NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi

LLO.410.018.04.2019

Zbigniew Burzyński
Prezydent Miasta Kutno
Urząd Miasta Kutno
Plac Marsz. J. Piłsudskiego 18
99-300 Kutno

WYSTĄPIENIE POKONTROLNE

P/19/007 – Wdrożenie przez administrację publiczną regulacji dotyczących ochrony danych osobowych po wejściu w życie RODO

NAJWYŻSZA IZBA KONTROLI
Delegatura w Łodzi
ul. Kilińskiego 210, 93-106 Łódź
T +48 42 239 32 00, F +48 42 239 32 90
llo@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Kutno, Plac Marsz. J. Piłsudskiego 18, 99-300 Kutno (dalej Urząd).
Kierownik jednostki kontrolowanej	Zbigniew Burzyński, Prezydent Miasta Kutno od 24 listopada 2014 r. (dalej Prezydent Miasta)
Zakres przedmiotowy kontroli	1. Organizacja ochrony danych osobowych w jednostce. 2. Wykorzystanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych. 3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi, w jednostce.
Okres objęty kontrolą	Od 25 maja 2018 r. do czasu zakończenia kontroli oraz dla zdarzeń wcześniejszych, jeśli mają wpływ na kontrolowaną działalność.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Łodzi
Kontroler	Arkadiusz Kałużny, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LLO/181/2019 z dnia 13 września 2019 r.

(Dowód: akta kontroli str. 1-3)

[1] Dz. U. z 2019 r. poz. 489 ze zm., dalej ustawa o NIK.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie prawidłowo przygotowano się do wdrożenia 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)[3] – dalej RODO. Ochrona danych osobowych była prowadzona zgodnie z wymogami określonymi w powołanym rozporządzeniu. W wyniku kontroli stwierdzono jednak nieprawidłowości polegające na niestosowaniu zasad ustalonych w wewnętrznych procedurach bezpieczeństwa.

W Urzędzie opracowano system przetwarzania i zabezpieczania danych osobowych zgodny z wymogami RODO. Pracownicy Urzędu zostali przeszkoleni w związku z wejściem w życie nowych przepisów prawa i zapoznani ze zaktualizowanymi procedurami w zakresie bezpieczeństwa informacji. Realizując obowiązki określone w RODO, Prezydent Miasta Kutno powołał Inspektora Ochrony Danych (IOD) i umożliwił mu realizację zadań w sposób niezależny. Nie dotrzymał jednak terminów powiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD, a także Zastępcy IOD. Osoba pełniąca funkcję IOD posiadała odpowiednie przygotowanie merytoryczne i doświadczenie zawodowe. W kontrolowanym okresie IOD wywiązywał się z nałożonych na niego obowiązków, z wyjątkiem aktualizacji wymaganego procedurami wewnętrznymi rejestru zawartych umów o powierzenie przetwarzania danych osobowych. Rejestr ten prowadzony był nierzetelnie, bowiem ujęto w nim jedynie 62% umów zawartych z podmiotami przetwarzającymi dane osobowe na polecenie Administratora. Pozostałe rejestry, wymagane na podstawie RODO, prowadzone były prawidłowo.

Gmina Miasto Kutno organizowała spotkania z dyrektorami i prezesami podległych jednostek, na których poruszane były zagadnienia z zakresu ochrony danych osobowych. Każda z tych jednostek wyznaczyła IOD i opracowała zasady ochrony danych we własnym zakresie.

Zgromadzone w Urzędzie dane osobowe były przetwarzane wyłącznie przez osoby posiadające stosowne upoważnienie w tym zakresie lub na podstawie umów. Administrator prawidłowo informował pracowników i petentów o przetwarzaniu ich danych osobowych, w tym o prowadzonym w Urzędzie monitoringu wizyjnym. Kamery monitoringu znajdowały się w dozwolonych miejscach i były prawidłowo oznaczone, jednak nagrania z kamer przechowywano dłużej niż dopuszczały uregulowania zawarte w procedurach wewnętrznych.

Wdrożone w Urzędzie środki techniczne i organizacyjne, służące zapewnieniu zdolności do szybkiego przywrócenia dostępności danych osobowych, były – z jednym wyjątkiem – zgodne z procedurami wewnętrznymi. Wbrew zasadom określonym w tych procedurach nie zabezpieczono jednego z pomieszczeń, w którym znajdowały się serwery, w urządzenia alarmu przeciwpożarowego.

W Urzędzie sporządzano i weryfikowano prawidłowość kopii zapasowych. Kopie przechowywano poza miejscem ich wytwarzania. Wszystkie komputery zabezpieczono przed szkodliwym oprogramowaniem oraz dostępem z zewnątrz.

W wyniku kontroli stwierdzono nieprawidłowości polegające na opóźnieniach lub braku blokowania kont dostępu do systemów informatycznych byłym pracownikom Urzędu. W jednym z funkcjonujących systemów nie ustawiono wymaganych w procedurach wewnętrznych parametrów złożoności haseł dostępu.

---

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[3] 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.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[4] kontrolowanej działalności

OBSZAR

1. Organizacja ochrony danych osobowych w jednostce

Opis stanu faktycznego

1.1. Przygotowanie dokumentacji wymaganej przepisami RODO.

W związku z wejściem w życie przepisów RODO, w ramach działań związanych z wdrożeniem *Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Kutno*, dokonano szacowania ryzyka dla bezpieczeństwa danych osobowych. Wyniki szacowania opracowano w zakresie własnym i przedstawiono w raporcie z dnia 4 kwietnia 2018 r., w którym wyznaczono ryzyko dla Urzędu, systemów informatycznych, komputerów przenośnych i nośników danych, odnosząc się do możliwych zagrożeń. W planie postępowania z ryzykiem wytypowano jedno zagrożenie, tj. zniszczenie urządzeń w Urzędzie. Po sprawdzeniu sposobu zabezpieczenia urządzeń, uznano iż zabezpieczono urządzenia przed ww. zagrożeniem.

