NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.10.2021

Jan Kasprowicz
Wójt Gminy Gietrzwałd
Urząd Gminy w Gietrzwałdzie
ul. Olsztyńska 2
11-036 Gietrzwałd

WYSTĄPIENIE POKONTROLNE

P/21/081 – Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy w Gietrzwałdzie, ul. Olsztyńska 2, 11-036 Gietrzwałd (dalej: Urząd)
Kierownik jednostki kontrolowanej	Jan Kasprowicz, Wójt Gminy Gietrzwałd, od 10 sierpnia 2017 r. (dalej: Wójt lub Administrator)
Zakres przedmiotowy kontroli	1. Organizacja bezpieczeństwa informacji 2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji w pracy zdalnej
Okres objęty kontrolą	Lata 2020 – 2021 (do dnia zakończenia kontroli)[1], z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowane obszary działalności
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Olsztynie
Kontrolerzy	1. Marcin Wójcik, inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/109/2021 z 14 września 2021 r. 2. Adam Rączkiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/122/2021 z 11 października 2021 r.

(akta kontroli str. 1-4)

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Urzędzie funkcjonował System Zarządzania Bezpieczeństwem Informacji („SZBI"), na który składały się: Polityka Bezpieczeństwa Informacji („PBI"), Instrukcja zarządzania systemem informatycznym oraz Polityka Ochrony Danych („POD"). Odmienne uregulowanie w tych dokumentach niektórych kwestii nie zapewniało jednak pełnej spójności SZBI.

W Urzędzie nie w pełni przestrzegano wymogów określonych w SZBI. Dotyczyło to nierealizowania obowiązków w zakresie: pisemnego potwierdzania zapoznawania pracowników z regulacjami wewnętrznymi, wydawania pracownikom upoważnień do przetwarzania danych osobowych oraz prowadzenia szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji.

Stwierdzono również przypadki niewywiązywania się z obowiązków nałożonych rozporządzeniem 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]. W 2020 r. w Urzędzie nie zapewniono bowiem wykonania

[1] Czynności kontrolne zakończono w dniu 19 listopada 2021 r.

[2] Dz. U. z 2020 r. poz. 1200 ze zm., dalej: ustawa o NIK.

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

[4] Dz. U. z 2017 r. poz. 1247.

wymaganych tym rozporządzeniem: corocznego audytu zgodności oraz okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji. Nie dokonywano także aktualizacji PBI w celu dostosowania regulacji w niej zawartych do zmieniającego się otoczenia, w związku ze zmianami w powszechnie obowiązujących przepisach.

Prawidłowo natomiast wdrożono i stosowano określone w SZBI rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej. Zagadnienia dotyczące pracy zdalnej uregulowano stosownymi zarządzeniami Wójta, a przyjęte rozwiązania techniczne i informatyczne umożliwiały jej wykonywanie. Realizację zadań w systemie pracy zdalnej poprzedzono działaniami zmierzającymi do przekazania pracownikom informacji w zakresie bezpiecznego łączenia się z siecią wewnętrzną Urzędu. Kontrola wykazała jednak, że nie wykorzystano w pełni możliwości skonfigurowania serwera Urzędu w zakresie ustawień wymuszających od użytkowników stosowania haseł o złożoności zgodnej z wymogami obowiązujących regulacji wewnętrznych.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1 W okresie objętym kontrolą w Urzędzie funkcjonował SZBI opracowany na podstawie 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] oraz Polskiej Normy PN-ISO/IEC 27001:2014. Elementy składowe tego systemu stanowiły wprowadzone zarządzeniami Wójta: Polityka Bezpieczeństwa Informacji oraz Instrukcja zarządzania systemem informatycznym[7], Polityka ochrony danych[8]. Ponadto w Urzędzie wprowadzono Regulamin pracy zdalnej[9].

Zawarte w nich zapisy określały metody monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI zgodnie z §20 ust. 1 rozporządzenia KRI. Pomiędzy niektórymi regulacjami zawartymi w PBI oraz POD istniały rozbieżności dotyczące: formy i zakresu danych wymaganych określonymi w nich wzorami dokumentów: upoważnień do przetwarzania danych osobowych, ewidencji osób upoważnionych do przetwarzania danych osobowych, rejestru incydentów oraz terminów okresowych kontroli uprawnień użytkowników (zagadnienie opisano w sekcji „Stwierdzone nieprawidłowości" w pozycji nr 1).

