NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.015.05.2018
P/18/006

# WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

# I. Dane identyfikacyjne kontroli

| | |
|---|---|
| *Numer i tytuł kontroli* | P/18/006 – Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego"[1] |
| *Jednostka przeprowadzająca kontrolę* | Najwyższa Izba Kontroli<br>Delegatura w Krakowie |
| *Kontroler* | Małgorzata Kram, specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/157/2018 z dnia 27 sierpnia 2018 r. |
| | (dowód: akta kontroli str. 1 do 2) |
| *Jednostka kontrolowana* | Urząd Miasta Jordanów[2] (dalej: *Urząd)* |
| *Kierownik jednostki kontrolowanej* | Iwona Bilska (dalej: *Burmistrz)* |
| | (dowód: akta kontroli str. 102) |

# II. Ocena kontrolowanej działalności

**Ocena ogólna**

Najwyższa Izba Kontroli ocenia pozytywnie mimo stwierdzonych nieprawidłowości[3] działalność Burmistrza w zakresie zarządzania bezpieczeństwem informacji. W Urzędzie podejmowano działania na rzecz zapewnienia bezpieczeństwa informacji, zapewniono organizację bezpieczeństwa informacji, wprowadzono zabezpieczenia techniczne w celu zapewnienia ochrony przetwarzanych informacji, nie podjęto jednak niezbędnych działań mających na celu zapobieganie incydentom bezpieczeństwa, tj. nie prowadzono okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia 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[4], oraz w Urzędzie nie przewidziano formalnych rozwiązań związanych z ryzykiem wystąpienia zakłóceń w normalnym funkcjonowaniu środowiska informatycznego w związku z wdrażaniem nowych wersji oprogramowania (dotyczących tzw. zarządzania zmianą). Ponadto w 2017 r. w Urzędzie nie został przeprowadzony audyt wewnętrzny z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. W Urzędzie natomiast:

- opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji, zgodnie z § 20 ust. 1 w związku z ust. 3 rozporządzenia KRI,
- zaktualizowano na dzień 25 maja 2018 r. obowiązującą w Urzędzie dokumentacji w zakresie ochrony danych osobowych pod kątem dostosowania do wymogów wynikających z przepisów rozporządzenia 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)[5],
- przeprowadzono analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych, o której mowa w art. 32 RODO.

[1] Kontrolą objęto okres od 1 czerwca 2017 r. do czasu zakończenia czynności kontrolnych w jednostce kontrolowanej.
[2] Urząd Miasta Jordanów, ul. Rynek 1, 34-240 Jordanów
[3] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.
[4] Dz. U. z 2017 r. poz. 2247, dalej: *rozporządzenie KRI*.
[5] Dz. Urz. UE L119 z 4.05.2016, str. 1, ze zm., dalej: *RODO*.

W Urzędzie prawidłowo monitorowano zajętość dysków i prowadzono aktualizację oprogramowania systemowego oraz sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono również wymóg przechowywania kopii zapasowych poza miejscem ich wytworzenia, zabezpieczono serwerownię. Komputery Urzędu zostały zabezpieczone przed szkodliwym oprogramowaniem i nie pozostawiono możliwości instalowania dowolnego oprogramowania użytkownikom niebędącym pracownikami służb informatycznych, co było zgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI.

# III. Opis ustalonego stanu faktycznego

## 1. Organizacja bezpieczeństwa informacji.

Opis stanu faktycznego

1.1. W Urzędzie opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji. Zapisy odnoszące się do bezpieczeństwa informacji zamieszczono w nw. dokumentach:

- Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym wprowadzona Zarządzeniem Nr 99/2015 Burmistrza Miasta Jordanowa z dnia 25 października 2015 r., która regulowała m.in.: cele polityki bezpieczeństwa danych osobowych; podstawowe zasady przetwarzanych w Urzędzie informacji w tym ochrony danych osobowych; powierzenie przetwarzania danych osobowych, udostępnianie danych osobowych; wykaz budynków, pomieszczeń lub i części tworzących obszar w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania; opis struktury zbiorów danych; opis sposobu przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych; postępowanie w przypadku stwierdzenia naruszenia ochrony danych osobowych; przepisy karne i porządkowe.