(dowód: akta kontroli str. 4-10)

W Urzędzie zaktualizowano dokumentację z zakresu ochrony danych osobowych. Zarządzeniem z dnia 18 maja 2018 r.[5] w sprawie ochrony danych osobowych w Urzędzie Prezydent Miasta wprowadził do stosowania *Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Kutno* (dalej *Polityka bezpieczeństwa*). Dokumentacja ta uwzględniała wymogi RODO. Ustalono w niej m.in. środki techniczne i organizacyjne dotyczące ochrony danych, procedury dotyczące: analizy ryzyka i planu postępowania z ryzykiem, współpracy z podmiotami zewnętrznymi, zarządzania incydentami, realizacji praw osób, odbierania zgód oraz informowania osób, doraźnych kontroli, procedurę kluczy.

Zarządzeniem z dnia 18 stycznia 2019 r. w sprawie ochrony danych osobowych w Urzędzie Prezydent Miasta zaktualizował *Politykę bezpieczeństwa*. Aktualizacja polegała m.in. na wprowadzeniu: zapisów dotyczących monitoringu wizyjnego Urzędu, procedury zarządzania i przetwarzania danych systemu monitoringu miejskiego w Kutnie, dokonywania oceny skutków przetwarzania dla ochrony danych osobowych.

Stosownie do postanowień art. 30 ust. 1 i 2 RODO, w Urzędzie utworzono *Rejestr czynności przetwarzania danych osobowych* i *Rejestr kategorii czynności przetwarzania*. Sporządzony został również *Wykaz naruszeń ochrony danych osobowych,* który uwzględniał dane określone w art. 33 ust. 5 RODO.

(dowód: akta kontroli str. 32-119, 691-798)

Zatwierdzoną przez Prezydenta Miasta *Politykę bezpieczeństwa* udostępniono w pełnym zakresie wszystkim pracownikom Urzędu, poprzez opublikowanie jej w systemie elektronicznego obiegu dokumentów. Ponadto kierownicy komórek organizacyjnych zostali zobowiązani do przekazania pracownikom informacji o nowych regulacjach w sprawie ochrony danych osobowych.

(dowód: akta kontroli str. 229-232)

1.2. Wyznaczenie i działanie Inspektora Ochrony Danych.

Zgodnie z art. 37 ust. 1 lit. a RODO, Prezydent Miasta z dniem 25 maja 2018 r. wyznaczył IOD. Zadania IOD określono w *Regulaminie Organizacyjnym Urzędu Miasta Kutno* oraz *Polityce bezpieczeństwa*.

IOD posiadał niezbędne kwalifikacje, o których mowa w art. 37 ust. 5 RODO.

---

[4] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[5] Zarządzenie weszło w życie 25 maja 2018 r.

Zastępcę IOD Prezydent Miasta wyznaczył dnia 18 stycznia 2019 r.

(dowód: akta kontroli str. 67-123, 156-158)

W okresie objętym kontrolą IOD i jego zastępca byli pracownikami Urzędu. IOD zatrudniony był na samodzielnym stanowisku *Specjalisty ds. BHP*, a Zastępca IOD na stanowisku *Starszego informatyka* w *Biurze Informatyków*.

Zadania wykonywane w ramach umowy o pracę nie powodowały konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

(dowód: akta kontroli str. 124-147)

Zgodnie z art. 38 ust. 3 RODO, IOD podlegał najwyższemu kierownictwu Administratora danych osobowych, tj. Prezydentowi Miasta.

(dowód: akta kontroli str. 148-159)

Aktualny kontakt do IOD podany był w ogólnodostępnych informacjach – m.in. na stronie internetowej Urzędu.

Na stronie internetowej Urzędu nie udostępniono danych Zastępcy IOD. Uzupełniono je w dniu 25 września 2019 r. (opisano w sekcji *Stwierdzone nieprawidłowości*).

(dowód: akta kontroli str. 250-251, 263-266, 1894-1895)

O wyznaczeniu IOD i Zastępcy IOD poinformowano Prezesa Urzędu Ochrony Danych Osobowych (dalej Prezes UODO). W obu przypadkach zawiadomienia przesłano z opóźnieniem (opisano w sekcji *Stwierdzone nieprawidłowości*).

W okresie objętym kontrolą nie było zmian na stanowiskach IOD i jego zastępcy.

(dowód: akta kontroli str. 11-14, 248-249)

IOD realizował zadania określone w art. 39 RODO oraz w *Polityce bezpieczeństwa*, m.in. poprzez:

- udział w opracowaniu klauzul informacyjnych i procedur zawartych w *Polityce bezpieczeństwa*,
- prowadzenie szkoleń pracowników z zakresu ochrony danych osobowych,
- opracowanie i aktualizację dokumentacji dotyczącej szacowania ryzyka dla przetwarzania danych,
- udział w usuwaniu i niszczeniu danych osobowych, które nie były już wykorzystywane,
- udzielanie informacji i porad z zakresu ochrony danych osobowych,
- konsultacje z organem nadzorczym.

(dowód: akta kontroli str.267-392)

1.3. Inne działania jednostki związane z wdrażaniem RODO.

Zgodnie z art. 13 ust. 1 i 2 RODO Administrator danych osobowych informował osoby przebywające w Urzędzie o przetwarzaniu ich danych osobowych. Stosowne powiadomienia w tym zakresie zawarte były m.in. w ogólnodostępnych pomieszczeniach i na stronie internetowej Urzędu.

