NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.013.04.2018
P/18/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 90-980 Łódź
T +48 42 239 32 00, F +48 42 239 32 90
llo@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli	P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Łodzi
Kontroler	Piotr Rydygier, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LLO/102/2018 z dnia 5 lipca 2018 r. (dowód: akta kontroli str. 1)
Jednostka kontrolowana	Urząd Gminy w Ujeździe, Plac Kościuszki 6, 97-225 Ujazd (dalej: „Urząd")
Kierownik jednostki kontrolowanej	Artur Pawlak, Wójt Gminy Ujazd od dnia 1 grudnia 2014 r. (dowód: akta kontroli str. 2)
Okres objęty kontrolą	Od 1 czerwca 2017 r. do dnia zakończenia czynności kontrolnych w jednostce, tj. do 6 września 2018 r.

Wykaz skrótów i objaśnienie pojęć użytych w wystąpieniu:

- rozporządzenie KRI – rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[1];
- RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[2];
- administrator – zgodnie z definicją zawartą w RODO, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
- Administrator Bezpieczeństwa Informacji, ABI – osoba nadzorująca z upoważnienia administratora danych osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
- Administrator Systemów Informatycznych, ASI – osoba odpowiedzialna za funkcjonowanie systemu (-ów) lub sieci informatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci informatycznych;
- incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają prawdopodobieństwo zakłócenia działań biznesowych i zagrażają zachowaniu bezpieczeństwa informacji;

---

1 Dz. U. z 2017 r. poz. 2247.

2 Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1. Tekst rozporządzenia dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1527242776060&uri=CELEX:32016R0679

- Inspektor Ochrony Danych, IOD – wyznaczany w związku z art. 37 RODO. Zasadniczą rolą inspektorów ochrony danych jest doradzanie administratorowi danych i weryfikacja prawidłowości wykonywania obowiązków wynikających z przepisów prawa dotyczących przetwarzania danych;
- Polityka Bezpieczeństwa Informacji, PBI – zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce;
- System Zarządzania Bezpieczeństwem Informacji, SZBI – system stanowiący część całościowego systemu zarządzania, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

II. Ocena kontrolowanej działalności

Ocena ogólna i jej uzasadnienie

Najwyższa Izba Kontroli ocenia negatywnie[3] działalność Wójta Gminy Ujazd w zakresie zarządzania bezpieczeństwem informacji. W działalności Urzędu stwierdzono szereg nieprawidłowości, w tym m.in.:

- nie opracowano kompletnego systemu zarządzania bezpieczeństwem informacji, w szczególności polityki bezpieczeństwa informacji, co było niezgodne z § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI,
- identyfikacja posiadanych i przetwarzanych zbiorów danych podlegających zabezpieczeniu była niekompletna, co było działaniem nierzetelnym,
- nie zapewniono utrzymania 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,
- z uwagi na przechowywanie kopii zapasowych w tym samym pomieszczeniu, co zgromadzone dane oraz brak testowania tych kopii, nie zapewniono odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego na ochronie przed utratą, co stanowiło naruszenie § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI,
- nie przeszkolono osób zaangażowanych w proces przetwarzania informacji, co było niezgodne z § 20 ust. 2 pkt 6 rozporządzenia KRI (z wyjątkiem szkoleń związanych z wdrożeniem *RODO*),
- w 2017 r. nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI, który stanowi, że audyt wewnętrzny w zakresie bezpieczeństwa informacji przeprowadza się nie rzadziej niż raz na rok.

Ponadto, Najwyższa Izba Kontroli zwróciła uwagę m.in. na:

- udostępnienie *Instrukcji zarządzania systemami informatycznymi* wszystkim pracownikom w pełnym zakresie, wykraczającym poza wykonywane obowiązki,
- nieprowadzenie pisemnej dokumentacji dotyczącej zarządzania uprawnieniami użytkowników systemów informatycznych, którzy zostali pracownikami Urzędu przed 28 maja 2018 r.,
- brak ewidencji dostępu osób do pomieszczenia serwerowni.

W Urzędzie prawidłowo realizowano zadania dotyczące m.in.:

- przeprowadzenia aktualizacji uregulowań wewnętrznych w zakresie ochrony danych osobowych, pod kątem ich dostosowania do wymogów w zakresie ochrony danych osobowych w związku z wejściem w życie przepisów *RODO*,

[3] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

– powołania Inspektora Ochrony Danych i umożliwienia mu realizacji zadań w sposób niezależny, stosownie do art. 37 ust. 1 lit. a *RODO*,
– zapewnienia, że pracownicy Urzędu uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI.

III. Opis ustalonego stanu faktycznego

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Urzędzie nie zostały opracowane kompletne regulacje wewnętrzne składające się na System Zarządzania Bezpieczeństwem Informacji, wskazane w § 20 ust. 1 rozporządzenia KRI w związku z § 20 ust. 3 rozporządzenia KRI. Obowiązująca w Urzędzie *Polityka ochrony danych osobowych* oraz *Instrukcja zarządzania systemami informatycznymi*[4] dotyczyły bezpieczeństwa danych osobowych (opisano w punkcie 1 ustalonych nieprawidłowości). Zgodnie z wymogami wynikającymi z rozporządzenia KRI, ww. dokumentacja powinna odnosić się do wszystkich danych przetwarzanych w Urzędzie (nie zaś ograniczać do danych osobowych).

(dowód: akta kontroli, str. 85–148, 149–240, 284–298, 305–307, 450–452)

1.2. W związku z wejściem w życie RODO, w Urzędzie wprowadzono z dniem 28 maja 2018 r. *Politykę ochrony danych osobowych* oraz *Instrukcję zarządzania systemami informatycznymi.* Ponadto od 11 czerwca 2018 r. wprowadzono *Regulamin określający zasady i procedury korzystania z legalnego oprogramowania, sprzętu komputerowego, sieci komputerowej i poczty elektronicznej oraz zasady przeglądu oprogramowania w zakresie jego ważności, legalności i ochrony prawnej*[5].