- Aktualizacja Polityki Bezpieczeństwa i Instrukcja Zarzadzania Systemem Informatycznym wprowadzona Zarządzeniem Nr 46/2017 Burmistrza Miasta Jordanowa z dnia 11 sierpnia 2017 r., wprowadziła aktualizację Polityki Bezpieczeństwa Danych Osobowych Urzędu Miasta Jordanowa i Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych Urzędu Miasta Jordanowa. związaną z wdrażaniem nowych programów księgowo-budżetowych, podatkowych w ramach realizowanego projektu unijnego „E-Jordanów – wdrażanie innowacyjnych i kompleksowych usług publicznych w Mieście Jordanowie”.

- Polityka Ochrony Danych Urzędu Miasta Jordanowa wprowadzona Zarządzeniem Nr 25/2018[6] Burmistrza Miasta Jordanowa z dnia 26 czerwca 2018 r. reguluje m.in.: cel wdrażania polityki ochrony danych; podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych; podstawy przetwarzania danych osobowych, środki techniczne i organizacyjne zapewniające bezpieczeństwo danych ;obowiązki po stronie użytkowników; przenośne nośniki danych oraz komputery przenośne; sposób, miejsce i okres przechowywania elektronicznych nośników informacji zwierających dane osobowe oraz nośników kopii zapasowych; pracę w systemach informatycznych; sposób postępowania z dokumentami papierowymi zwierającymi dane osobowe, przesyłanie dokumentów za pośrednictwem poczty elektronicznej, szkolenia z ochrony danych osobowych; umowy powierzenia; procedurę zgłaszania naruszeń danych osobowych; bezpieczeństwo informacji; przeprowadzanie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji; audyt wewnętrzny w zakresie bezpieczeństwa informacji.

- Regulamin funkcjonowania, obsługi i eksploatacji monitoringu wizyjnego na terenie Urzędu Miasta Jordanowa oraz obszarze miejscowości Jordanów wprowadzony

[6] dalej: Zarządzenie nr 25/2018.

Zarządzeniem nr 17/2018 Burmistrza Miasta Jordanowa z 25 maja 2018 r., który reguluje zagadnienia m.in. związane z funkcjonowaniem monitoringu i jego celów.

Urząd działał na podstawie Statutu Urzędu Miasta Jordanowa przyjętego Uchwałą Rady Miasta Jordanowa Nr XIV/118/2015 z dnia 29 grudnia 2015 r. w sprawie nadania statutu Urzędu Miasta Jordanowa ze zmianami[7].

Regulamin Organizacyjny Urzędu Miasta Jordanowa został przyjęty Zarządzeniem wewnętrznym Nr 34/2017 Burmistrza Miasta Jordanowa z dnia 12 grudnia 2017 r. w sprawie nadania regulaminu Organizacyjnego Urzędu Miasta Jordanowa ze zmianami wprowadzonymi Zarządzeniem wewnętrznym Nr 6/2018 Burmistrza Miasta Jordanowa z dnia 5 marca 2018 r. w sprawie zmiany Regulaminu Organizacyjnego Urzędu Miasta Jordanowa. Zmiana dotyczyła m.in. § 34 związanego z zadaniami Inspektora Ochrony Danych wynikającymi z art. 39 RODO

(dowód: akta kontroli str. 3 do 15, 16 do 31)

1.2. W okresie objętym kontrolą w Urzędzie obowiązywały następujące uregulowania w zakresie ochrony danych osobowych:

- Polityka Bezpieczeństwa i Instrukcja Zarzadzania Systemem Informatycznym wprowadzona Zarządzeniem Nr 99/2015 Burmistrza Miasta Jordanowa z dnia 25 października 2015 r.,
- Aktualizacja Polityki Bezpieczeństwa i Instrukcja Zarzadzania Systemem Informatycznym wprowadzona Zarządzeniem Nr 46/2017 Burmistrza Miasta Jordanowa z dnia 11 sierpnia 2017 r.,
- Polityka Ochrony Danych Urzędu Miasta Jordanowa wprowadzona Zarządzeniem Nr 25/2018 Burmistrza Miasta Jordanowa z dnia 26 czerwca 2018 r.