W okresie objętym kontrolą nie wszyscy pracownicy Urzędu przetwarzający dane potwierdzili pisemnie zapoznanie się z regulacjami określonymi w SZBI. Znajomość PBI potwierdzili oni w toku kontroli NIK[10]. Pisemne potwierdzenie znajomości POD złożyło 20 z 45 pracowników przetwarzających dane osobowe w latach 2020-2021 (zagadnienie opisano w sekcji „Stwierdzone nieprawidłowości" w pozycjach nr 2 i 3). Do dnia zakończenia kontroli z Regulaminem pracy zdalnej zapoznało się 34 pracowników. Zgodnie z zapisami PBI oraz POD osoby przetwarzające dane

[5] 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.

[6] Dalej: rozporządzenie KRI.

[7] Zarządzenie Nr 19/2017 Wójta z dnia 27 lutego 2017 r.

[8] Zarządzenie Nr 79/2019 Wójta z dnia 13 sierpnia 2019 r.

[9] Zarządzenie Nr 103/2021 Wójta z dnia 10 września 2021 r.

[10] Nastąpiło to w dniach od 27 października do 2 listopada 2021 r.

osobowe powinny posiadać pisemne upoważnienie do przetwarzania takich danych. W prowadzonym przez Urząd rejestrze upoważnionych do przetwarzania danych osobowych ostatniego wpisu dokonano 14 maja 2018 r., pomimo iż w okresie objętym kontrolą zatrudniano pracowników przetwarzających dane osobowe (zagadnienie opisano w sekcji „Stwierdzone nieprawidłowości" w pozycji nr 4).

(akta kontroli str. 6-241)

1.2 W ramach SZBI odpowiedzialność za bezpieczeństwo informacji w Urzędzie przypisano Inspektorowi Danych Osobowych („IDO") w zawartych umowach na świadczenie tej usługi oraz Administratorowi Systemu Informatycznego („ASI").

Do zadań IDO, zgodnie z zawartymi umowami oraz POD, należał nadzór i aktualizacja dokumentacji z zakresu ochrony danych osobowych. Na podstawie PBI oraz zakresu obowiązków Informatyka, do zadań ASI[11] należał nadzór nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym pod kątem infrastruktury teleinformatycznej Urzędu oraz współpraca z IDO w zakresie kontroli nad przestrzeganiem zasad ochrony danych osobowych.

W okresie objętym kontrolą nie określono osoby odpowiedzialnej za aktualizację PBI, co wpłynęło na niedokonanie, wymaganej § 20 ust. 2 pkt 1 rozporządzenia KRI, aktualizacji PBI w stosunku do zmieniającego się otoczenia (zagadnienie opisano w sekcji „Stwierdzone nieprawidłowości" w pozycji nr 5).

(akta kontroli str. 242-253)

1.3 Funkcję IDO powierzono zewnętrznej firmie na podstawie umowy o świadczenie usług[12]. Funkcja ta została przypisana wyznaczonemu pracownikowi zleceniobiorcy, posiadającemu zgodnie z art. 37 ust. 1 RODO odpowiednie kwalifikacje zawodowe[13] w dziedzinie ochrony danych osobowych. Zawarte umowy określały także zakres zadań powierzonych IDO, do których zgodnie z art. 39 RODO należało:

- informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO,
- monitorowanie przestrzegania rozporządzenia RODO, innych przepisów o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

(akta kontroli str. 254-296)

1.4 Procedury wdrożone w ramach SZBI określały zasady postępowania z przeznaczonymi do użytku służbowego elektronicznymi nośnikami danych[14]

[11] Pismem z 12 czerwca 2019 r. Wójt wyznaczył informatyka Urzędu Administratorem Systemu Informatycznego.

[12] Umowa z dnia 2 stycznia 2020 r. oraz umowa z dnia 28 grudnia 2020 r.

[13] Kwalifikacje potwierdzone świadectwem ukończenia studiów podyplomowych w zakresie ochrony danych osobowych i bezpieczeństwa informacji w jednostkach sektora publicznego oraz certyfikatami ukończenia szkoleń z zakresu ochrony danych osobowych oraz RODO.

[14] Według SZBI elektronicznymi nośnikami danych były: pendrive, pamięć typu flash, dysk zewnętrzny, płyta CD-R oraz DVD.

w zakresie: sposobu szyfrowania, przechowywania danych na nośnikach (jedynie w przypadkach, gdy jest to konieczne oraz przez czas niezbędny do spełnienia celu), a także kasowania danych oraz fizycznego zniszczenia nośnika. W SZBI określono również zasady niszczenia dokumentacji papierowej.