(dowód: akta kontroli str. 250-263, 1894-1895, 1927)

W dniach od 18 do 28 grudnia 2018 r. w Urzędzie przeprowadzono audyt wewnętrzny w zakresie przeglądu i analizy stanu funkcjonowania strony Biuletynu Informacji Publicznej Urzędu. Audyt ten obejmował m.in. sprawdzenie, czy realizowany jest zakres i tryb przekazywania informacji do zamieszczenia na stronie oraz czy treści udostępnianych informacji zostały zabezpieczone przed ich zniszczeniem i modyfikacją przez osoby nieuprawnione. We wskazanym obszarze nie sformułowano zastrzeżeń.

W dniach od 28 stycznia do 1 lutego 2019 r. UODO przeprowadził w Urzędzie kontrolę dotyczącą przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego. Kontrola wykazała m.in., że niewłaściwie oznaczono obszar objęty miejskim monitoringiem wizyjnym i nie zamieszczono klauzul informacyjnych pod punktami kamerowymi. Stwierdzono także, że w analizie ryzyka opracowanej w Urzędzie nie uwzględniono miejskiego monitoringu wizyjnego.

Wszystkie stwierdzone uchybienia zostały terminowo usunięte.

(dowód: akta kontroli str. 393-467)

W związku z wejściem w życie RODO, w Urzędzie przeprowadzono niżej wymienione szkolenia i spotkania uwzględniające zagadnienia związane z ochroną danych osobowych:

– w dniu 21 maja 2018 r. odbyło się spotkanie Prezydenta Miasta z kadrą kierowniczą, na którym omówiono wdrożenie *Polityki bezpieczeństwa*,

– w dniu 30 maja 2018 r. pracownicy Straży Miejskiej zostali przeszkoleni przez IOD w zakresie ochrony danych osobowych,

– w dniu 14 czerwca 2018 r. podmiot zewnętrzny przeprowadził dla pracowników Urzędu szkolenie pod nazwą *RODO wybrane zagadnienia*. Obejmowało ono także polskie regulacje dotyczące ochrony danych osobowych. W szkoleniu uczestniczyło 135 osób, tj. 74,6% pracowników zatrudnionych na stanowiskach związanych z przetwarzaniem danych osobowych,

– w dniu 16 października 2019 r. podmiot zewnętrzny przeprowadził dla pracowników Urzędu szkolenie z zakresu ochrony danych osobowych i bezpieczeństwa informacji w kontekście obowiązywania RODO oraz regulacji prawnych zapewniających stosowanie RODO. Uczestniczyły w nim 144 osoby, tj. 75,4% pracowników zatrudnionych na stanowiskach związanych z przetwarzaniem danych osobowych.

Wszyscy pracownicy Urzędu zostali zapoznani przez IOD z przepisami dotyczącymi ochrony danych osobowych oraz *Polityką bezpieczeństwa*.

(dowód: akta kontroli str. 468-499)

W związku z wdrażaniem RODO, w okresie od maja 2018 r. do końca września 2019 r. w Urzędzie poniesiono wydatki w kwocie 53,9 tys. zł. Środki te przeznaczono na: wynagrodzenie IOD (49,4 tys. zł), szkolenia w zakresie ochrony danych (3,8 tys. zł), zakup oprogramowania i opiekę autorską (0,7 tys. zł).

(dowód: akta kontroli str.229-245)

Na Gminę Miasto Kutno nie zostały nałożone kary pieniężne lub inne sankcje, zasadne w przypadku niewłaściwego stosowania przepisów RODO.

(dowód: akta kontroli str. 229-232)

1.4. Nadzór nad podległymi jednostkami w obszarze stosowania RODO.

Zastępca Prezydenta Miasta wyjaśnił iż: *każda jednostka organizacyjna podległa Gminie Miasto Kutno zatrudnia bądź wyznacza własnego IOD i opracowuje zasady ochrony danych we własnym zakresie. Do chwili obecnej nie wpłynęły żadne skargi na podległe jednostki w zakresie przetwarzania danych osobowych. Gmina Miasto Kutno organizowała spotkania z dyrektorami i prezesami podległych jednostek, na których poruszane były zagadnienia z zakresu ochrony danych osobowych. Gmina Miasto Kutno zobowiązała podległe jednostki do wdrożenia procedur dotyczących RODO. Z informacji posiadanych przez Urząd Miasta wynika, że wszystkie podległe jednostki posiadają wdrożone procedury RODO i wyznaczyły IOD.*

(dowód: akta kontroli str. 229-232)

W każdej z 28 jednostek organizacyjnych ustanowiono administratora i inspektora ochrony danych, a informacje o administratorze i inspektorze ochrony danych zostały zamieszczone na stronach internetowych tych jednostek.

(dowód: akta kontroli str. 501-597)

W badanym okresie *Biuro Audytu Wewnętrznego* przeprowadziło w dniach 18 - 28 grudnia 2018 r. audyt wewnętrzny w Szkole Podstawowej nr 9 w Kutnie w zakresie bezpieczeństwa i ochrony danych osobowych, w tym bezpieczeństwa systemów informatycznych. Audytorzy Urzędu ustalili, iż jednostka organizacyjna posiadała politykę ochrony danych osobowych, z którą zapoznali się pracownicy szkoły. Administrator wyznaczył inspektora ochrony danych i powiadomił o tym fakcie

Prezesa UODO. Zastosowane w polityce ochrony danych osobowych środki techniczne i organizacyjne zostały dobrane na podstawie przeprowadzonej analizy i oceny ryzyka w stosunku do zidentyfikowanych zasobów związanych z przetwarzaniem danych. Jednostka organizacyjna prowadziła rejestr czynności przetwarzania danych osobowych i wypełniała obowiązki informacyjne wynikające z art. 13 i 14 RODO. W rekomendacjach audytorzy zalecili dokonanie szczegółowej weryfikacji procesu inwentaryzacji pod kątem spełnienia wymogów 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[6].