Pracownicy Urzędu byli zobowiązani do przestrzegania ustaleń i zasad określonych w ww. uregulowaniach wewnętrznych i składali oświadczenia o zapoznaniu się z ich treścią.

Na tablicach informacyjnych oraz w Biuletynie Informacji Publicznej zostały zamieszczone klauzule informacyjne dla klientów Urzędu dotyczące przetwarzania i ochrony danych osobowych. Klauzule dla wykonawców zamówień publicznych zamieszczono na stronie BIP. Uruchomiono skrzynkę e-mail, służącą do kontaktu z powołanym w Urzędzie IOD. Kontrola wykazała, że korespondencja była odbierana. Opracowano wzory oświadczeń pracowników w zakresie przetwarzania danych osobowych, których podpisane egzemplarze przechowywano w aktach osobowych. Zostały przygotowane wzory umów z kontrahentami, zawierające uregulowania w zakresie administrowania danymi osobowymi, powierzenia ich przetwarzania oraz zabezpieczenia danych – prowadzono rejestr zawartych ww. umów.

(dowód: akta kontroli, str. 149–240, 287–292, 311–328)

1.3. Wprowadzając *Politykę ochrony danych osobowych* ustalono wykaz zabezpieczeń, w tym zasady ochrony fizycznej pomieszczeń i budynków. Do czasu kontroli zaktualizowano częściowo wykaz i strukturę zbiorów danych osobowych. W *Instrukcji zarządzania systemami informatycznymi* zaktualizowano procedury tworzenia kopii zapasowych.

(dowód: akta kontroli, str. 87–132, 139–141, 149–240, 246–247, 329–339, 345–395)

[4] Zarządzenie nr 95/2018 Wójta Gminy Ujazd z dnia 28 maja 2018 r.
[5] Zarządzenie nr 103/2018 Wójta Gminy Ujazd z dnia 11 czerwca 2018 r.

1.4. Na podstawie stosownych zarządzeń Wójta Gminy Ujazd wyznaczeni zostali pracownicy Urzędu na stanowiska odpowiedzialne za bezpieczeństwo informacji, tj. ABI (od 30 grudnia 2016 r.) i Zastępca Inspektora Ochrony Danych Osobowych (od 25 maja 2018 r.) – osoba ta z dniem 27 sierpnia 2018 r. została IOD. Określone zostały zakresy obowiązków na tych stanowiskach. ABI i IOD podlegali bezpośrednio Wójtowi. Ponadto zadania z zakresu bezpieczeństwa informacji należały od 1 czerwca 2017 r. do zakresu obowiązków pracownika zatrudnionego na stanowisku podinspektora ds. administrowania siecią i bezpieczeństwa informacji, który podlegał kierownikowi Referatu Organizacyjno-Administracyjnego. Ww. pracownicy posiadali kompetencje do pełnienia powierzonych im zadań z zakresu bezpieczeństwa informacji, poparte wykształceniem, praktyką zawodową, szkoleniami i kursami, obejmującymi również problematykę RODO.

(dowód: akta kontroli, str. 293–300, 305–307, 415–449, 453–454)

1.5. Zgodnie z art. 37 ust. 1 lit. a) RODO, 27 sierpnia 2018 r. w Urzędzie został wyznaczony IOD, o czym zawiadomiono Urząd Ochrony Danych Osobowych. Pracownik pełniący tę funkcję posiadał niezbędne kwalifikacje, wynikające z art. 37 ust. 5 RODO. Osoba ta pełniła wcześniej funkcję zastępcy IOD.

(dowód: akta kontroli, str. 415–431, 479–481)

1.6. W zmienionym w dniu 23 sierpnia 2018 r. Regulaminie Organizacyjnym Urzędu wyodrębniono IOD jako oddzielne stanowisko, podlegające bezpośrednio Wójtowi. Zakres zadań IOD został określony w ustalonym dla niego *Zakresie obowiązków, uprawnień i odpowiedzialności pracownika samorządowego*. Spełniono tym samym wymóg art. 38 ust. 1 RODO. Do obowiązków IOD należały również sprawy z zakresu kultury, zadania wynikające z ustawy o ochronie zabytków i opiece nad zabytkami, koordynacja udostępniania informacji publicznej, prowadzenie rejestru zarządzeń, upoważnień i pełnomocnictw wydanych przez Wójta. Wykonywanie tych obowiązków nie wywoływało konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO. (dowód: akta kontroli, str. 415–418, 456–477,)

1.7.-1.8 *Polityka ochrony danych osobowych* i *Instrukcja zarządzania systemami informatycznymi*, były dostępne dla wszystkich pracowników Urzędu – opublikowano je w całości na stronie BIP i przesłano pracownikom pocztą elektroniczną, nie tylko dla osób odpowiedzialnych za realizację poszczególnych czynności (dalszy opis w sformułowanych uwagach).

(dowód: akta kontroli, str. 119–257, 478)

1.9. W Urzędzie nie zidentyfikowano części zbiorów danych podlegających zabezpieczeniu, a realizowane w tym zakresie działania dotyczyły jedynie danych osobowych. W *Polityce ochrony danych osobowych* określono procedury identyfikacji zbiorów danych osobowych podlegających zabezpieczeniu, w tym wykaz aktywów. Sporządzony do czasu kontroli wykaz zbiorów danych osobowych nie obejmował wszystkich zbiorów (dalszy opis w punkcie 2 ustalonych nieprawidłowości). Dla każdego zbioru danych osobowych w wykazie określono techniczne i organizacyjne środki bezpieczeństwa.