Urząd w kontrolowanym okresie nie posiadał elektronicznych nośników służących do przechowywania danych, które należałoby wpisać do prowadzonego rejestru nośników do przechowywania informacji. Wprowadzone regulacje nie dopuszczały do korzystania z prywatnych nośników danych bez zgody Administratora lub zgody ASI.

(akta kontroli str. 7-227, 297-299)

1.5 PBI zawierała zapisy zabraniające wynoszenia komputerów przenośnych poza siedzibę Urzędu bez zgody Administratora. Opisano w niej podstawowe warunki niezbędne dla zapewnienia bezpieczeństwa sprzętu poza siedzibą Urzędu, takie jak sposób przechowywania danych na dysku szyfrowanym, transport w sposób minimalizujący ryzyko kradzieży lub zniszczenia, zakaz korzystania z komputera w miejscach publicznych lub środkach transportu publicznego czy uniemożliwienie korzystania z komputera przez osoby niepowołane.

Wójt w Zarządzeniu, w którym wprowadzono pracę zdalną na skutek pandemii Covid-19[15] określił, że oryginały dokumentów wpływających do Urzędu po ich dekretacji, miały być przekazywane pracownikom wykonującym pracę w Urzędzie, a jeżeli wymagał tego zakres zadań - udostępniane pracownikom wykonującym pracę zdalną w wersji elektronicznej za pośrednictwem szyfrowanych połączeń. W Zarządzeniu Wójta Nr 174/2020 z dnia 4 grudnia 2020 r. w sprawie wykonywania czynności pracy zdalnej w Urzędzie dopuszczono możliwość posiadania przez pracownika poza miejscem pracy, dokumentów jawnych z zachowaniem zasad obiegu dokumentów.

(akta kontroli str. 7-227)

1.6 W Zarządzeniu nr 39/2020 z dnia 21 marca 2020 r., wprowadzającym pracę zdalną, określono możliwość zdalnego dostępu do systemów informacyjnych Urzędu za pośrednictwem szyfrowanych połączeń przy użyciu odpowiedniego oprogramowania. Kierownicy komórek organizacyjnych za pomocą bezpiecznego łącza byli zobowiązani przekazywać pracownikom merytorycznym wersję elektroniczną dokumentów w zakresie wykonywanych zadań. Z kolei w Zarządzeniu Wójta Nr 174/2020 doprecyzowano, że pracownicy w celu wykonywania obowiązków służbowych zobowiązani byli stosować urządzenia pracodawcy przystosowane do pracy zdalnej oraz odpowiednio zabezpieczone.

W SZBI określono zasady przesyłania informacji za pośrednictwem poczty elektronicznej, m.in. zobowiązując do:

- używania mechanizmów kryptograficznych według określonych wytycznych dla informacji wrażliwych wysyłanych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację,
- zachowania ostrożności przy wpisywaniu adresu odbiorcy oraz umieszczania prośby o potwierdzenie otrzymania i zapoznania się z wiadomością przez adresata,
- korzystania przez użytkowników z poczty elektronicznej prywatnej w celach służbowych jedynie po uzyskaniu pisemnej zgody Administratora Danych lub ASI[16].

(akta kontroli str. 7-227)

[15] Zarządzenie Wójta Gminy Gietrzwałd Nr 39/2020 z dnia 21 marca 2020 r. w sprawie wykonywania czynności pracy zdalnej w Urzędzie.

[16] W okresie objętym kontrolą żaden z pracowników nie posiadał takiej zgody.

1.7 W ramach SZBI określono zasady zarządzania incydentami związanymi z bezpieczeństwem informacji, które opisano zarówno w PBI oraz POD. W PBI określono, że w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego, takiego jak naruszenie integralności, poufności lub dostępności informacji, niepoprawne działanie systemu lub sprzętu każdy z pracowników jest zobowiązany poinformować ASI lub IDO w celu dokonania wstępnej identyfikacji zdarzenia. Z zaistniałego zdarzenia należało sporządzić raport, a następnie uzupełnić prowadzony rejestr incydentów według wzoru określonego w PBI. Po każdorazowym dokonaniu wpisu ASI powinien dokonać analizy poprzednich incydentów w celu minimalizacji wystąpienia ryzyka jego ponownego wystąpienia.

