Źródło: stock.adobe.com

Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego

Od 1 czerwca 2017 r. do dnia zakończenia kontroli w 2018 r.

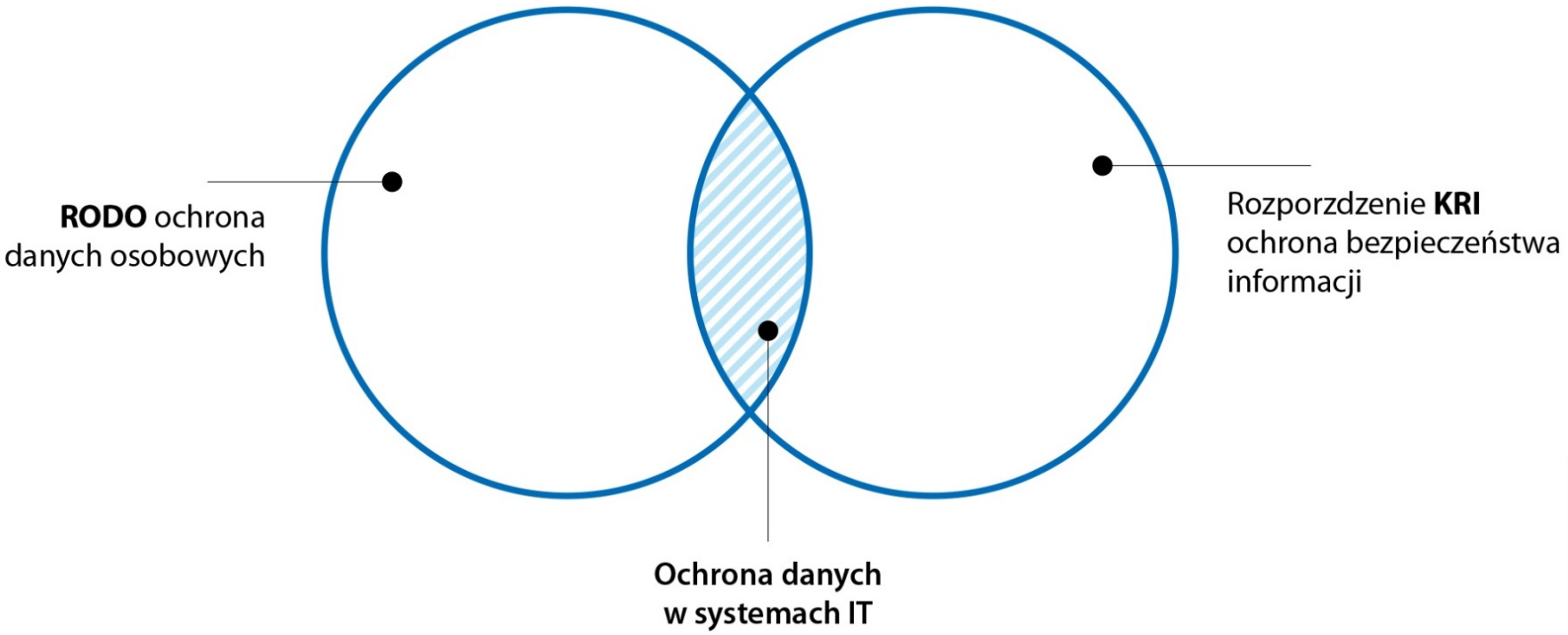
Najwyższa Izba Kontroli

Warszawa, maj 2019 r.

01 Dlaczego podjęliśmy kontrolę?

- W związku z coraz szerszym wykorzystywaniem systemów informatycznych do realizacji zadań w administracji publicznej konieczne jest zabezpieczenie danych o obywatelach.
- Wejście w życie przepisów RODO w zakresie ochrony danych osobowych wprowadziło nowe wymogi dla zaprojektowania i wdrożenia całego systemu tej ochrony, w tym ustanowienia procedur dla wszystkich procesów zachodzących w urzędzie.
- Wcześniejsze kontrole, w których badano wybrane aspekty bezpieczeństwa informacji wykazały, że kierownicy urzędów nie nadają bezpieczeństwu informacji należytej wagi, nie wdrażają i nie aktualizują zasad bezpieczeństwa, nie zapewniają odpowiednich narzędzi IT lub nie w pełni je stosują.
- Stale wzrasta zainteresowanie obywateli elektroniczną formą załatwiania spraw w urzędach.

02 Zakres ochrony bezpieczeństwa informacji w kontekście ochrony danych osobowych



Źródło: Opracowanie własne NIK.

03 Co kontrolowaliśmy?

Czy przyjęte i wdrożone rozwiązania organizacyjne i techniczne zapewniają bezpieczeństwo przetwarzania informacji w urzędzie?

W szczególności:

- Czy zapewniono należytą organizację bezpieczeństwa informacji (polityki, procedury, instrukcje, dedykowane zasoby osobowe, techniczne)?
- Czy rozwiązania techniczne są wdrożone i wykorzystywane a rozwiązania organizacyjne stosowane i egzekwowane?
- Czy są cyklicznie podejmowane działania mające na celu zapobieganie incydentom bezpieczeństwa informacji (szkolenia, analiza incydentów, audyty, analiza ryzyka)?

