach jednak podkreślano, że „wyciek” nie miał charakteru nielegalnego, a pobieranie danych miało związek z zadaniami wykonywanymi przez kancelarie komornicze. W przekazy medialne wkraść się zatem pewien chaos informacyjny, a do Rzecznika Praw Obywatelskich zwracają się zaniepokojeni obywatele.

Obywatele mają prawo oczekiwać, że wszystkie informacje pozyskiwane na ich temat będą odpowiednio zabezpieczone. Jest to standard wynikający z art. 47 oraz 51 Konstytucji RP. W swoich skargach informują zatem Rzecznika, że po pierwsze obawiają się, czy ich dane nie posłużą np. do zaciągnięcia kredytu, a po drugie domagają się skutecznych działań od właściwych organów państwowych, które są zobowiązane do zabezpieczenia danych zbieranych na temat obywatela.

Zgodnie z art. 6 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2016 r. poz. 722 ze zm.), rejestr PESEL jest centralnym zbiorem danych, prowadzonym przez ministra właściwego do spraw informatyzacji. W związku z tym w tej konkretnej sprawie skierowałem wystąpienie do Minister Cyfryzacji, jak również do Generalnego Inspektora Ochrony Danych Osobowych, a także do Prezesa Krajowej Rady Komorniczej. Należy jednak zaznaczyć, że **Minister Spraw Wewnętrznych i Administracji jest organem powołanym do ochrony bezpieczeństwa i porządku publicznego, w tym również bezpieczeństwa związanego z ujawnianiem informacji gromadzonych na temat obywateli przez upoważnione do tego ustawowo podmioty.** Sytuacja z dostępem do rejestru PESEL, bez wskazywania na obecnym etapie czy doszło do wycieku z rejestru,

czy też dostęp miał charakter legalny, skłania zatem do ogólniejszej refleksji na temat działań właściwych organów w tym zakresie.

W szczególności należy mieć na uwadze raport Najwyższej Izby Kontroli z 14 kwietnia 2016 r. (KPB.410.004.05.2015), poświęcony zapewnieniu bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych, z którego jasno wynika, że skontrolowane przez NIK systemy ochrony danych nie zapewniają ich bezpieczeństwa. Działania realizowane w celu jego zapewnienia są prowadzone opieszale, bez z góry przygotowanego planu, a środki przeznaczane na ten cel są niewystarczające. W efekcie istnieje ryzyko, że działanie istotnych dla funkcjonowania państwa systemów teleinformatycznych zostanie zakłócone, a dane w nich się znajdujące trafią w niepowołane ręce. W odniesieniu do MSW, Najwyższa Izba Kontroli oceniła poziom zarządzania bezpieczeństwem systemów teleinformatycznych jako początkowy/doraźny (por. ww. raport NIK, s. 37-38). Wskazano m.in., że ministerstwo dostrzegало potrzebę zapewnienia bezpieczeństwa IT, jednakże było ono zapewniane na doraźnych zasadach, zależało głównie od pojedynczych osób i nie podlegało pomiarowi. Podkreślono, że w ministerstwie nie wprowadzono formalnych podstaw do Systemu Zarządzania Bezpieczeństwem Informacji pomimo, że istniała w tej jednostce świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego. Nie powołano również właściwej komórki odpowiedzialnej za zarządzanie bezpieczeństwem systemów teleinformatycznych, pomimo że wyniki przeprowadzonych audytów rekomendowały powołanie jednej komórki organizacyjnej w tym zakresie. Co szczególnie istotne, nie przeprowadzono procesu identyfikacji zasobów istotnych dla realizowanych zadań, nie przypisano im istotności i niezbędnych poziomów ochrony, a także nie określono procedur reagowania na incydenty, a nawet nie wprowadzono jednoznacznej definicji incydentu bezpieczeństwa.

Kontrola, której dotyczy przywoływany wyżej raport NIK przeprowadzona została w 2015 r. W związku z powyższym, działając na podstawie art. 13 ust. 1 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2014 r., poz. 1648 ze zm.), **zwracam się do Pana Ministra z prośbą udzielenie informacji na temat działań prowadzonych w celu zapewnienia bezpieczeństwa informatycznego w MSWiA oraz jednostkach podległych, a także ewentualnych innych projektach mających na celu zapobieganie zdarzeniom podobnym do tych, o których informowały w ostatnich dniach media.**