W Procedurze zgłaszania naruszeń danych osobowych (załącznik do POD) określono klasyfikacje naruszeń (wewnętrzne, zewnętrzne, niskie lub wysokie) oraz sposób dalszego postępowania w przypadku stwierdzenia naruszenia zabezpieczeń. W okresie objętym kontrolą zidentyfikowano jeden incydent[17], który zaewidencjonowano w rejestrze naruszeń ochrony danych prowadzonym na podstawie POD. W ramach działań naprawczych incydent został zgłoszony dostawcy usługi oraz dokonano zmiany zabezpieczeń Urzędu.

(akta kontroli str. 7-227, 300-313)

1.8 W okresie objętym kontrolą praca zdalna w Urzędzie była podejmowana na podstawie Zarządzeń Wójta w sprawie wykonywania czynności pracy zdalnej w Urzędzie. Według przyjętych uregulowań w okresie od 25 maja do 9 sierpnia 2020 r. decyzję o wykonywaniu pracy zdalnej podejmował każdorazowo Wójt indywidualnie w stosunku do pracownika, określając każdorazowo jej zasady. W pozostałym okresie praca zdalna miała odbywać się pod nadzorem kierowników komórek organizacyjnych Urzędu, a samodzielnych stanowisk pracy pod nadzorem Wójta.

W SZBI określono zasady obwiązujące przy przetwarzaniu danych chronionych na komputerach przenośnych poza siedzibą Urzędu między innymi w zakresie złożoności hasła czy korzystania z komputera w sposób minimalizujący ryzyko uszkodzenie lub podejrzenia danych przez osoby nieupoważnione.

We wprowadzonym przez Wójta w dniu 10 września 2021 r. regulaminie pracy zdalnej określono m.in. warunki podjęcia pracy zdalnej, podstawowe zasady dotyczące bezpieczeństwa pracy zdalnej w zakresie BHP oraz zasady dotyczące bezpieczeństwa informacji obejmujące metody zabezpieczania przekazywanych informacji czy sposób postępowania z dokumentami w formie papierowej.

Regulamin określał także: wzór polecenia pracy zdalnej, wzór potwierdzenia wykonania pracy zdalnej oraz wzór protokołu z przekazania mienia pracownikowi.

Wójt podał, że w 2020 r. nie wprowadzono regulaminu pracy zdalnej, gdyż nie było i nie ma przepisu, który nakładałby na pracodawcę taki obowiązek. Regulamin pracy zdalnej wprowadzono w związku ze spodziewaną kolejną falą pandemii COVID – 19 oraz potrzebą usystematyzowania procedur w jednym dokumencie.

(akta kontroli str. 314-324, 526-528)

1.9 Zgodnie z zapisami POD oraz PBI szkolenia pracowników Urzędu powinny być przeprowadzane w przypadku każdej istotnej zmiany zasad lub procedur ochrony informacji, a nowo zatrudnieni pracownicy mieli obowiązek zaznajomić się z przepisami prawa w zakresie ochrony danych osobowych. Wiedza nowo zatrudnionych pracowników powinna być weryfikowana poprzez test na platformie e-learningowej. Ponadto PBI określała, że osoby zaangażowane w proces

[17] Próba włamania na konto użytkownika w wykupionym przez Urząd serwisie skutkująca jego zablokowaniem.

przetwarzania informacji niezależnie od zmian prawnych powinny odbywać szkolenia nie rzadziej niż raz w roku. Określała ona również zagadnienia, które powinny być objęte szkoleniami w celu uświadamiania oraz kształcenia pracowników zaangażowanych w proces przetwarzania informacji.

Mimo zapisów ujętych w SZBI, w okresie objętym kontrolą w Urzędzie nie prowadzono szkoleń dla pracowników, w tym nowo zatrudnionych w celu zwiększenia ich wiedzy w zakresie zagrożeń dotyczących bezpieczeństwa informacji. Urząd nie posiadał oraz nie dysponował dostępem do platformy e-learningowej, o której mowa w regulacjach wewnętrznych (zagadnienie opisano w sekcji „Stwierdzone nieprawidłowości" w pozycji nr 6).