04 Kogo kontrolowaliśmy?

Kontrolą objęto łącznie 23 jednostki z obszaru pięciu województw (mazowieckiego, podlaskiego, łódzkiego, małopolskiego i dolnośląskiego), w tym:

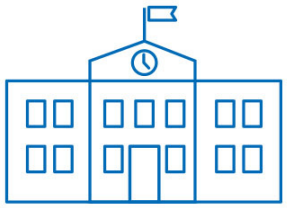
- dziewięć starostw powiatowych;
- 14 urzędów miast/miast i gmin/gmin.

Stwierdzony stan – nienależyta organizacja bezpieczeństwa informacji

- W 14 urzędach (61%) stwierdzono, że brak było systemowego podejścia dla zapewnienia bezpieczeństwa informacji, o którym mowa w § 20 ust. 1 rozporządzenia KRI. Opracowane i wdrożone regulacje dotyczyły głównie ochrony danych osobowych i nie obejmowały bezpieczeństwa innych informacji. W urzędach tych nie ustanowiono polityk bezpieczeństwa informacji.
- W sześciu urzędach (26%) nie przeprowadzono aktualizacji uregulowań wewnętrznych w zakresie ochrony danych osobowych w związku z wejściem w życie przepisów RODO.
- We wszystkich kontrolowanych urzędach, na podstawie art. 37 ust. 1 RODO zostali powołani Inspektorzy Ochrony Danych (IOD), jednak w pięciu (22%) stwierdzono, że inne zadania i obowiązki wykonywane przez osobę pełniącą funkcję IOD mogły powodować konflikt interesów, o którym mowa w art. 38 ust. 6 RODO.
- W 17 urzędach (74%) nie utrzymywano aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.

Stwierdzony stan – nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji lub ich brak

- W 19 z 23 kontrolowanych urzędów (83%) wystąpiły nieprawidłowości w zakresie zarządzania uprawnieniami użytkowników w systemach informatycznych.



23 kontolowane jednostki

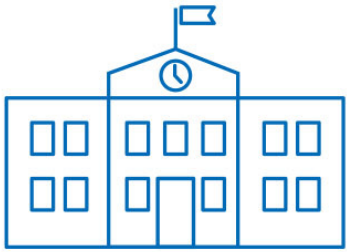
Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Stwierdzony stan – nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji lub ich brak

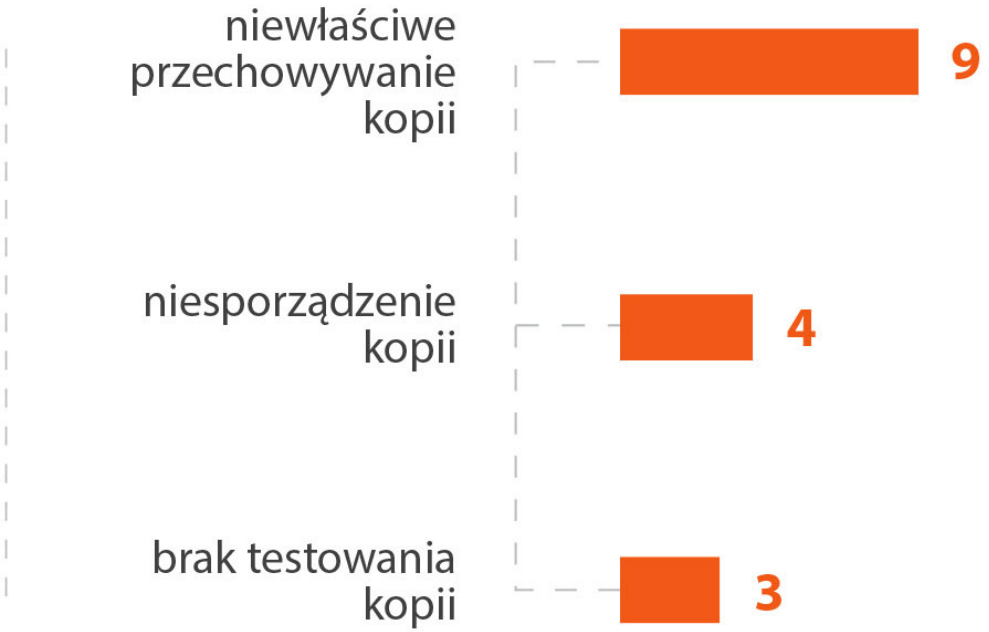
- Pomimo ustanowienia wymogów w zakresie uzyskiwania dostępu do systemów informatycznych, w 13 kontrolowanych urzędach (57%) zasady te nie były przestrzegane. Użytkownicy stosowali hasła dostępu krótsze niż wymagane.
- W ośmiu urzędach (35%) nie określono szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych poza ich siedzibami, gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI.
- W 16 kontrolowanych urzędach (70%) nie stosowano rozwiązań polegających na szyfrowaniu dysków twardych komputerów przenośnych, przez co nie minimalizowano ryzyka nieuprawnionego dostępu do danych zgromadzonych na tych urządzeniach w razie ich utraty.
- W dziesięciu kontrolowanych urzędach (43%) zastosowano zabezpieczenia fizyczne serwerowni, które w niewystarczającym stopniu chroniły te pomieszczenia. Było to niezgodne z § 20 ust. 2 pkt 9 rozporządzenia KRI.