(dowód: akta kontroli str. 640-660)

W kontrolowanym okresie do Urzędu nie wpłynęły skargi na podległe jednostki w zakresie przetwarzania danych osobowych.

(dowód: akta kontroli str. 229-232, 661-667)

Stwierdzone nieprawidłowości

W działalności Urzędu w zakresie organizacji ochrony danych osobowych stwierdzono następujące nieprawidłowości:

Administrator danych osobowych z opóźnieniem zawiadomił Prezesa UODO o wyznaczeniu IOD i Zastępcy IOD. W odniesieniu do IOD, wyznaczonego z dniem 25 maja 2018 r., zawiadomienie przesłano 15 czerwca 2018 r., tj. siedem dni po terminie określonym w art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[7]. Dla Zastępcy IOD, wyznaczonego 18 stycznia 2019 r., zawiadomienie przesłano 23 września 2019 r., tj. cztery miesiące po terminie określonym w art. 10 ust. 1 w zw. z art. 11a ust. 3 ustawy o ochronie danych osobowych.

Dodatkowo, danych Zastępcy IOD nie udostępniono na stronie internetowej Urzędu. Stanowiło to naruszenie art. 11 w zw. z art. 11a ust. 3 ustawy o ochronie danych osobowych. Dane te uzupełniono w trakcie kontroli NIK, 25 września 2019 r.

(dowód: akta kontroli str. 11-14, 67-119, 248-262)

Zastępca Prezydenta Miasta wyjaśnił, iż opóźnienie zawiadomienia Prezesa UODO o wyznaczeniu IOD było spowodowane względami technicznymi, leżącymi po stronie operatora, tj. brakiem dostępności do platformy. Opóźnienie w przekazaniu zawiadomienia o wyznaczeniu Zastępcy IOD oraz zamieszczenia jego danych na stronie internetowej Urzędu wynikło z przeoczenia zmian przepisów prawa, wprowadzających taki obowiązek.

(dowód: akta kontroli str. 229-232, 265-266, 1501-1504)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w obszarze organizacji ochrony danych osobowych. Stwierdzone nieprawidłowości, polegające na opóźnieniu w przekazaniu Prezesowi UODO informacji o wyznaczeniu IOD i jego zastępcy oraz na niezamieszczeniu danych Zastępcy IOD na stronie internetowej Urzędu miały charakter formalny i nie wpłynęły na obniżenie oceny.

OBSZAR

2. Wykorzystywanie wdrożonych rozwiązań organizacyjnych w zakresie ochrony danych osobowych

Opis stanu faktycznego

2.1. Prowadzenie rejestrów wymaganych przepisami RODO.

Prowadzony w Urzędzie *Rejestr czynności przetwarzania danych osobowych* zawierał wymagane informacje, wymienione w art. 30 ust. 1 RODO. Rejestr ustalał kategorie danych wyłącznie w zakresie niezbędnym dla celów przetwarzania. Dla

[6] Dz. U. z 2017 r. poz. 2247.

[7] Dz. U. z 2019 r. poz. 1781, dalej ustawa o ochronie danych osobowych.

każdego wyszczególnionego w rejestrze zbioru danych osobowych określono podstawę ich przetwarzania.
W okresie objętym kontrolą rejestr ten był na bieżąco aktualizowany.

(dowód: akta kontroli str. 668-796, 1049-1156, 1501-1510)

Prowadzony w Urzędzie *Rejestr kategorii czynności przetwarzania* zawierał wszystkie wymagane informacje, wymienione w art. 30 ust. 2 RODO. W wyniku kontroli nie stwierdzono okoliczności uzasadniających konieczność aktualizacji rejestru.

(dowód: akta kontroli str. 797-1027)

2.2. Upoważnienia do przetwarzania danych.

Zgodnie z wytycznymi określonymi w § 112 p. 4b *Polityki bezpieczeństwa*, w Urzędzie prowadzono *Ewidencję osób upoważnionych do przetwarzania danych osobowych*. W ewidencji tej ujęto aktualnych pracowników Urzędu, stażystów, osoby wykonujące zadania na podstawie umów zleceń oraz osoby powołane zarządzeniami Prezydenta Miasta do komisji funkcjonujących w Urzędzie.
Kontrola zgodności zakresu upoważnień do przetwarzania danych osobowych wydanych wybranym 34 pracownikom[8] z danymi przetwarzanymi przez nich w ramach wykonywanych obowiązków służbowych, nie wykazała rozbieżności.

(dowód: akta kontroli str. 95-96, 1157-1413, 1927)

W wyniku badania 14 celowo dobranych umów zleceń, związanych z przetwarzaniem danych osobowych, ustalono, że we wszystkich przypadkach Administrator udzielił zleceniobiorcy stosownego upoważnienia.

(dowód: akta kontroli str. 1414-1459)

Zasady blokowania praw dostępu do systemów komputerowych ustalono w *Polityce bezpieczeństwa*. Zgodnie z tymi zasadami w Urzędzie należy zapewnić niezwłoczne blokowanie zbędnych kont użytkowników oraz uprawnień (§ 77) oraz niezwłoczne odebranie i zablokowanie praw dostępu użytkownikom, którzy nie są już pracownikami (§ 66).
Po dniu 25 maja 2018 r. w Urzędzie rozwiązano umowy o pracę z czternastoma osobami, a sześć osób zmieniło stanowisko pracy. Osoby, które zmieniły stanowisko, posiadały dostęp jedynie do systemów informatycznych obsługiwanych na nowych stanowiskach. W przypadku osób, z którymi rozwiązano umowy o pracę (14), sześciu osobom zablokowano dostęp do systemów najpóźniej z ostatnim dniem okresu zatrudnienia. Pozostałym ośmiu pracownikom pozostawiono aktywne konta poczty e-mail, w tym czterem pracownikom w jednym z użytkowanych systemów informatycznych usunięto konta po 1-6 miesiącach od rozwiązania stosunku pracy i jednej osobie nie wyłączono konta w domenie (opisano w sekcji *Stwierdzone nieprawidłowości*).