(akta kontroli str. 325-332)

1.10 W PBI oraz POD określono, że zgodnie z § 20 ust. 2 pkt 1 rozporządzenia KRI będą one podlegały aktualizacji w zakresie dotyczącym zmieniającego się otoczenia. Zarówno PBI oraz POD zawierały zapisy dotyczące obowiązku przeprowadzania okresowego (nie rzadziej niż raz na rok) audytu wewnętrznego w zakresie bezpieczeństwa informacji, w celu utrzymania wysokiego poziomu bezpieczeństwa informacji. W obu regulacjach wewnętrznych opisano również, jakie elementy powinna zawierać okresowa analiza ryzyka bezpieczeństwa informacji w celu wyznaczenia właściwych kierunków działania kierownictwa oraz określenia priorytetów do zarządzania ryzykami i zabezpieczeniami.

Ostatni audyt w zakresie bezpieczeństwa informacji przeprowadzono w Urzędzie w 2019 r. W jego wyniku wydano cztery zalecenia pokontrolne[18]. Urząd w 2020 r. nie przeprowadził audytu wewnętrznego (zagadnienie opisano w sekcji „Stwierdzone nieprawidłowości" w pozycji nr 7). Audyt bezpieczeństwa informacji za 2021 r. został podjęty w toku kontroli NIK w dniu 28 października 2021 r. i na dzień zakończenia czynności kontrolnych (19 listopada 2021 r.) nie został zakończony.

Zgodnie z zapisami PBI Urząd powinien prowadzić okresowe analizy ryzyka utraty integralności, dostępności oraz poufności informacji w celu wyznaczenia właściwych kierunków działań kierownictwa oraz określenia priorytetów dla zarządzania ryzykami i zabezpieczeniami. W okresie od 1 stycznia 2020 r. do 14 listopada 2021 r. nie przeprowadzono w Urzędzie analizy ryzyka w powyższym zakresie (zagadnienie opisano w sekcji „Stwierdzone nieprawidłowości" w pozycji nr 8). W 2021 r. w ramach kontroli zarządczej zidentyfikowano ryzyka w zakresie zapewnienia ochrony danych osobowych (między innymi ryzyko wycieku danych osobowych, możliwość nieautoryzowanego użycia urządzeń) czy nadzoru nad systemem komputerowym (utrata danych lub nieautoryzowany dostęp do zasobów informatycznych) lecz nie obejmowały one działań, o których mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI, minimalizujących zidentyfikowane ryzyka.

(akta kontroli str. 343-362)

Stwierdzone nieprawidłowości

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

1. W Urzędzie w odmienny sposób uregulowano niektóre elementy dotyczące zagadnień związanych z bezpieczeństwem informacji, tj.:

- wzory określone w ramach PBI (np. wzór upoważnienia do przetwarzania danych osobowych, wzór ewidencji osób upoważnionych do przetwarzania

[18] Urząd zrealizował dwa zalecenia. Pierwsze dotyczące powołania pełnomocnika ds. ochrony informacji niejawnych oraz drugie przeprowadzenia serwisowania sprzętu. Nie zrealizowano wniosku w zakresie dostosowania upoważnień do określonych wymogów oraz wniosku dotyczącego przeprowadzania raz do roku audytu zgodności z rozporządzeniem KRI.

danych osobowych czy wzór rejestru incydentów) różniły się w zakresie prezentowanych danych od tożsamych wzorów określonych w POD,

- odmiennie określono terminy okresowej kontroli uprawnień użytkowników (wg PBI powinny odbywać się co najmniej raz na rok, a wg POD co najmniej raz na kwartał).

Tym samym nie zapewniono spójności regulacji składających się na SZBI.

W POD określono wprawdzie, że w przypadku odrębnych uregulowań występujących w innych procedurach, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych, lecz nie wskazano, które unormowania należy uznać za zapewniające wyższy poziom bezpieczeństwa.

Wójt podał, że Inspektor Ochrony Danych tworząc POD nie miał informacji dotyczącej istnienia PBI. Zarówno Polityka Bezpieczeństwa Informacji, Instrukcja zarządzania systemem informatycznym, jak i Polityka Ochrony Danych są obecnie przez Urząd aktualizowane. W trakcie przygotowywania powyższych dokumentów zostaną one dostosowane tak, aby uregulowania określające hierarchie ich zapisów, wzajemne powiazania i zależności były spójne.