Ww. zarządzeniach wprowadzających uregulowania w zakresie bezpieczeństwa danych osobowych ochrony zasobów informatycznych zobowiązano wszystkich pracowników do stosowania zasad, określonych w tych dokumentach. Opracowano także wzory oświadczeń dla pracowników w zakresie przetwarzania danych osobowych, których podpisane egzemplarze przechowywano w Urzędzie. Dokumentacja uwzględniła wymogi RODO.

(dowód: akta kontroli str. 3 do 6, 7 do 15, 164, 167)

W dniu 23 maja 2018 r. przeprowadzono audyt zewnętrzny dotyczący m.in. analizy ryzyka w zakresie danych osobowych realizowany przez firmę zewnętrzną zajmującą się audytem, doradztwem finansowym i gospodarczym. Zadanie realizowano na podstawie umowy nr AGP.272.1.2018.KW z dnia 27 kwietnia 2018 r. w sprawie pełnienia na rzecz Urzędu *funkcji Administratora Bezpieczeństwa Informacji (ABI) oraz świadczenia doradztwa informatycznego a po 25 maja 2018 r. wykonywania funkcji Inspektora Ochrony Danych Osobowych zgodnie z wymogami RODO*. Realizację ww. przewidziano na okres od 1 maja 2018 r. do 31 grudnia 2018 r.

(dowód: akta kontroli str. 53 do 75, 146 do 159)

1.3. W Urzędzie wyznaczono pracowników odpowiedzialnych za bezpieczeństwo informacji. Burmistrz na podstawie zawartej umowy (opisanej powyżej w punkcie 1.2) wyznaczył pracownika Zleceniobiorcy[8] na stanowisko Inspektora Ochrony Danych. Zrealizował tym samym wymogi art. 37 ust. 1 RODO. Zgodnie z art. 37 ust. 5 RODO, wyznaczony IOD posiadał odpowiednie kwalifikacje zawodowe do pełnienia tej funkcji. Burmistrz określił także w zakresie czynności Informatyka zadania administratora systemów informatycznych.

(dowód: akta kontroli str. 97 do 101, 164, 146 do 159)

[7] Uchwała Rady Miasta Jordanowa Nr XXII /183/2016 z dnia 21 listopada 2016r. r. ws. zmiany statutu Urzędu Miasta Jordanowa; Uchwała Rady Miasta Jordanowa Nr XXXIII /301/2017 z dnia 28 grudnia 2016r. r. ws. zmiany statutu Urzędu Miasta Jordanowa.

[8] Zleceniobiorca poinformował w dniu 25 maja 2018 r., że IOD będzie M. C-W., której udzielił pisemnego upoważnienia do realizacji czynności określonych w umowie.

1.4. Regulamin Organizacyjny Urzędu przewidywał zlecenie zadań IOD podmiotowi zewnętrznemu na podstawi umowy cywilnoprawnej. Wyznaczenie na tej podstawie, w oparciu o umowę cywilnoprawną zapewniało niezależność działań inspektora oraz brak w jego działalności konflikt interesów.

(dowód: akta kontroli str. 3 do 6, 7 do 15, 146 do 159)

1.5. W Urzędzie zidentyfikowano zbiory przetwarzanych danych podlegające zabezpieczeniu. Zasoby baz danych obejmowały pięć systemów dziedzinowych prowadzonych w formie elektronicznej. Regulacje wewnętrzne stanowiące dokumenty wykonawcze wymagane przez PBI są dostępne wyłącznie dla osób odpowiedzialnych za realizację poszczególnych czynności wymaganych tymi dokumentami.

(dowód: akta kontroli str. 16 do 31, 38 do 75, 164, 199)

1.6. Urząd posiadał aktualne informacje o zasobach informatycznych obejmującą ich rodzaj i konfigurację zgodnie z wymogami § 20 ust. 2 pkt 2 rozporządzenia KRI Jak ustalono, zasoby teleinformatyczne Urzędu zostały przypisane do osób, które odpowiadały za dany sprzęt. Rejestr prowadzony był z wykorzystaniem systemu elektronicznego. W wyniku badania, opartego o dobór celowy 15 użytkowanych urządzeń[9] ustalono, że system ten zawierał pełną informację o tych zasobach teleinformatycznych Urzędu.