(dowód: akta kontroli str. 88-89, 1460-1503, 1511-1515)

W §§ 33 - 36 *Polityki bezpieczeństwa* ustalono zasady współpracy z podmiotami zewnętrznymi. Wskazano m.in., iż każdorazowe skorzystanie z usług podmiotu przetwarzającego poprzedzone jest zawarciem umowy powierzenia przetwarzania danych osobowych. IOD prowadzi rejestr zawartych umów o powierzenie przetwarzania danych osobowych oraz dokonuje czynności kontrolnych procesu.

(dowód: akta kontroli str. 84)

Analiza 13 losowo wybranych umów zawartych z podmiotami zewnętrznymi wykazała, że:

– w każdym przypadku Administrator zawarł z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych, zawierającą wszystkie elementy wymagane na podstawie art. 28 ust. 3 RODO oraz *Polityki bezpieczeństwa*,

[8] Do kontroli wybrano w sposób celowy wszystkich 26 pracowników *Wydziału Finansów i Budżetu* i ośmiu pracowników *Wydziału Spraw Obywatelskich*.

– w każdej z umów zawarto zapis, iż Administrator jest uprawniony do kontroli sposobu wykonania umowy przez przetwarzającego,
– rejestr zawartych umów o powierzenie przetwarzania danych prowadzony był w formie odrębnego spisu spraw. Ujęto w nim siedem z 13 objętych kontrolą umów powierzenia.

(dowód: akta kontroli str. 1583-1650, 1657-1676, 1678-1716)

Ogółem, według stanu na dzień 6 października 2019 r., w ww. rejestrze ujęto 13 z 21 zawartych umów powierzenia (opisano w sekcji *Stwierdzone nieprawidłowości*).

(dowód: akta kontroli str. 1532-1582, 1651-1656, 1663-1665, 1672-1676, 1693-1699, 1705-1707, 1731-1733)

W kontrolowanym okresie nie przeprowadzono żadnej kontroli sposobu wykonania umowy powierzenia przez przetwarzającego dane osobowe, natomiast nadzór nad wywiązaniem się z zapisów umowy powierzenia przetwarzania danych realizowany był w ramach całościowego nadzoru nad prawidłowym wykonaniem umowy głównej. Jak wyjaśnił Zastępca Prezydenta Miasta, nie skorzystano z prawa kontroli środków zastosowanych przez podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych, ponieważ nie było ku temu żadnych przesłanek, wskazujących na naruszanie postanowień umowy. Nie było również żadnych skarg od osób fizycznych, których dane przetwarzały podmioty przetwarzające o jakimkolwiek naruszeniu ich praw.

(dowód: akta kontroli str. 1501-1504, 1928)

W kontrolowanym okresie Gmina Miasto Kutno wykonywała zadania podmiotu przetwarzającego. Zgodnie z art. 28 ust. 3 RODO przetwarzanie odbywało się na podstawie umów[9], a także na podstawie przepisów ustaw[10] i wytycznych wskazujących dodatkowe obowiązki podmiotu przetwarzającego. Analiza postanowień wszystkich obowiązujących umów (7) wykazała, że w Urzędzie wywiązano się z obowiązków nałożonych na podmiot przetwarzający.

(dowód: akta kontroli str. 797-1048, 1876-1878)

2.3. Monitoring wizyjny Urzędu.

Prowadzenie monitoringu wizyjnego w Urzędzie uregulowane zostało w §§ 17 – 24 *Polityki bezpieczeństwa*. Zgodnie z tymi uregulowaniami (§ 20) nagrania obrazu przechowuje się przez okres nieprzekraczający 30 dni.

Stosownie do postanowień zawartych w art. 22^2 ustawy z dnia 26 czerwca 1974 r. - kodeks pracy[11], monitoring nie obejmował pomieszczeń wskazanych w ww. artykule. Kamery były prawidłowo oznakowane, zaś przy wejściach do Urzędu rozmieszczono klauzule informacyjne dotyczące monitoringu. Nagrania z monitoringu były prawidłowo zabezpieczone. Przechowywano je przez okres dłuższy niż 30 dni (opisano w sekcji *Stwierdzone nieprawidłowości*).

(dowód: akta kontroli str. 82-83, 1767-1770, 1927)

2.4. Ochrona systemów informatycznych.

W *Polityce bezpieczeństwa* ustanowiono środki techniczne i organizacyjne służące ochronie danych osobowych (§§ 12 – 16) oraz procedurę kluczy (§§ 56 – 60).

Zgodnie z § 13 pkt 9 *Polityki bezpieczeństwa* pomieszczenia, w których przetwarzano zbiory danych osobowych, zabezpieczone były przed skutkami pożaru

---

[9] Umowy o dofinansowanie projektów realizowanych w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020 zawarte między 8 września 2016 r. i 17 października 2017 r., z aneksami zawartymi między 14 i 30 sierpnia 2019 r.

[10] Ustawy z 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy (Dz. U. z 2019 r. poz. 1291 ze zm.), ustawy z 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2019 r. poz. 653 ze zm.), ustawy z 28 listopada 2014 r. Prawo o aktach stanu cywilnego (Dz. U. z 2018 r. poz. 2224 ze zm.), ustawy z 24 września 2010 r. o ewidencji ludności (Dz. U. z 2019 r. poz. 1397 ze zm.).