(akta kontroli str. 6-241, 495-528)

2. Wbrew określonemu w PBI obowiązkowi przyjęcia od pracowników pisemnych „Oświadczeń o znajomości Polityki Bezpieczeństwa Informacji i zachowaniu w poufności informacji”[19], 32 pracowników Urzędu potwierdziło pisemnie zapoznanie się z ww. dokumentem dopiero w trakcie kontroli NIK. Nastąpiło to w dniach od 27 października do 2 listopada 2021 r., pomimo że ww. dokument obowiązywał od 27 lutego 2017 r.

Wójt podał, że w związku ze zmianami kadrowymi na stanowiskach odpowiedzialnych za bezpieczeństwo informacji i ochronę danych osobowych, pomimo starannego zapoznania się z posiadanymi dokumentami, nie stwierdzono w nich potwierdzenia zapoznania się z wymienionym zarządzeniem. Mało prawdopodobnym wydaje się fakt nie zapoznania pracowników z tym dokumentem, jednakże na skutek stwierdzonego braku, postanowiono ponownie zapoznać pracowników Urzędu z wymienionym zarządzeniem.

(akta kontroli str. 6-241, 529-540)

3. Pomimo określonego w POD wymogu pisemnego potwierdzenia zapoznania się z tym dokumentem, potwierdzenie takie w wymaganej formie[20] złożyło jedynie 20 z 45 pracowników Urzędu (44,4%) przetwarzających dane osobowe w latach 2020-2021.

Wójt podał, że wszyscy pracownicy Urzędu zapoznają się z przepisami wewnętrznymi w momencie zatrudnienia i są zobowiązani do ich przestrzegania, co potwierdzają własnoręcznym podpisem przyjmując do wiadomości zakres czynności obowiązujący na danym stanowisku. Jednakże mając na uwadze wskazaną przez NIK sytuację, niedopatrzenie w postaci braku odrębnych oświadczeń zostanie jak najszybciej zniwelowane.

(akta kontroli str. 6-241, 546-547)

4. Pomimo wymogów ustanowionych w PBI i POD, dla części pracowników Urzędu przetwarzających dane osobowe, nie udzielono na piśmie upoważnień do przetwarzania tych danych. Dotyczyło to 23 z 45 pracowników Urzędu. W przypadku

[19] Wzór oświadczenia stanowił załącznik nr 4 do PBI.

[20] Tj. w „Wykazie osób zapoznanych z Polityką Ochrony Danych” sporządzonym według wzoru stanowiącego załącznik nr 1 do POD.

trzech innych pracowników przetwarzających takie dane udzielone im upoważnienia wygasły w 2018 r.

Wójt podał, że w wyniku ustaleń z IDO przyjęto, że formą upoważnienia do przetwarzania danych osobowych jest zakres czynności każdego pracownika Urzędu, a w obowiązującym systemie prawnym nie ma obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych. IDO nie poinformował o konieczności udokumentowania tej zmiany.

NIK zauważa jednak, że obowiązek upoważniania pracowników do przetwarzania danych osobowych na piśmie wynika z zarządzeń Wójta: nr 19/2017 z 27 lutego 2017 r. wprowadzającego PBI oraz nr 79/2019 z 13 sierpnia 2018 r. wprowadzającego POD. Obie te regulacje określiły wzór upoważnienia do przetwarzania danych osobowych[21], co jednoznacznie wskazuje, że upoważnienie takie powinno stanowić odrębny dokument względem pracowniczego zakresu obowiązków.

(akta kontroli str. 6-241, 533-540)

5. W Urzędzie nie zrealizowano określonego § 20 ust. 2 pkt 1 rozporządzenia KRI obowiązku w zakresie zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. Dotyczyło to PBI, w której:

- zamieszczone były nieaktualne podstawy prawne,
- nie dokonano aktualizacji treści w związku z wprowadzeniem rozporządzenia RODO[22], w tym min. nie zastąpiono funkcji administratora bezpieczeństwa informacji funkcją inspektora ochrony danych.

Kontrola wykazała przy tym, że do zaistniałej sytuacji przyczyniło się niewyznaczenie osoby, która przejęłaby obowiązek aktualizacji PBI po pracowniku pełniącym do 31 maja 2019 r. funkcję administratora bezpieczeństwa informacji.
Wójt podał, że w związku z kontrolą ujawniły się braki w tym zakresie w dokumentacji Urzędu, dlatego też 28 października 2021 r. został podpisany aneks do umowy świadczenia funkcji Inspektora Ochrony Danych, w którym to zleceniobiorca zobowiązał się do przygotowania pełnej dokumentacji związanej z bezpieczeństwem informacji.