(dowód: akta kontroli str. 54 do 64, 90 do 96, 164, 170 do 198

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

**Ocena cząstkowa**

Najwyższa Izba Kontroli ocenia pozytywnie działalność Burmistrza w zakresie organizacji bezpieczeństwa informacji. Ocenę taką uzasadnia ustanowienie i wdrożenie kompleksowego systemu zarządzania bezpieczeństwem informacji, który stanowi podstawowy element zapewnienia bezpieczeństwa informacji zgromadzonych i przetwarzanych przez Urząd.

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

2.1. Urząd zapobiegał możliwości zainstalowania nieautoryzowanego oprogramowania zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI. Stwierdzono, że w przypadku 10 komputerów objętych oględzinami zastosowane ustawienia nie pozwalały na zainstalowanie przez użytkowników nieautoryzowanego oprogramowania. Uprawnienia administratora posiadał tylko pracownik pionu informatycznego.

(dowód: akta kontroli str. 164, 170 do 198)

[9] Komputerów stacjonarnych oraz przenośnych, serwerów, sprzętu sieciowego i urządzeń peryferyjnych (drukarek).

2.2. Zasady obowiązujące przy nadawaniu, modyfikowaniu i odbieraniu uprawnień użytkownikom systemów informatycznych określono kolejno w Polityce Bezpieczeństwa i Instrukcji Zarzadzania Systemem Informatycznym wprowadzonej Zarządzeniem Nr 99/2015 Burmistrza Miasta Jordanowa z dnia 25 października 2015r., Aktualizacji Polityki Bezpieczeństwa i Instrukcji Zarzadzania Systemem Informatycznym wprowadzonej Zarządzeniem Nr 46/2017 Burmistrza Miasta Jordanowa z dnia 11 sierpnia 2017r., Polityce Ochrony Danych Urzędu Miasta Jordanowa wprowadzonej Zarządzeniem Nr 25/2018 Burmistrza Miasta Jordanowa z dnia 26 czerwca 2018r. Analiza zadań służbowych realizowanych przez 15 pracowników Urzędu (w tym pięciu na stanowiskach kierowniczych) wykazała, że każdy z nich, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI, uczestniczył w procesie przetwarzania informacji w stopniu adekwatnym do realizowanych przez nich zadań. W okresie objętym kontrolą w Urzędzie troje pracowników zmieniło komórkę organizacyjną i każde z nich zgodnie ze zmienionym zakresem czynności uczestniczyło w stopniu adekwatnym w procesie przetwarzania informacji.

(dowód: akta kontroli str. 7 do 15, 32 do 35, 102 do 133, 134 do 145, 170 do 198)

2.3. Kontrolą objęto uprawnienia dostępu do systemów informatycznych wszystkich sześciu osób, które w okresie od 1 czerwca 2017 r. do 10 października 2018 r. zakończyły zatrudnienie w Urzędzie i realizowały zadania z wykorzystaniem systemów informatycznych (stanowiska administracyjne). Stwierdzono, że zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI dostęp do systemów informatycznych dla każdej w tych osób został zablokowany.

(dowód: akta kontroli str. 134 do 145, 170 do 198)

2.4. Realizując wymogi § 20 ust. 2 pkt 7 rozporządzenia KRI w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem jako zabezpieczenia techniczne wprowadzone w systemach informatycznych Urzędu w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem zastosowano m.in.:

- wprowadzenie unikanych identyfikatorów użytkowników
- haseł dostępu o wymuszanej złożoności i sile (co najmniej 8 znaków, przynajmniej jedna duża litera, przynajmniej jedna cyfra)

W Urzędzie zastosowano rozwiązanie polegające na centralnym zarządzaniu komputerami.

W ramach kontroli zabezpieczeń technicznych wykorzystywanych w systemach informatycznych zbadano trzy systemy dziedzinowe. We wszystkich przypadkach wprowadzona została polityka haseł wymuszająca na użytkownikach wprowadzenie haseł zawierających minimum osiem znaków (duże, małe litery i cyfry, a także znaki specjalne), zaś okres ważności hasła został określony na 30 dni.