[11] Dz.U. z 2019 r. poz. 1040 ze zm.

za pomocą systemu alarmowego (z wyjątkiem jednego z pomieszczeń, w którym znajdowały się serwery) i wolnostojących gaśnic na korytarzach (opisano w sekcji *Stwierdzone nieprawidłowości*). Dostęp do ww. pomieszczeń kontrolowany był przez system monitoringowy, a poza godzinami pracy Urzędu także przez służbę ochrony. Okna były odpowiednio zabezpieczone. Klucze do pomieszczeń udostępniane były zgodnie z procedurą wewnętrzną.

(dowód: akta kontroli str. 77-82, 87)

W pomieszczeniach, w których znajdowały się serwery, zapewniono podtrzymanie zasilania. Zastosowane rozwiązania zabezpieczały te pomieszczenia przed nieuprawnionym dostępem. W jednej z serwerowni zainstalowany był system alarmu pożarowego. W drugim pomieszczeniu z serwerami, nieposiadającym alarmu pożarowego, znajdowały się materiały łatwopalne, które zostały usunięte z tego pomieszczenia w trakcie kontroli.

(dowód: akta kontroli str. 1771-1791, 1797-1841, 1927)

Zasady tworzenia i przechowywania kopii zapasowych danych określono w § 14 pkt 12 i §§ 89 - 91 *Polityki bezpieczeństwa*. W Urzędzie ostatnie kopie wykonano i przechowywano zgodnie z ustalonymi w tym zakresie zasadami. Kopie znajdowały się w innym miejscu niż bazy danych, co minimalizowało ryzyko ich utraty. Kierownik *Biura Informatyków* wyjaśnił m.in., że program służący do wykonywania kopii dokonuje ich weryfikacji w trakcie tworzenia kopii.

(dowód: akta kontroli str. 79-81, 90, 1771-1772)

Komputery Urzędu były zabezpieczone programem antywirusowym. Program ten blokował także dostęp osobom nieuprawnionych do portów USB. Ponadto w Urzędzie stosowano zabezpieczenia na styku sieci lokalnej z siecią Internet.

(dowód: akta kontroli str. 1771-1796)

W systemach informatycznych Urzędu, w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem, wprowadzono zabezpieczenia polegające na konieczności logowania się do systemu (identyfikator i hasło). Wymogi dotyczące złożoności haseł zostały określone w *Polityce bezpieczeństwa*. W dokumencie tym wskazano m.in. wymagania odnośnie długości hasła (§ 14 pkt 8 lit. d oraz § 68 pkt 1).

(dowód: akta kontroli str. 79-80, 88)

W wyniku kontroli 10 losowo wybranych stanowisk komputerowych pod kątem stosowanych przez użytkowników haseł dostępu oraz zawieszania pracy w systemach komputerowych ustalono, że:

- celem uruchomienia komputerów wszyscy pracownicy wprowadzali hasła spełniające wymogi w zakresie liczby znaków (minimum osiem),
- każdy pracownik logował się do kolejnych systemów, wykorzystywanych na danych stanowiskach pracy (łącznie pięć systemów). Logując się do czterech systemów pracownicy wprowadzali hasła spełniające wymogi w zakresie liczby znaków. Piąty system, do którego logowała się jedna z 10 objętych kontrolą osób, uruchomił się po wprowadzeniu mniejszej niż wymagana liczby znaków. W systemie tym nie wprowadzono ustawień wymuszających wprowadzenie haseł zgodnych z wymogami *Polityki bezpieczeństwa* (opisano w sekcji *Stwierdzone nieprawidłowości*),
- czterech z 10 pracowników potrafiło blokować stację roboczą. W procedurach wewnętrznych nie ustalono zasad zawieszania pracy w systemach informatycznych.

(dowód: akta kontroli str. 1511-1515)

Stwierdzone nieprawidłowości

W działalności Urzędu w obszarze wykorzystywania wdrożonych rozwiązań organizacyjnych w zakresie bezpieczeństwa danych osobowych, stwierdzono następujące nieprawidłowości:

1. Wbrew wymogom określonym w § 66 i § 77 Polityki bezpieczeństwa, byłym pracownikom Urzędu nie blokowano lub z opóźnieniem usuwano konta dostępu do niektórych systemów informatycznych. Stwierdzona nieprawidłowość dotyczyła łącznie ośmiu z 14 skontrolowanych przypadków (57%), w których:
- ośmiu osobom pozostawiono aktywne konta poczty e-mail. Konta te usunięto w trakcie kontroli NIK, po upływie od czterech do szesnastu miesięcy od rozwiązania umów o pracę,
- czterem osobom w jednym z użytkowanych systemów informatycznych usunięto konta w dniu 26 listopada 2018 r., tj. po upływie od jednego do sześciu miesięcy od rozwiązania umów,
- jednej osobie nie wyłączono konta w domenie. Konto to zablokowano w trakcie kontroli NIK, po czternastu miesiącach od rozwiązania stosunku pracy.

(dowód: akta kontroli str. 88, 1496-1500, 1511-1515)

Zastępca Prezydenta Miasta wyjaśnił, że opóźnienie miało miejsce z powodu niedopatrzenia. Byli pracownicy nie mieli dostępu do kont wyłączonych z opóźnieniem, ponieważ dostęp był możliwy jedynie z komputerów znajdujących się w budynku Urzędu. Poczta elektroniczna służy pracownikom do korespondencji jawnej i nie mogą jej wykorzystywać do celów prywatnych.

(dowód: akta kontroli str. 1501-1504, 1528-1531, 1797)

2. Wymagany w Urzędzie na podstawie procedur wewnętrznych[12] rejestr zawartych umów o powierzenie przetwarzania danych z podmiotami przetwarzającymi prowadzony był nierzetelnie. Według stanu na dzień 6 października 2019 r. wpisano do niego 13 z 21 zawartych umów o powierzenie przetwarzania danych osobowych (62%). Rejestr został uzupełniony w trakcie kontroli NIK.