(akta kontroli str. 6-241, 495-525)

6. W latach 2020-2021 nie zapewniono szkoleń osobom zaangażowanym w proces przetwarzania informacji. Było to niezgodne z wymogami z § 20 ust. 2 pkt 6 rozporządzenia KRI, a także uregulowaniami wewnętrznymi zawartymi w PBI oraz POD. Ostatnie szkolenie pracowników przetwarzających dane osobowe w zakresie bezpieczeństwa informacji odbyło się 19 kwietnia 2018 r.[23], pomimo że w PBI przewidziano wymóg szkolenia pracowników nie rzadziej niż raz w roku. Spośród 45 pracowników, 23 uczestniczyło w szkoleniach zorganizowanych do 19 kwietnia 2018 r., a 22 od momentu zatrudnienia w Urzędzie nie odbywało żadnych szkoleń na temat zagrożeń dotyczących bezpieczeństwa informacji. Ponadto zgodnie z PBI oraz POD wiedza nowo zatrudnionych pracowników powinna być weryfikowana poprzez test na platformie e-learningowej, lecz Urząd nie posiadał oraz nie dysponował dostępem do takiej platformy.

Wójt podał, że w 2020 r. w związku z wystąpieniem pandemii COVID-19 nie przeprowadzono szkoleń ze wskazanego zakresu z uwagi na fakt, że priorytetem

[21] Wzory określono w załączniku nr 5 do PBI oraz załączniku nr 11 do POD.

[22] 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).

[23] Dotyczyło ono wdrożenia przepisów w zakresie RODO.

Urzędu było zapewnienie ciągłości jego pracy, przy jednoczesnym znacznym ograniczeniu kadrowym jednostki (spowodowanym również zakażeniem pracowników wirusem SARS-CoV-2), a nadmiar zadań powierzanych jednostkom samorządu terytorialnego oraz zmiany na poszczególnych stanowiskach pracy w Urzędzie spowodowały, że pracownicy nie mieli możliwości uczestniczenia w szkoleniach. Jednakże, w związku z częściowym „uspokojeniem" się sytuacji pod koniec 2021 r. planowane jest przeprowadzenie wymaganych szkoleń i weryfikacja przekazanej wiedzy. Wójt podał również, że szkolenie w formie zdalnej wraz z testem weryfikującym (e-learning) nie odbyło się w 2020 r., w związku ze zbyt małą ilością sprzętu komputerowego wynikającego z ograniczonych środków finansowych.

(akta kontroli str. 6-241, 325-332, 529-542)

7. W Urzędzie w 2020 r. nie przeprowadzono corocznego audytu w zakresie bezpieczeństwa informacji, który był wymagany przez § 20 ust. 2 pkt 14 rozporządzenia KRI.

Wójt podał, że za przeprowadzenie audytu w zakresie bezpieczeństwa informacji odpowiedzialny był Informatyk, który kończąc pracę w Urzędzie w 2019 r.[24] nie poinformował o konieczności przeprowadzania takiego audytu nie rzadziej niż raz na rok.

NIK zauważa, że obowiązek przeprowadzenia takiego audytu wynika z przepisów powszechnie obowiązujących. O istnieniu tego obowiązku Urząd został poinformowany również w Raporcie z audytu wewnętrznego z 14 marca 2019 r., w którym zalecono przeprowadzanie audytu zgodności z rozporządzeniem KRI minimum raz do roku.

(akta kontroli str. 333-334, 495-525)

8. W Urzędzie w 2020 r., wbrew wymogowi § 20 ust. 2 pkt 3 rozporządzenia KRI, nie przeprowadzono okresowej analizy ryzyka w zakresie bezpieczeństwa informacji.

W złożonym wyjaśnieniu Wójt podał, że rok 2020 był szczególny w związku z wystąpieniem pandemii. Pracownicy Urzędu skupili się na wykonywaniu najważniejszych zadań mających zapewnić funkcjonowanie Urzędu. Instytucje mogące wykonać to zadanie na zlecenie Urzędu, również miały trudności. W związku z novum, jakim było pojawienie się pandemii, Urząd był zmuszony ściśle określić priorytety w wykonywaniu nałożonych zadań. W wyniku dużej ilości obowiązków ustalono, że wskazane analizy ryzyka zostaną przeprowadzone pod koniec 2021 r.