(dowód: akta kontroli str.164, 167, 170 do 198)

2.5. Na pięć stanowiskach pracy, realizujących zadania w miejscach gdzie dostęp mają klienci Urzędu (oględziny stanowisk pracy gdzie obywatele załatwiają sprawy z zakresu m.in. wydawania dowodów osobistych) monitory trzech pracowników zostały usytuowane w sposób, uniemożliwiający interesantom wgląd do wyświetlanych na ekranie danych, co było zgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI (dalszy opis w części *Ustalone nieprawidłowości*).

(dowód: akta kontroli str. 164, 170 do 198)

2.6. Pracownicy Urzędu korzystali z 8 komputerów przenośnych. W Urzędzie nie ustanowiono zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość (dalszy opis w części *Ustalone nieprawidłowości*).

(dowód: akta kontroli str. 90 do 96, 164, 170 do 198)

2.7. W przypadku czterech z ośmiu komputerów przenośnych użytkowanych przez pracowników Urzędu zastosowano szyfrowania dysków twardych w celu minimalizowania ryzyka nieuprawnionego dostępu do informacji, co było zgodne z wymogami § 20 ust. 2 pkt 9 i 11 rozporządzenia KRI. Kolejne trzy z ośmiu posiadanych przez Urząd laptopów były przeznaczone do likwidacji i przechowywano je magazynie a jeden używany był wyłącznie do prezentacji w czasie szkoleń poza siecią Urzędu w związku z tym nie zastosowano na tych urządzeniach szyfrowania ich dysków.

(dowód: akta kontroli str. 90 do 96, 164, 170 do 198)

2.8. W serwerowni Urzędu zapewniono rozwiązania w zakresie podtrzymania zasilania oraz warunków środowiskowych pracy serwerów i urządzeń sieciowych, dostęp do niego został ograniczony, zapewniono ochronę fizyczną pomieszczeń.

(dowód: akta kontroli str. 164, 170 do 198)

*2.9.* W okresie objętym kontrolą w Urzędzie dokonywano zakupu sprzętu komputerowego i oprogramowania. W trakcie kontroli zbadano wszystkie cztery[10] umowy na zakup i serwis oprogramowania pod kątem zawarcia w nich zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, wymagany na podstawie § 20 ust. 2 pkt 10 rozporządzenia KRI. Zamieszczono w nich zapisy chroniące dostęp do danych (m.in. podpisanie odrębna umowy powierzenia przetwarzania danych osobowych; dostęp do danych wyłącznie w celu wykonania prac serwisowych, po naprawie problemów zobowiązanie do usunięcia danych osobowych; oświadczenie, że dane osobowe są zabezpieczone przed udostępnieniem osobom nieupoważnionym; serwis gwarancyjny w miejscu użytkowania sprzętu w obecności ASI, jeżeli nie ma możliwości naprawy na miejscu na czas naprawy poza siedzibą będzie sprzęt zabierany bez dysku twardego).

(dowód: akta kontroli str. 164, 199 do 204)

2.10. W Urzędzie nie przewidywano przekazywania sprzętu IT poza jednostkę (np. do serwisu lub zbycie sprzętu) i nie ustalono zasad dotyczących takiego przekazywania. W okresie objętym kontrolą niezbędne naprawy dokonywano we własnym zakresie (pracownicy komórki IT).

(dowód: akta kontroli str. 164, 170 do 198)

2.11. Stosownie do § 20 ust. 2 pkt 12 lit. a i f *rozporządzenia KRI* w Urzędzie przeprowadzano aktualizacje systemów operacyjnych. Wykorzystywane systemy operacyjne były objęte wsparciem producenta (Windows 10).

(dowód: akta kontroli str. 90 do 96, 164, 170 do 198)

2.12. W Urzędzie przeprowadzano regularne tworzenie i testowanie kopii zapasowych danych i oprogramowania aplikacyjnego, w którym przetwarzane są dane stosownie do § 20 ust. 2 pkt 12 lit. b i e oraz § 20 ust. 2 pkt 7 rozporządzenia KRI. Sprawdzanie kopii zapasowych dokonywane było codziennie poprzez weryfikację wielkości pliku kopii oraz odtwarzanie baz danych i maszyn wirtualnych. Kopie były przechowywane poza miejscem wytworzenia.