(dowód: akta kontroli, str. 149–161, 188–189, 330, 345–395, 497–504)

1.10. W Urzędzie nie prowadzono wymaganej na podstawie § 20 ust. 2 pkt 2 rozporządzenia KRI inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację (dalszy opis w punkcie 3 ustalonych nieprawidłowości). Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił, że w około 75% zaawansowane są prace dotyczące opracowania i wdrożenia systemu ewidencjonującego zasoby sprzętowe. Osoby odpowiadające za dany sprzęt informatyczny wskazane były w ewidencji środków trwałych.

(dowód: akta kontroli, str. 26–30)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. W Urzędzie nie zostały opracowane kompletne regulacje wewnętrzne składające się na system zarządzania bezpieczeństwem informacji, w szczególności nie opracowano polityki bezpieczeństwa informacji.
   Było to niezgodne z § 20 ust. 1 rozporządzenia KRI stanowiącego, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto, § 20 ust. 3 rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-EN ISO/IEC 27001[6], a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[7]. W pkt. 5.1 normy PN-EN ISO/IEC 27002 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji.
   Wójt Gminy Ujazd wyjaśnił m.in., że w dniu 10 sierpnia 2018 r. Urząd zakupił Polskie Normy, na podstawie których powinno odbywać się zarządzenie bezpieczeństwem informacji. W oparciu o wytyczne zawarte w normach opracowana zostanie dokumentacja stanowiąca SZBI, w tym PBI. Urząd opracuje i wdroży procedury zarządzania: ryzykiem, konfiguracją, zmianami i wykonywania testów oraz procedury zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji w ramach przygotowania dokumentacji stanowiącej SZBI.
   (dowód: akta kontroli, str. 284–286, 289-291, 450–452)

2. W Urzędzie nie zidentyfikowano wszystkich posiadanych i przetwarzanych zbiorów danych (innych niż zbiory danych osobowych); nie sklasyfikowano ich z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację; nie przypisano informacjom odpowiedniego poziomu ochrony. Było to niezgodne z pkt. A.8.1.1 i A.8.2.1 załącznika A normy PN-EN ISO/IEC 27001:2017 stanowiącymi, że należy zidentyfikować informacje, aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów; informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację. Jak wyjaśniła Zastępca IOD w wykazie ujęto 25 zbiorów, tj. około połowę. Zakończenie opracowania wykazu przewidywane jest do końca października 2018 r.
   (dowód: akta kontroli, str. 149–161, 188–189, 330, 345–395, 497–504)

3. W Urzędzie nie prowadzono inwentaryzacji zasobów informatycznych, która zawierałaby pełne i aktualne informacje w zakresie posiadanego sprzętu

---

6 Polska Norma PN-EN ISO/IEC 27001:2017 *Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

7 W tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

informatycznego oraz jego konfiguracji, co było niezgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI.
Wójt Gminy Ujazd wyjaśnił m.in., że polecił stworzenie aktualnej bazy. Obecnie ewidencja zawiera spis wszystkich komputerów, ich podzespołów wraz z aktualnie zainstalowanym oprogramowaniem. Stworzona została baza użytkowników z opisem przynależności do referatów oraz osób odpowiedzialnych za poszczególne urządzenia i elementy sieci informatycznej. Zakończenie ewidencji sprzętu i oprogramowania planowane jest do 10 września 2018 r.

(dowód: akta kontroli, str. 2, 6–30, 259 i 260)

Uwagi dotyczące badanej działalności

Wszystkim pracownikom Urzędu została udostępniona *Instrukcja zarządzania systemami informatycznymi*, która zawierała m.in. uregulowania dotyczące zabezpieczeń fizycznych i technicznych, nadawania/cofania uprawnień, zabezpieczenia systemu informatycznego, wykonywania przeglądów i konserwacji, postępowania z nośnikami i sprzętem poza Urzędem. NIK zwraca uwagę, że szczegółowe informacje w tym zakresie powinny być udostępniane wyłącznie pracownikom odpowiedzialnym za realizację zadań wynikających z uregulowań, a nie wszystkim pracownikom Urzędu, ponieważ stwarza to ryzyko, że informacje w nich zawarte mogą być wykorzystane do przełamania ustanowionych w Urzędzie zabezpieczeń.

(dowód: akta kontroli, str. 241–257, 478)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Wójta Gminy Ujazd w zakresie organizacji bezpieczeństwa informacji. Ocenę uzasadnia przede wszystkim brak opracowania kompletnego SZBI, identyfikacji wszystkich zbiorów danych podlegających zabezpieczeniu, oraz nieposiadanie pełnej informacji o wykorzystywanych zasobach informatycznych.

2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji

Opis stanu faktycznego

2.1. W § 3 pkt 7 *Polityki Bezpieczeństwa Informacji* z 2015 r. oraz w *Regulaminie Ochrony Danych Osobowych* (załącznik nr 12 do *Polityki ochrony danych osobowych* z 28 maja 2018 r.) zawarty był zakaz samowolnego instalowania programów komputerowych przez pracowników. W trakcie oględzin 10 komputerów ustalono, że zalogowani do nich użytkownicy nie mieli przyznanych uprawnień administracyjnych, umożliwiających instalację dowolnego oprogramowania. Kontrola ustaliła również, że w Urzędzie zabezpieczono komputery przed nieautoryzowanym dostępem nośników pamięci przenośnej. Powyższe działania były zgodne z wymogami określonymi w § 20 ust. 2 pkt 4 rozporządzenia KRI.

(dowód: akta kontroli, str. 12–13, 29–31, 95, 218–229)

2.2. W Urzędzie określono, w *Instrukcji zarządzania systemem informatycznym* z 12 maja 2015 r. i w *Instrukcji zarządzania systemami informatycznymi* z 28 maja 2018 r., zasady nadawania/cofania uprawnień do pracy w systemach informatycznych w zakresie dotyczącym danych osobowych.