(dowód: akta kontroli str.1532-1766)

Zastępca Prezydenta Miasta wyjaśnił, iż w jednym przypadku naczelnik wydziału przeoczył przekazanie informacji do IOD o zawartej umowie. W pozostałych przypadkach IOD przez niedopatrzenie nie uwzględnił umów w rejestrze, gdyż zostały one przesłane IOD w formie elektronicznej.

(dowód: akta kontroli str. 1853-1857, 1890-1893)

3. Wbrew zasadzie określonej § 20 *Polityki bezpieczeństwa*, zapisy z monitoringu prowadzonego w Urzędzie przechowywano przez okres dłuższy niż 30 dni. Najstarszy zapis nagrania z monitoringu pochodził z 8 września 2019 r., tj. sprzed 46 dni od daty nagrania.

(dowód: akta kontroli str. 82, 1767-1770)

Zastępca Prezydenta Miasta wyjaśnił m.in., iż kamery załączane są za pomocą detektora ruchu. Im mniej osób porusza się w zasięgu kamery, tym mniej jest zapisu na dysku rejestratora i czas zapisu się wydłuża. Przy dużej liczbie osób poruszających się przed obiektywami kamer, czas nagrania może być krótszy niż 30 dni. Zastępca Prezydenta Miasta wskazał także, że obowiązujące przepisy pozwalają przechowywać nagrania z monitoringu do 90 dni.

(dowód: akta kontroli str. 1849-1852)

NIK zauważa, iż okres przechowywania nagrań z monitoringu nie przekroczył czasu ustalonego w art. 22^2 § 3 kodeksu pracy (do 3 miesięcy). Wskazuje równocześnie, iż w obowiązujących procedurach wewnętrznych, skrócono ten czas do 30 dni. Tym samym nagrania z monitoringu mogły być przechowywane wyłącznie przez okres w nich wyznaczony.

4. W pomieszczeniu Urzędu, w którym znajdowały się serwery, nie zainstalowano urządzeń systemu alarmowego służącego ochronie przeciwpożarowej. Stanowiło

[12] Na podstawie § 36 Polityki bezpieczeństwa.

to naruszenie § 13 pkt 9 *Polityki bezpieczeństwa*, zgodnie z którym pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu alarmowego.

(dowód: akta kontroli str. 77-78, 1771-1773)

Zastępca Prezydenta Miasta wyjaśnił, iż przy ww. pomieszczeniu na korytarzu zainstalowana jest kamera i system czujek przeciwpożarowych. Kilkadziesiąt metrów dalej, na tym samym poziomie, znajduje się dyżurka ochrony. Zapewnia to pełne bezpieczeństwo serwerowni. Aktualnie trwają prace przygotowawcze do przeniesienia serwerowni.

(dowód akta kontroli str. 1853-1858)

W ocenie NIK, aktualny sposób zabezpieczenia ww. pomieszczenia, nie spełnia wymogów określonych w *Polityce bezpieczeństwa*.

5. Jeden z pięciu skontrolowanych systemów komputerowych, zawierających dane osobowe, nie zapewniał stosowania metod uwierzytelniania zgodnych z wymogami określonymi § 14 pkt 8 lit. d oraz § 68 pkt 1 *Polityki bezpieczeństwa*. W systemie brak było bowiem odpowiednich ustawień w zakresie minimalnej liczby znaków. System uruchomił się po wpisaniu hasła składającego się z mniejszej liczby znaków niż określono w procedurach.

(dowód: akta kontroli str. 88, 1511-1515)

Zastępca Prezydenta Miasta wyjaśnił m.in., iż pracownicy firmy od której zakupiono ww. program informowali, iż są w nim ustawione polityki, które weryfikują prawidłowość hasła. Administrator Systemów Informatycznych nie miał wiedzy, że polityki te nie działają. Problem zgłoszono autorom programu i jest on aktualnie weryfikowany. Obecnie Administrator Systemów Informatycznych zastosował takie ustawienie haseł do ww. programu, które wykorzystuje wymaganą liczbę znaków.

(dowód: akta kontroli str. 1501-1504)

6. Jedna z 10 skontrolowanych osób, posiadających dostęp do ww. systemów posługiwała się hasłem dostępu niespełniającym wymogów określonych § 14 pkt 8 lit. d oraz § 68 pkt 1 *Polityki bezpieczeństwa* w zakresie minimalnej liczby znaków. Hasło zawierało mniej znaków niż określono w *Polityce bezpieczeństwa*.

(dowód: akta kontroli str. 88, 1511-1515)

Pracownik wyjaśnił, że powodem stosowania przez niego hasła krótszego niż wymagane był fakt, iż program nie pilnował i nie informował o długości znaków. Od dnia 21 października 2019 r. wprowadzono logowanie z użyciem domeny, która pilnuje i informuje o długości znaków.

(dowód: akta kontroli str. 1516-1518)

OCENA CZĄSTKOWA

Wymagane przepisami RODO rejestry, tj. *Rejestr czynności przetwarzania danych osobowych* i *Rejestr kategorii czynności przetwarzania* prowadzone były zgodnie z obowiązującymi przepisami prawa. Dane osobowe były przetwarzane wyłącznie przez osoby posiadające stosowne upoważnienie w tym zakresie lub na podstawie umów. Wdrożone w Urzędzie środki techniczne i organizacyjne służące zapewnieniu zdolności do szybkiego przywrócenia dostępności danych osobowych, były – z jednym wyjątkiem – zgodne z procedurami wewnętrznymi. Wbrew zasadom określonym w tych procedurach nie zabezpieczono jednego z pomieszczeń, w którym znajdowały się serwery, w urządzenia alarmu służącego ochronie przeciwpożarowej.