(dowód: akta kontroli str. 170 do 198)

[10] 1. Umowa nr 1- system dziedzinowy ADAS firmy Tensoft, K40/Gd/2002 z 01.09.2002r.; Umowa nr 2 - ZRPU.042.1.1a.2017 z 28.02.2017 r., Dostawa i wdrożenie systemów informatycznych w ramach projektu eJordanów – wdrożenie innowacyjnych i kompleksowych usług publicznych w Mieście Jordanów, Umowa nr 3 ZRPU.042.1.1c.2017 z 03.04.2017 r.; Zakup wraz z wdrożeniem i szkoleniem pracowników modułu Ewidencja Kadrowa (EK); Umowa nr 4 - zakup modułu Płace (PL) Systemu informatycznego KSAT2000i, AGP.2600.23.2017.KW z 26.09.2017 r

2.13. W Urzędzie wdrożono zabezpieczenia przed instalacją szkodliwego oprogramowania na komputerach wykorzystywanych przez pracowników zgodnie z § 20 ust. 2 pkt 12 lit. f rozporządzenia KRI. Na podstawie oględzin 10 komputerów ustalono, że był na nich zainstalowany i uruchomiony program antywirusowy, który wykorzystywał aktualną na moment badania wersję definicji wirusów.

(dowód: akta kontroli str. 170 do 198)

2.14. Pojemność nośników pamięci systemów Urzędu była na bieżąco monitorowana przez informatyka i nie przekraczała progu ostrzegawczego na poziomie 80% zajętości przestrzeni, mimo że w ramach obowiązujących w Urzędzie uregulowań nie zostały określone zasady monitorowania stanu pojemności przestrzeni dyskowej w serwerach Urzędu. Działanie pracowników Urzędu było zgodne z zaleceniem sformułowanym w pkt A.12.1.3 załącznika A normy PN-ISO/IEC 27001:2017.

(dowód: akta kontroli str. 160 do 163, 170 do 198)

2.15. W Urzędzie nie przewidziano formalnych rozwiązań związanych z ryzykiem wystąpienia zakłóceń w normalnym funkcjonowaniu środowiska informatycznego w związku z wdrażaniem nowych wersji oprogramowania (dotyczących tzw. zarządzania zmianą) (dalszy opis w części: *Ustalone nieprawidłowości*).

(dowód: akta kontroli str. 7 do 15, 16 do 31, 164)

2.16. W Urzędzie w okresie od 25 maja 2018 r. wprowadzono rejestr czynności przetwarzania danych, spełniający wymogi określone w art. 30 ust. 1 RODO. Rejestr ten został wprowadzony Zarządzeniem nr 18/2018 Burmistrza Miasta Jordanowa z dnia 25 maja 2018 r.

(dowód: akta kontroli str. 76 do 89)

Ustalone nieprawidłowości

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

1. W Urzędzie nie ustanowiono zasad (procedury) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI.

Burmistrz wyjaśnił, że posiadane urządzenia przenośne wykorzystywane do pracy mobilnej posiadają niezbędne hasła i zostały zaszyfrowane.

(dowód: akta kontroli str. 205 do 207)

Zdaniem NIK, biorąc pod uwagę możliwość wynoszenia sprzętu poza siedzibę Urzędu, zastosowanie rozwiązania polegającego na szyfrowaniu dysków twardych komputerów przenośnych może być niewystarczające gdyż istnieją także inne zagrożenia umożliwiające dostęp do danych zgromadzonych na urządzeniach mobilnych (np. kradzież, zgubienie, praca w miejscach publicznych – pociąg, autobus). Wprowadzenie szczegółowych zasad zachowania się pracowników w czasie pracy poza Urzędem, zmniejszy ryzyko dostępu do danych osób nieuprawnionych.