(dowód: akta kontroli, str. 135–138, 244–245, 253)

Na podstawie badania próby 15 użytkowników systemów informatycznych kontrola ustaliła, że wszyscy posiadali uprawnienia do pracy w systemach adekwatne do zakresu realizowanych zadań. Przed 28 maja 2018 r. pracownicy otrzymywali imienne upoważnienia do przetwarzania danych osobowych w określonych w upoważnieniu systemach informatycznych, a po 28 maja 2018 r. otrzymali nowe upoważnienia, zgodnie z zajmowanym stanowiskiem, do przetwarzania danych osobowych w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych, zgodne ze wzorem określonym w *Polityce Ochrony Danych*

Osobowych. Zgodnie z wymogiem *Polityki ochrony danych osobowych* sporządzono ewidencję osób upoważnionych do przetwarzania danych osobowych. Powyższe działania były zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI. W okresie objętym kontrolą nie wystąpił przypadek zmiany stanowiska pracy przez pracownika.
Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił, że przed wprowadzeniem w życie *Polityki ochrony danych osobowych* i *Instrukcji zarządzania systemami informatycznymi* z 28 maja 2018 r. uprawnienia dostępu do określonych systemów informatycznych – wewnętrznych, (administracyjno-księgowych) i zewnętrznych aplikacji (np. Geoportal, Besti@, KOBiZE) nadawał pracownikom po uzyskaniu od ich przełożonego ustnej informacji, do jakiego systemu pracownik został upoważniony. Czynności tej nie dokumentował, ponieważ nie było określonego takiego wymogu w obowiązujących wówczas uregulowaniach wewnętrznych.

(dowód: akta kontroli, str. 506–510, 511, 512–528, 552)

Tylko osobie przyjętej do pracy po 28 maja 2018 r. podinspektor ds. administrowania siecią i bezpieczeństwa informacji nadał uprawnienia użytkownika systemów informatycznych w sposób określony załącznikiem nr 2 (*Zlecenie modyfikacji uprawnień: nadania, zmiany, anulowania zakresu uprawnień użytkownika*) do *Instrukcji zarządzania systemami informatycznymi* z 28 maja 2018 r. Nadanie ww. uprawnień pracownikom zatrudnionym przed 28 maja 2018 r. nie zostało w ten sposób udokumentowane. Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił, że dla pracowników zatrudnionych przed 28 maja 2018 r. dokumentu tego nie sporządzał, ponieważ uważał, że ma on zastosowanie w przypadku nadawania nowych uprawnień (dalszy opis w punkcie 1 sformułowanych uwag).

(dowód: akta kontroli, str. 23, 25, 253, 552)

W wyniku kontroli ustalono, że jedna osoba, która nie była już pracownikiem Urzędu, posiadała upoważnienie do danych *Krajowej bazy o emisjach gazów cieplarnianych i innych substancji*, niezawierającej danych osobowych (dalszy opis w punkcie 3 ustalonych nieprawidłowości).

(dowód: akta kontroli, str. 544–551)

W Urzędzie nie uwzględniono w upoważnieniach i nie udokumentowano procesu nadania uprawnień 2 użytkownikom do pracy w systemie *BESTi@*, który nie służy przetwarzaniu danych osobowych (dalszy opis w punkcie 4 ustalonych nieprawidłowości).

(dowód: akta kontroli, str. 529–543, 657, 658)

2.3. W okresie objętym kontrolą pracę w Urzędzie zakończyło 6 pracowników, którzy mieli dostęp do systemów informatycznych. W wyniku oględzin 13 komputerów w referatach, w których osoby te były zatrudnione, ustalono, że ich konta w systemach informatycznych zostały usunięte. Zasady wyrejestrowania pracownika, którego zatrudnienie ustało, było uregulowane § 14 i § 15 *Instrukcji zarządzania systemem informatycznym* z 2015 r. – nie było wymagane dokumentowanie tego faktu. Odbieranie uprawnień dostępu do systemów informatycznych zostało sformalizowane od 28 maja 2018 r. – wprowadzono formularz „Zlecanie modyfikacji uprawnień: (...)". Do czasu kontroli zaistniał jeden przypadek odebrania uprawnień wg powyższej procedury – konto pracownika zostało usunięte w ostatnim dniu pracy. Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił, że wcześniej odbierał uprawnienia dostępu do systemów informatycznych osobom, które zakończyły pracę w Urzędzie, po uzyskaniu o tym informacji od przełożonego danego pracownika, lecz nie było to dokumentowane.

(dowód: akta kontroli, str. 21–26, 137–138)

2.4. Wymogi dotyczące złożoności haseł do systemów informatycznych zostały określone w *Instrukcji zarządzania systemami informatycznymi*. W myśl tych zasad, każdy z użytkowników winien stosować hasła o wymaganej złożoności (składające się z 12 znaków), z częstotliwością wymuszaną przez system. Komputery Urzędu nie były zarządzane centralnie w oparciu o mechanizm *Active Directory*. W Instrukcji nie zróżnicowano wymogów złożoności haseł w zależności od istotności informacji i rodzaju systemu. W wyniku badania 10 stanowisk komputerowych (na których pracowano łącznie w 7 systemach) ustalono, że: użytkownicy posiadają unikalne identyfikatory; nie nastąpiło automatyczne logowanie do komputera bez wprowadzania hasła; hasła miały co najmniej 12 znaków. W rejestrze operatorów w przypadku 2 komputerów wykazane były odpowiednio daty zmiany hasła – 2015-12-14 i 2016-02-03. Mimo dokonanej w trakcie badania zmiany hasła daty te w rejestrze operatorów pozostały niezmienione. Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił, po konsultacjach z serwisem oprogramowania systemów księgowych, że przyczyną nieaktualizowania się daty zmiany hasła była niewłaściwa konfiguracja konta użytkownika w chwili tworzenia konta. Ustawienia konta zostały niezwłocznie poprawione. W Urzędzie nie korzystano w celach służbowych z adresów poczty elektronicznej zamieszczonych na serwisach komercyjnych.