Stwierdzony stan – nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji lub ich brak

- W 11 urzędach (48%) stwierdzono nieprawidłowości w zakresie tworzenia, przechowywania oraz testowania kopii zapasowych.



23 kontolowane jednostki



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Stwierdzony stan – nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji lub ich brak

- W 13 kontrolowanych urzędach (56%) wykorzystywano komputery z zainstalowanym systemem operacyjnym nie posiadającym już wsparcia producenta, co niekorzystnie wpływało na poziom bezpieczeństwa, a ponadto było niezgodne z § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI.
- W 12 urzędach (52%) w umowach na zakup lub serwis sprzętu komputerowego/oprogramowania objętych badaniem stwierdzono brak zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI.
- W pięciu kontrolowanych urzędach (22%) nie był prowadzony rejestr czynności przetwarzania danych osobowych, co było niezgodne z art. 30 RODO.

Stwierdzony stan – niewystarczające działania w celu zapobiegania incydentom bezpieczeństwa

- W 11 urzędach (48%) nie powadzono okresowych analiz ryzyka utraty integralności, poufności, dostępności, co było niezgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI.
- W siedmiu urzędach (30%) nie przeprowadzono analizy procesów przetwarzania danych osobowych i nie dokonano oceny stopnia zapewnienia ich bezpieczeństwa w odniesieniu do stwierdzonych ryzyk, o których mowa w art. 32 ust. 1 RODO.
- W 16 urzędach (70%) w 2017 r. nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.
- W pięciu urzędach (22%) nie ustanowiono procedur wewnętrznych zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji, wymaganych w myśl § 20 ust. 2 pkt 13 rozporządzenia KRI.

Stwierdzony stan – kontrole bezpieczeństwa w j.s.t. prowadzone przez wojewodów

W okresie od 1 stycznia 2016 r. do końca lutego 2018 r. wojewodowie przeprowadzili łącznie w j.s.t. w 12 województwach tylko 40 kontroli dotyczących zapewnienia bezpieczeństwa informacji dla systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej.

W przypadku czterech województw, w których kontrole j.s.t. nie były prowadzone, wskazywano na brak pracowników posiadających kwalifikacje do prowadzenia kontroli w tym zakresie.

Wojewodowie wskazali, że planowane są kolejne kontrole w powyższym zakresie.

Ocena ogólna
– rodzaje ocen kontrolowanej działalności wykonywanej w badanych j.s.t. [%]

Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Ocena ogólna

NIK negatywnie oceniła wykonywanie przez blisko 70% skontrolowanych urzędów jednostek samorządu terytorialnego zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji w okresie objętym kontrolą. W 61% kontrolowanych urzędów brak było systemowego podejścia do zapewnienia bezpieczeństwa informacji.

W wielu kontrolowanych urzędach j.s.t. nie dostrzegano występujących zagrożeń. W 48% jednostek nie dokonywano analiz ryzyka, a w 70% nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji. Brak cyklicznych analiz ryzyka i nieprowadzenie audytów bezpieczeństwa nie pozwalał na identyfikację istotnych ryzyk w zakresie bezpieczeństwa informacji. **Kontrola wykazała, że w wielu urzędach j.s.t. zasady mające na celu zwiększenie bezpieczeństwa przetwarzania danych nie były przestrzegane,** w szczególności w ponad 80% kontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych.

Wyniki kontroli wskazują, że o ile w urzędach j.s.t. w większości podjęto działania w celu dostosowania do RODO, to w dalszym ciągu często nie są przestrzegane wymogi dotyczące bezpieczeństwa informacji wynikające z obowiązującego od 2012 r. rozporządzenia KRI.

14 Wnioski

Minister Cyfryzacji

Istnieje potrzeba szerokiego promowania/informowania organów administracji o wymogach w zakresie bezpieczeństwa informacji określonych w rozporządzeniu KRI i ich wpływie na zapewnienie ochrony danych osobowych.

Wojewodowie

Objąć kontrolami większą liczbę urzędów j.s.t. w zakresie zapewnienia bezpieczeństwa informacji dla systemów teleinformatycznych oraz rejestrów publicznych.

W związku z ustaleniami kontroli NIK, dotyczącymi działań j.s.t. związanych z zapewnieniem wdrożenia niektórych wymogów RODO, informacja o wynikach tej kontroli została przekazana także Prezesowi Urzędu Ochrony Danych Osobowych.

Źródło: stock.adobe.com

Najwyższa Izba Kontroli

Departament Administracji Publicznej