2. Na 5 stanowiskach pracy, realizujących zadania w miejscach gdzie dostęp mają klienci Urzędu (oględziny stanowisk pracy gdzie obywatele załatwiają sprawy m.in. w Referacie Inwestycji, Rozwoju Gospodarki i Pozyskiwania Funduszy) monitory dwóch pracowników zostały usytuowane w sposób, umożliwiający interesantom wgląd do wyświetlanych na ekranie danych, co było niezgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI. W czasie kontroli NIK zmieniono ustawienia dwóch pozostałych monitorów w taki sposób, że wyświetlane na nich dane nie były widoczne dla osób nieuprawnionych. Z uwagi na usunięcie nieprawidłowości NIK odstępuje od sformułowania wniosku w tym zakresie.

3. W Urzędzie nie przewidziano formalnych rozwiązań związanych z ryzykiem wystąpienia zakłóceń w normalnym funkcjonowaniu środowiska informatycznego w związku z wdrażaniem nowych wersji oprogramowania (dotyczących tzw. zarządzania zmianą). Według wyjaśnień Burmistrz w okresie objętym kontrolą nie zaistniała potrzeba

wprowadzania zmian a dopiero na podstawie przeprowadzonego audytu zostaną przygotowane odpowiednie procedury.

(dowód: akta kontroli str. 205 do 207)

**Ocena cząstkowa**

Najwyższa Izba Kontroli ocenia pozytywnie, mimo stwierdzonych nieprawidłowości, wdrożone i wykorzystywane w Urzędzie rozwiązania organizacyjne i techniczne, zapewniające bezpieczeństwo informacji. Komputery Urzędu zostały zabezpieczone programem antywirusowym przed szkodliwym oprogramowaniem oraz przed możliwością instalowania dowolnego oprogramowania przez użytkowników. W Urzędzie sporządzano i weryfikowano prawidłowość kopii zapasowych. Spełniono również wymóg przechowywania kopii poza miejscem ich wytwarzania. Stwierdzona nieprawidłowość dotyczyła braku szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych poza siedzibą Urzędu, gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI. Ponadto w Urzędzie nie przewidziano formalnych rozwiązań związanych z ryzykiem wystąpienia zakłóceń w normalnym funkcjonowaniu środowiska informatycznego w związku z wdrażaniem nowych wersji oprogramowania (dotyczących tzw. zarządzania zmianą). Realizacja działań w celu zapobiegania incydentom bezpieczeństwa informacji.

# 3. Realizacja działań w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

3.1. W Urzędzie nie prowadzono okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI (opis w części *Ustalone nieprawidłowości*).

(dowód: akta kontroli str. 3 do 35, 164)

3.2. W Urzędzie przygotowano rejestr zgłaszania incydentów dotyczących danych osobowych wynikający z art. 33 RODO w zakresie zgłaszania incydentów dotyczących danych osobowych. Stosowny wzór dokumentu i procedurę zawarto w Zarządzeniu 25/2018. W ww. rejestrze nie odnotowano żadnych wpisów do czasu kontroli NIK.

(dowód: akta kontroli str. 3 do 35, 164, 168)

3.3. W okresie objętym kontrolą w Urzędzie wdrożone były procedury wewnętrzne zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji, o których mowa w § 20 ust. 2 pkt 13 rozporządzenia KRI. W Urzędzie wprowadzono zarządzeniem Burmistrza zasady niezbędne do ochrony zasobów informatycznych. Ustalono w nim postępowanie w przypadku naruszenia ochrony danych, w tym danych osobowych, m.in. konieczność niezwłocznego zgłaszania incydentów utraty lub kradzieży nośników danych do ASI, automatyczne zapisywanie monitorowanych danych o nieudanych próbach logowania do systemu.

(dowód: akta kontroli str. 32, 164, 168)

3.4. Urząd zapewnił szkolenia pracowników zaangażowanych w proces przetwarzania informacji stosownie do wymogów § 20 ust. 2 pkt 6 rozporządzenia KRI W okresie objętym kontrolą zorganizowano dwukrotnie szkolenia dla pracowników w zakresie obowiązujących w Urzędzie przepisów bezpieczeństwa informacji, bezpiecznej pracy w systemach informatycznych, ochrony danych i budynków, a także przepisów RODO. Szkolenia były prowadzone przez zewnętrznego prelegenta (IOD) oraz ASI. Z zakresu bezpieczeństwa informacji zostali przeszkoleni wszyscy pracownicy Urzędu, co zostało potwierdzone podpisem na liście obecności. W okresie objętym kontrolą ASI uczestniczył indywidualnie w szkoleniach zewnętrznych, obejmujących szczegółowe zagadnienia związane m.in. z wejściem w życie przepisów RODO.