(dowód: akta kontroli, str. 245–246, 279–280, 281–283)

2.5. Na dwóch stanowiskach pracy realizujących zadania m.in. z zakresu wydawania dowodów osobistych oraz na pięciu stanowiskach w Referacie Planowania Przestrzennego i Gospodarki Komunalnej i trzech stanowiskach w Referacie Podatków i Opłat monitory zostały usytuowane w sposób uniemożliwiający interesantom wgląd do wyświetlanych danych. W punkcie 1.4 załącznika nr 12 do *Polityki ochrony danych osobowych* zobowiązano pracowników do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych. Powyższe działanie spełniało wymogi § 20 ust. 2 pkt 7 rozporządzenia KRI.

(dowód: akta kontroli, str. 14, 218–220)

2.6. W Urzędzie ustanowiono procedury[8] umożliwiające bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, zgodnie z wymogiem § 20 ust. 2 pkt 8 rozporządzenia KRI. Z dwóch pracowników, którzy użytkowali komputery przenośne jedna osoba potwierdziła zapoznanie się z regulaminem użytkowania komputerów przenośnych i zobowiązała do jego stosowania; druga osoba nie miała możliwości zapoznania się z regulaminem z powodu usprawiedliwionej nieobecności. W ramach ww. procedur opisano zasady korzystania ze sprzętu informatycznego minimalizujące ryzyka kradzieży informacji — dysk szyfrowany, zabezpieczenie hasłem, zabezpieczenia w czasie transportu. W procedurach tych nie zawarto obowiązku podłączenia przez pracowników Urzędu komputerów przenośnych do lokalnej sieci komputerowej jednostki w celu aktualizacji oprogramowania. Wójt Gminy Ujazd wyjaśnił, że komputery te nie były używane do pracy z bazami danych Urzędu. Były w nich użytkowane pakiety biurowe. Dalszy opis w punkcie 2 sformułowanych uwag.

(dowód: akta kontroli, str. 256–257, 575–579)

2.7. Zgodnie z postanowieniami Regulaminu użytkowania komputerów przenośnych, dyski w będących w użyciu trzech komputerach przenośnych były zaszyfrowane. Dodatkowym zabezpieczeniem były hasła dostępu do kont użytkowników. W przypadkach potrzeby przeniesienia danych pracownicy korzystali z jednego

---

[8] Regulamin użytkowania komputerów przenośnych w urzędzie Gminy w Ujeździe, stanowiący załącznik nr 5 do *Instrukcji zarządzania systemami informatycznymi*

służbowego, zaszyfrowanego pendrive. Działania te zminimalizowały ryzyko nieuprawnionego dostępu do informacji, zgodnie z wymogami § 20 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(dowód: akta kontroli, str. 250, 256–257, 277, 278)

2.8. W serwerowni Urzędu zastosowano zabezpieczenia fizyczne w celu uniemożliwienia nieuprawnionemu ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji, stosownie do wymogu § 20 ust. 2 pkt 9 rozporządzenia KRI. Serwery umieszczone były w wyodrębnionym pomieszczeniu, posiadającym m.in. klimatyzację i zabezpieczenia przeciwwłamaniowe oraz przeciwpożarowe. Zapewniono podtrzymanie zasilania poprzez wyposażenie serwera w zasilacz UPS. W trakcie kontroli NIK trwały uzgodnienia z gestorem sieci elektrycznej warunków włączenia zakupionego już agregatu prądotwórczego dla potrzeb zasilania sieci informatycznej. Podjęto działania zmierzające do zainstalowania sieci elektrycznej przeznaczonej wyłącznie dla sprzętu komputerowego. Nie prowadzono ewidencji wejść/wyjść do pomieszczenia serwerowni (dalszy opis w punkcie 3 sformułowanych uwag).

(dowód: akta kontroli, str. 3–11, 15–20, 74–83, 258)

2.9. W wyniku badania pięciu z 13 obowiązujących w okresie objętym kontrolą umów z kontrahentami, dotyczących dostaw sprzętu informatycznego i/lub świadczenia usług telekomunikacyjnych/serwisowych/utrzymaniowych, ustalono, że w czterech[9] z nich zostały zawarte wymogi dotyczące zachowania poufności informacji, uzyskanych w związku z realizacją umowy. W przypadku jednej umowy[10] nie zawarto takich postanowień (dalszy opis w punkcie 1 ustalonych nieprawidłowości).

Zasady zachowania poufności zostały także określone w umowie powierzenia przetwarzania danych osobowych, zawartej przez Urząd z dostawcą usługi poczty elektronicznej. Postanowienia dotyczące prywatności i ochrony danych osobowych zawierał również regulamin świadczenia usług przez dostawcę usługi.

(dowód: akta kontroli, str. 580–603, 503, 553–574)

2.10. W Urzędzie zostały określone zasady dotyczące postępowania w przypadku przekazywania sprzętu informatycznego poza jednostkę. W rozdziale 9 *Instrukcji zarządzania systemami informatycznymi* (w rozdziale *Procedura wykonywania przeglądów i konserwacji*) przewidziano w przypadku napraw dokonywanych na zewnątrz wymontowanie dysków i wszelkich nośników z komputerów oraz kart pamięci z urządzeń mobilnych. W przypadku naprawy sprzętu z danymi na nośniku, dane te mają być zaszyfrowane, a sprzęt przekazany do serwisu bez podania hasła. Kontrola wykazała, że w okresie od 1 czerwca 2017 r. w Urzędzie wystąpił jeden przypadek przekazania sprzętu komputerowego (laptopa) do serwisu — sprzęt przekazano po wymontowaniu dysku twardego. Nie została określona procedura postępowania w przypadku zbycia sprzętu. Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił, że w Urzędzie nie praktykuje się zbywania sprzętu informatycznego, wyeksploatowany sprzęt poddawany jest kasacji.