W wyniku kontroli stwierdzono także przypadki opóźnień i braku blokowania kont dostępu do systemów informatycznych byłym pracownikom Urzędu. Dodatkowo, w jednym z systemów, w którym nie ustawiono wymaganych w procedurach wewnętrznych parametrów, stosowano hasła dostępu niespełniające wymogów

w zakresie liczebności znaków. W trakcie kontroli NIK wprowadzono właściwe ustawienia w tym systemie.
Wymagany na podstawie procedur wewnętrznych rejestr zawartych umów o powierzenie przetwarzania danych osobowych prowadzony był nierzetelnie.

OBSZAR

3. Zarządzanie danymi osobowymi przetwarzanymi, w tym gromadzonymi, w jednostce

Opis stanu faktycznego

3.1. Postępowanie w przypadku naruszenia ochrony danych osobowych.
W okresie objętym kontrolą w Urzędzie trzykrotnie odnotowano naruszenie ochrony danych osobowych. Stwierdzone incydenty dotyczyły uszkodzenia magistrali zasilającej energią elektryczną część miasta, nieumyślnego pozyskania danych przez stażystę oraz wysłania korespondencji na adres prywatny, zamiast firmowy. W żadnym przypadku nie było zasadne przesyłanie zawiadomień do Prezesa UODO. Pomimo, iż ryzyko naruszenia praw lub wolności osób było niskie, w jednym przypadku Administrator powiadomił osobę, której naruszenie ochrony danych dotyczyło. Powzięto także natychmiastowo stosowne środki naprawcze.

(dowód: akta kontroli str. 386-391, 1528-1531)

3.2. Postępowanie z danymi osobowymi.
Do Urzędu nie zgłoszono żądań dotyczących usunięcia, sprostowania, bądź uzupełnienia niekompletnych danych osobowych.

(dowód: akta kontroli str. 1501-1504)

W ogólnodostępnych miejscach w budynku Urzędu nie znajdowały się informacje, które mogą naruszać ochronę danych osobowych osób fizycznych.

(dowód: akta kontroli str. 1894-1895, 1927)

Administrator uregulował zasady niszczenia dokumentów zawierających dane osobowe. W *Polityce bezpieczeństwa* wskazano m.in., że dokumenty zawierające dane osobowe po ustaniu przydatności przekazywane są do archiwum lub niszczone w sposób mechaniczny za pomocą niszczarek (§ 13 pkt 10). Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji (§ 16 pkt 9). Po upływie okresu przechowywania uzyskane w wyniku monitoringu nagrania zawierające dane osobowe podlegają zniszczeniu poprzez nadpisanie obrazu na dysku lub zniszczenie nośnika CD w niszczarce (§ 22).
W okresie objętym kontrolą dokonano jednego komisyjnego zniszczenia dokumentacji papierowej zawierającej dane osobowe.
W § 106 *Polityki bezpieczeństwa* ustalono, że przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu, wymagają obecności pracownika *Biura Informatyków* lub innej wyznaczonej osoby oraz zweryfikowania tożsamości osoby dokonującej prac serwisowych.

(dowód: akta kontroli str. 78, 81-82, 92, 305, 1853-1858)

3.3. Ochrona danych osobowych pracowników.
Po wejściu w życie RODO pracodawca, jako Administrator danych osobowych, powiadomił wszystkich pracowników Urzędu o przetwarzaniu ich danych osobowych. Informacje w tym zakresie zawierały elementy wymagane na podstawie art. 13 ust. 1 i 2 RODO. Pracownicy na piśmie wyrazili zgodę na przetwarzanie ich danych osobowych. Zgody pracowników znajdowały się w aktach osobowych[13].

(dowód: akta kontroli str. 1896-1898)

[13] Badaniem objęto 10 losowo wybranych pracowników Urzędu.

Obowiązku informacyjnego z art. 13 RODO dopełniono także w przypadku zawierania umów cywilnoprawnych oraz przy rekrutacji pracowników. Ustaleń dokonano na podstawie badania losowo wybranych 11 umów cywilnoprawnych oraz sześciu postępowań konkursowych, przeprowadzonych w badanym okresie.

(dowód: akta kontroli str. 1416-1425, 1431-1442, 1765-1766, 1899-1915)

W ogłoszeniach Prezydenta Miasta w sprawie naborów wskazano, iż kandydaci w wymaganej dokumentacji muszą złożyć oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, a także zapoznać się z klauzulą informacyjną w sprawie rekrutacji. Klauzula dostępna była w *Wydziale Organizacyjno-Administracyjnym* i na stronie BIP Urzędu.

Naczelnik *Wydziału Organizacyjno-Administracyjnego* wyjaśnił, iż *Urząd Miasta zobowiązany jest stosować przepisy Rozporządzenia Rady Ministrów z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjnej /.../. W odniesieniu do dokumentacji pochodzącej z naboru Urząd stosuje symbole klasyfikacyjne: IV – 2110 /.../ – to „Konkursy na stanowiska w urzędach" z kategorią archiwalną B o okresie przechowywania 5 lat. W myśl tych przepisów dokumentacja osoby, która została przyjęta do pracy jest włączana do akt osobowych.*

(dowód: akta kontroli str. 1900-1926)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie zarządzania danymi osobowymi przetwarzanymi w jednostce.

IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Przechowywanie nagrań z monitoringu Urzędu przez okres zgodny z procedurami wewnętrznymi.
2. Zapewnienie w pomieszczeniach, w których znajdują się serwery, systemu alarmu służącego ochronie przeciwpożarowej.
3. Rzetelne prowadzenie rejestru umów o powierzenie przetwarzania danych osobowych.
4. Przestrzeganie procedur wewnętrznych w zakresie blokowania kont dostępu do systemów informatycznych dla osób, z którymi rozwiązano umowę o pracę.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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 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.

Łódź, dnia 10 grudnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Łodzi

Kontroler
Arkadiusz Kałużny
Starszy inspektor kontroli państwowej

podpis

Dyrektor
Przemysław Szewczyk

podpis