(dowód: akta kontroli str. 36 do 37, 164, 169)

3.5. W Urzędzie nie przeprowadzono w 2017 r. okresowego audytu wewnętrznego z zakresu bezpieczeństwa (dalszy opis w części Ustalone nieprawidłowości)..

(dowód: akta kontroli str. 164, 205)

3.6. W Urzędzie została przeprowadzona analiza procesów przetwarzania danych, o której mowa w art. 32 ust. 1 RODO.

(dowód: akta kontroli str. 3 do 31, 38 do 53, 164)

Ustalone nieprawidłowości

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

1. W Urzędzie nie przeprowadzano okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji, co było niezgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI.

§ 20 ust. 2 pkt 3 rozporządzenia KRI stanowi, że zarządzanie bezpieczeństwem informacji jest realizowane m.in. poprzez przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Burmistrz wyjaśniła, że dopiero na podstawie przeprowadzonego prze zewnętrzna firmę audytu taka analiza zostanie przygotowana

(dowód: akta kontroli str. 205 do 207)

NIK wskazuje, że konieczność dokonywania cyklicznych analiz ryzyka utraty poufności, integralności i rozliczalności informacji wynika z przepisów rozporządzenia KRI. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie będących w posiadaniu lub przetwarzaniu urzędu. Rodzaj zastosowanych zabezpieczeń technicznych jak i ich poziom wynika zatem z szacowania ryzyka. Analiza taka powinna zatem być przeprowadzona cyklicznie, aby Urząd mógł zidentyfikować i ocenić ryzyka mające wpływ na jego działalność. Niewątpliwie zdarzeniem istotnie wpływającym na bezpieczeństwo informacji i wymuszającym jednocześnie przeprowadzenie tych analiz było wejście w życie przepisów RODO. Należy zauważyć, że czynność taka powinna mieć formę pisemną, tak aby stanowiła podstawę do kolejnych analiz.

2. W 2017 r. w Urzędzie nie został przeprowadzony audyt wewnętrzny z zakresu bezpieczeństwa informacji co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.

Burmistrz wyjaśniła, że z uwagi na nawał pracy i poszukiwania odpowiedniej osoby na stanowisko IOD (trzykrotny konkurs nie wyłonił chętnego) przesunięto audyt na 2018 r.

(dowód: akta kontroli str. 205 do 207)

**Ocena cząstkowa**

Najwyższa Izba Kontroli ocenia negatywnie działalność Burmistrza w zakresie zapobiegania incydentom bezpieczeństwa informacji, ze względu na nieprzeprowadzenie w 2017 r. audytu bezpieczeństwa informacji, a także ze względu na brak przeprowadzenia okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji co nie pozwalało ocenić czy podejmowane w Urzędzie działania minimalizujące takie ryzyko były wystarczające. Tym samym nie zastosowano się do wymogów § 20 ust. 2 pkt 3 rozporządzenia KRI, który nakłada obowiązek podejmowania działań stosownie do wyników przeprowadzonej analizy.

# 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[11], wnosi o:

1) przeprowadzenie okresowych analiz utraty integralności, dostępności lub poufności informacji, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI,

2) ustanowienie szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych,

3) zapewnienie realizacji okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji,

[11] Dz. U. z 2017 r. poz. 524 ze zm., dalej: *ustawa o NIK*.

4) przygotowanie formalnych rozwiązań związanych z ryzykiem wystąpienia zakłóceń w normalnym funkcjonowaniu środowiska informatycznego w związku z wdrażaniem nowych wersji oprogramowania (dotyczących tzw. zarządzania zmianą).

# 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 Krakowie.

Obowiązek poinformowania NIK o sposobie 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 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.

Kraków, dnia października 2018 r.

Kontroler
Małgorzata Kram
specjalista k.p.