(dowód: akta kontroli, str. 249–250, 485–487)

---

[9] 1. Umowa z 2.01.2017 r. z INFOSERWIS, dystrybutorem oprogramowania firmy Usługi Informatyczne INFO-SYSTEM Roman i Tadeusz Groszek s.j., dotycząca warunków serwisu oprogramowania. 2. Zlecenie nr 272.2.359.2017 z 12.12.2017 r. zakupu sprzętu komputerowego z firmy COCON Systemy komputerowe 3. Zlecenie nr 272.2.360.2017 z 12.12.2017 r. zakupu oprogramowania z firmy COCON Systemy komputerowe; 4. umowa z 29.12.2017 r. z INFOSERWIS, dystrybutorem oprogramowania firmy Usługi Informatyczne INFO-SYSTEM Roman i Tadeusz Groszek s.j. dotycząca warunków serwisu oprogramowania ;

[10] Umowa dzierżawy z 16 lipca 2018 r. urządzenia drukującego, z firmą Arcus S.A.

Ustalone nieprawidłowości

W działalności Urzędu w zakresie wdrożonych i wykorzystywanych rozwiązań organizacyjnych i technicznych zapewniających bezpieczeństwo informacji, stwierdzono następujące nieprawidłowości:

1. Wbrew wymogom określonym w § 20 ust. 2 pkt 10 rozporządzenia KRI, w zawartej w dniu 16 lipca 2018 r. umowie dzierżawy urządzenia drukującego (jedna z pięciu skontrolowanych umów), obejmującej zakresem m.in. świadczenie usług serwisowych, nie uwzględniono zapisów o zachowaniu w tajemnicy informacji uzyskanych/przetwarzanych w związku z realizacją tej umowy. Objęte umową urządzenie zostało wyposażone w pamięć umożliwiającą przechowanie dokumentów przeznaczonych do druku. Wójt Gminy Ujazd wyjaśnił, że w chwili podpisywania umowy zakładano, iż wszystkie czynności serwisowe będą odbywać się w siedzibie Urzędu pod nadzorem pracownika odpowiedzialnego za bezpieczeństwo informacji. W przypadku konieczności zabrania urządzenia przez serwis przygotowany zostałby dokument przekazania, zawierający klauzulę tajemnicy informacji. Zdaniem NIK brak zawarcia w umowie stosownych zapisów o zachowaniu w tajemnicy informacji uzyskanych w związku z realizacją umowy stwarzał ryzyko uzyskania nieautoryzowanego dostępu do informacji przechowywanych w tym urządzeniu.

   (dowód: akta kontroli, str. 598–603, 657,658)

2. Kopie zapasowe znajdowały się w tym samym pomieszczeniu co serwery z danymi. Nie były one także regularnie testowane, a w *Instrukcji zarządzania systemami informatycznymi* nie określono zasad testowania kopii. W Urzędzie nie zostało wprowadzone przewidziane w Instrukcji duplikowanie kopii w przestrzeni chmurowej, wyodrębnionej na zasobach dyskowych. Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił m.in., że w momencie wprowadzania instrukcji (28 maja 2018 r.) były podjęte prace wdrożeniowe w ramach przedsięwzięcia realizowanego z udziałem czterech jednostek samorządowych. Wdrożenie przewiduje się do końca września 2018 r. Nie określono zasad ich testowania.

   W ocenie NIK taki sposób postępowania nie zapewniał odpowiedniego poziomu bezpieczeństwa w systemie informatycznym, wymaganego § 20 ust. 2 pkt 12 rozporządzenia KRI. Równocześnie NIK zwraca uwagę, że zgodnie z pkt. A.12.3.1 normy PN-ISO/IEC 27001:2014-12 kopie zapasowe należy regularnie testować, zgodnie z ustaloną polityką kopii zapasowych.

   (dowód: akta kontroli, str. 241–247, 261–266)

3. W *Krajowej bazie o emisjach gazów cieplarnianych i innych substancji*, która nie służyła do przetwarzania danych osobowych, wpisana była jako upoważniony przedstawiciel m.in. inspektor, która od 27 września 2017 r. nie była pracownikiem Urzędu, co naruszało wymogi określone w § 20 ust. 2 pkt 5 rozporządzenia KRI. Kierownik Referatu Planowania Przestrzennego i Gospodarki Komunalnej wyjaśnił, że aktualizacji danych – cofnięcia uprawnień dla ww. osoby – nie dokonano wskutek przeoczenia. W związku z powyższym ustaleniem kontroli NIK w dniu 3 września 2018 r. został sporządzony i przesłany do *Krajowej bazy o emisjach gazów cieplarnianych i innych substancji* wniosek o usunięcie ww. byłego pracownika z tej bazy.

   (dowód: akta kontroli, str. 544–551)

4. W Urzędzie nie uwzględniono w upoważnieniach i nie udokumentowano procesu nadania uprawnień 2 użytkownikom do pracy w systemie *BeSTi@*, który nie służył przetwarzaniu danych osobowych, co naruszało wymogi określone w § 20

2.11. Stosownie do § 20 ust. 2 pkt 12 lit. a i f rozporządzenia KRI w Urzędzie przeprowadzano aktualizacje systemów operacyjnych. System operacyjny Windows XP zainstalowany był na jednym komputerze stacjonarnym, który nie miał uprawnień do baz danych Urzędu. Systemy operacyjne na pozostałych 33 komputerach stacjonarnych i czterech laptopach były objęte wsparciem producenta.

(dowód: akta kontroli, str. 267)

2.12. Zasady dotyczące tworzenia i przechowywania kopii zapasowych danych w Urzędzie zostały określone w *Instrukcji zarządzania systemami informatycznymi*. Zgodnie z Instrukcją zabezpieczono dostęp do miejsca przechowywania kopii. Proces tworzenia kopii został zautomatyzowany w oparciu o skrypt wykorzystujący programowe funkcje serwera – tworzono je z częstotliwością określoną w ww. Instrukcji na wydzielonej przestrzeni serwera i na dysku wymiennym Backup, znajdującym się również w serwerowni. Kopie zapasowe znajdowały się w serwerowni. Nie określono zasad ich testowania. Dalszy opis w punkcie 2 ustalonych nieprawidłowości. W okresie objętym kontrolą nie wystąpiły przypadki konieczności odtworzenia danych z kopii zapasowych.

(dowód: akta kontroli, str. 241–247, 261–266)

2.13. Na podstawie oględzin 10 komputerów ustalono, że był na nich zainstalowany i uruchomiony program antywirusowy, który wykorzystywał aktualną na moment badania wersję bazy definicji wirusów. Było to zgodne z § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI.

(dowód: akta kontroli, str. 32–60, 65–73)

2.14. W ramach obowiązujących w Urzędzie uregulowań nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Urzędu. Stosownie do zalecenia, sformułowanego w pkt A.12.1.3 załącznika A normy PN-ISO/IEC 27001:2017, pojemność była na bieżąco monitorowana, lecz niedokumentowana. Podinspektor ds. administrowania siecią i bezpieczeństwa informacji wyjaśnił, że poziom zajętości dysków był bezpieczny dla procesu zapisu danych, zwiększenie pojemności dysków będzie wymagane po osiągnięciu 75% zajętości.

Na podstawie oględzin dwóch serwerów wykorzystywanych w Urzędzie ustalono, że aktualna zajętość dysków twardych w obu serwerach nie przekraczała 50%. Pozostała do wykorzystania przestrzeń dysków była wystarczająca dla sprawnej pracy systemu i pozwalała na wcześniejsze przygotowanie się do zwiększenia dostępnej pojemności.

(dowód: akta kontroli, str. 61–64)

2.15. W uregulowaniach Urzędu z zakresu bezpieczeństwa informacji zostały uwzględnione niektóre działania, związane z zarządzaniem zmianami w wykorzystywanym oprogramowaniu. W *Instrukcji zarządzania systemami informatycznymi* została określona procedura wykonywania przeglądów i konserwacji systemów informatycznych, która stanowiła m.in., że wszelkie uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych. W instrukcji określono także obowiązki informatyka w zakresie sprawdzania poprawności działania systemu IT, identyfikacji i przyjmowania zgłoszeń o nieprawidłowościach w działaniu oprogramowania celem ich usunięcia.

(dowód: akta kontroli, str. 249–250)

2.16. Stosownie do art. 30 RODO, IOD sporządził i prowadził rejestr czynności przetwarzania. Rejestr zawierał informacje wynikające z art. 30 RODO, w tym ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, stosowanych zgodnie z wymaganiami art. 32 ust. 1 RODO.

(dowód: akta kontroli, str. 604–656)

ust. 2 pkt 5 rozporządzenia KRI. Wójt Gminy Ujazd wyjaśnił m.in., że do 28 maja 2018 r. uprawnienia dostępu do określonych systemów informatycznych, w tym do programu Besti@, były nadawane, lecz czynności tych nie dokumentowano, gdyż nie wynikało to z obowiązującej wówczas *Instrukcji zarządzania systemami informatycznymi*; zgodnie z obecnie obowiązującymi procedurami proces ten jest dokumentowany tylko dla pracowników przyjętych po dacie wprowadzenia nowej *Instrukcji zarządzania systemami informatycznymi*; wcześniej nadanych uprawnień nie ujęto w dokumentacji.

(dowód: akta kontroli, str. 529–543, 657, 658)

Uwagi dotyczące badanej działalności

1. NIK zwraca uwagę, że dla pracowników zatrudnionych przed 28 maja 2018 r. nie udokumentowano przydzielonych uprawnień użytkownika systemów informatycznych w sposób określony w załączniku nr 2 („Zlecenie modyfikacji uprawnień: nadania, zmiany, anulowania zakresu uprawnień użytkownika") do *Instrukcji zarządzania systemami informatycznymi* z 28 maja 2018 r.
2. W obowiązujących w Urzędzie procedurach nie zawarto obowiązku podłączenia przez pracowników komputerów przenośnych do lokalnej sieci komputerowej jednostki w celu aktualizacji oprogramowania. NIK zwraca uwagę, że regularne podłączenia pozwalają pracować na aktualnych ustawieniach systemu operacyjnego. W przeciwnym razie może to skutkować zmniejszeniem bezpieczeństwa informatycznego.
3. W Urzędzie nie była prowadzona ewidencja dostępu do pomieszczenia serwerowni. Zdaniem NIK, wprowadzenie ewidencji wejść i wyjść do serwerowni wpłynie na zwiększenie bezpieczeństwa infrastruktury IT zlokalizowanej w tym pomieszczeniu.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie wdrożone i wykorzystywane w Urzędzie Gminy Ujazd rozwiązania organizacyjne i techniczne, które nie zapewniały bezpieczeństwa informacji.

3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. Wymagany § 20 ust. 2 pkt 3 rozporządzenia KRI obowiązek przeprowadzania cyklicznej analizy ryzyka związanego z bezpieczeństwem informacji uregulowany został zarządzeniem Wójta Gminy Ujazd z dnia 5 kwietnia 2018 r.[11] w odniesieniu do przetwarzania danych osobowych. W zarządzeniu tym określono szczegółowe zasady procesu analizy ryzyka utraty poufności, rozliczalności i integralności, oraz zasady dokumentowania przeprowadzonej analizy.
Dokonana w maju 2018 r. ocena i analiza ryzyka dla poufności, rozliczalności i integralności wykazała jego średni poziom. Wskazano działania naprawcze, jakie podejmie Administrator Danych Osobowych w celu wyeliminowania zagrożeń.

(dowód: akta kontroli, str. 396–414)

3.2. Opracowana w Urzędzie, w treści *Polityki ochrony danych osobowych*, *Instrukcja postępowania z incydentami* definiowała katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisywała sposób reagowania na nie. Pracownicy Urzędu zostali zapoznani z Instrukcją i zobowiązani do stosowania jej zasad.

[11] Zarządzenie nr 55/2018 Wójta Gminy Ujazd z dnia 5 kwietnia 2018 r. w sprawie określenia Zasad przeprowadzania analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych.

W okresie od 1 czerwca 2017 r. w Urzędzie nie odnotowano wystąpienia incydentów z zakresu naruszenia bezpieczeństwa informacji, w tym dotyczących danych osobowych, z wyjątkiem krótkotrwałych braków zasilania, które nie wymagały stosowania zabezpieczeń innych niż zasilacze UPS.

(dowód: akta kontroli, str. 149–159, 216–217, 478, 482–484)

3.3. Szkolenia, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, pracowników Urzędu zaangażowanych w proces przetwarzania informacji związane były z ochroną danych osobowych.

W październiku 2016 r. firma zewnętrzna przeprowadziła w Urzędzie szkolenie pt. „Ochrona danych osobowych w instytucjach publicznych". Szkolenie obejmowało zagadnienia ochrony i bezpieczeństwa danych osobowych, kontroli ich przetwarzania, zagrożeń i zasad zabezpieczeń. W szkoleniu uczestniczyli wszyscy obecni wówczas pracownicy (33 osoby). W okresie objętym kontrolą 4 pracowników uczestniczyło w szkoleniach zewnętrznych dotyczących ochrony danych osobowych w związku RODO. IOD uczestniczyła w 4 szkoleniach, inspektor ds. administrowania siecią i bezpieczeństwa informacji w 2 szkoleniach, sekretarz w 1 szkoleniu i kierownik Referatu Organizacyjno-Administracyjnego w 1 szkoleniu. W sierpniu i wrześniu 2018 r., w związku z wejściem w życie przepisów RODO, 26 osób uczestniczyło w wewnętrznym szkoleniu z zakresu zasad ochrony danych osobowych, z uwzględnieniem zagrożeń bezpieczeństwa informacji. Wójt Gminy Ujazd wyjaśnił, że w tematyce szkolenia uwzględniono zapisy §20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli, str.287– 292, 491-494, 659, 660)

3.4. Ostatni audyt wewnętrzny z zakresu bezpieczeństwa informacji, w tym ochrony danych osobowych, przeprowadzono w Urzędzie w 2016 r. W 2017 r. i w 2018 r. (do czasu kontroli) audytu z zakresu bezpieczeństwa informacji nie przeprowadzono (dalszy opis w punkcie 1 ustalonych nieprawidłowości).

(dowód: akta kontroli, str. 159, 238, 488–496, 331–339, 505)

3.5. W związku z wejściem w życie przepisów RODO została przeprowadzona w Urzędzie szczegółowa analiza procesów przetwarzania danych osobowych i dokonano oceny stopnia zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk, o której mowa w art. 32 RODO.

(dowód: akta kontroli, str. 397–414, 495–496, 661–694)

Ustalone nieprawidłowości

W działalności Urzędu w zakresie podejmowanych działań w celu zapobiegania incydentom bezpieczeństwa informacji stwierdzono następującą nieprawidłowość:

W 2017 r. w Urzędzie nie został przeprowadzony audyt z zakresu bezpieczeństwa informacji. Było to niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. Wójt Gminy Ujazd wyjaśnił, że w budżecie gminy na lata 2017 i 2018 zabezpieczono środki na przeprowadzenie audytu z zakresu bezpieczeństwa informacji, jednak z uwagi na czynności zmierzające do wprowadzenia elektronicznego obiegu dokumentów EZD PUW, przebudowę i modernizacje serwerowni, nie było technicznych możliwości przeprowadzenia audytu. Planuje się jego przeprowadzenie do grudnia 2018 r.

(dowód: akta kontroli, str. 159, 238, 489–496)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie działania Urzędu w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na nieprzeprowadzenie w 2017 r. audytu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[12], wnosi o:

1) opracowanie i wdrożenie kompletnego systemu zarządzania bezpieczeństwem informacji, spełniającego wymogi rozporządzenia KRI;
2) prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację;
3) sporządzenie wykazu wszystkich zbiorów danych podlegających zabezpieczeniu;
4) zapewnienie dokumentowania procesu nadawania uprawnień do wszystkich systemów informatycznych w Urzędzie;
5) zawieranie w umowach z podmiotami zewnętrznymi, świadczącymi usługi informatyczne dla Urzędu, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
6) wdrożenie rozwiązań mających na celu ochronę danych przed utratą, poprzez przechowywanie kopii zapasowych poza miejscem ich wytwarzania;
7) regularne testowanie kopii zapasowych;
8) zapewnienie prowadzenia okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Łodzi.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Łódź, dnia 19 września 2018 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Piotr Rydygier
Główny specjalista kontroli państwowej

podpis

Dyrektor
Przemysław Szewczyk

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Łodzi
z up.
Grażyna Tużikiewicz-Gnitecka
wicedyrektor

podpis

[12] Dz. U. z 2017 r., poz. 524 ze zm.