(akta kontroli str. 335, 533-540)

OCENA CZĄSTKOWA

W Urzędzie w latach 2020-2021 funkcjonowały wprowadzone we wcześniejszym okresie regulacje wewnętrzne (PBI, Instrukcja zarządzania systemem informatycznym oraz POD), które składały się na SZBI. Oparto je m.in. na Polskiej Normie PN – ISO /IEC 27001:2014. Odmienne uregulowanie w tych dokumentach niektórych zagadnień nie zapewniało jednak pełnej spójności SZBI.

Nie w pełni przestrzegano zapisów wynikających z procedur określonych SZBI, gdyż nie realizowano obowiązków w zakresie: pisemnego potwierdzania zapoznawania pracowników z regulacjami wewnętrznymi, wydawania pracownikom upoważnień do przetwarzania danych osobowych oraz prowadzenia szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji. W Urzędzie nie zapewniono w 2020 r. wykonania, wymaganych rozporządzeniem KRI, corocznego audytu zgodności z tym rozporządzeniem, a także okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji. Nie dokonywano także

[24] Umowa rozwiązana w dniu 31 maja 2019 r.

wymaganych ww. rozporządzeniem przeglądów, co skutkowało niedostosowaniem PBI do zmienionego otoczenia.

OBSZAR

2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej

Opis stanu faktycznego

2.1 W 2020 r. pracę zdalną wykonywało ogółem 31 pracowników Urzędu, z tego 27 na podstawie polecenia pracodawcy, a 4 na podstawie złożonych wniosków. W 2021 r. pracę zdalną wykonywało 19 pracowników[25] - wszyscy na podstawie złożonych przez siebie wniosków. Wykonywanie pracy zdalnej odbywało się naprzemiennie, bowiem w każdej z komórek organizacyjnych wyznaczano pracowników pełniących dyżury w Urzędzie.

Nie wystąpiły przypadki świadczenia pracy zdalnej przez pracowników w okresie przebywania w izolacji lub na kwarantannie. Okres przebywania na kwarantannie oraz izolacji uznawany był za okres przebywania na zwolnieniu lekarskim.

Według oświadczenia Sekretarza Gminy polecenia wykonywania pracy zdalnej w 2020 r. były wydawane ustnie. Podobnie było w roku 2021, w którym zarówno wnioski pracowników na pracę zdalną, jak i zgody na jej wykonywanie w tym systemie miały formę ustną.

(akta kontroli str. 333-397)

2.2 Od pracowników Urzędu nie wymagano pisemnego potwierdzenia zapoznania się z zarządzeniami Wójta dotyczącymi wykonywania czynności pracy zdalnej.[26] Zarządzenia te zostały przesłane pocztą elektroniczną osobom na samodzielnych stanowiskach oraz kierownikom referatów Urzędu, w celu zapoznania podwładnych z ich treścią.

Z wyjaśnień pięciu pracowników objętych próbą kontrolną wynikało, że:

- przy wydawaniu im sprzętu komputerowego do pracy zdalnej otrzymali od informatyka wskazówki dotyczące korzystania z niego w ramach pracy zdalnej, w tym m.in. wymogów w zakresie zasad formułowania haseł, zasad funkcjonowania pulpitu zdalnego, pracy z komputerem w pomieszczeniu bez dostępu osób postronnych,
- pracę zdalną wykonywali z wykorzystaniem służbowego sprzętu komputerowego w wydzielonych pomieszczeniach prywatnych bez dostępu osób postronnych, stosowali wymogi dotyczące formułowania haseł, a także wygaszacz ekranu wymagający podania hasła do wznowienia pracy komputera lub wyłączali go po wykonaniu poszczególnych czynności.

(akta kontroli str. 398-417, 441-463)

2.3 Spośród 31 pracowników wykonujących pracę zdalną w 2020 r., 24 wykonywało ją z wykorzystaniem komputerów zapewnionych przez Urząd oraz z wykorzystaniem prywatnych telefonów komórkowych (tylko do komunikacji głosowej). W 2021 r. (do dnia 5 listopada) 17 z 19 pracowników wykonujących pracę zdalną korzystało z komputerów (laptopów) udostępnionych przez Urząd. Pracownicy wykonujący pracę zdalną nie korzystali w ww. latach z innych urządzeń teleinformatycznych, w tym prywatnych.

[25] Dane na 5 listopada 2021 r.

[26] Dotyczyło to zarządzeń Wójta Gminy: nr 39/20 z 21 marca 2020 r. w sprawie wykonywania czynności pracy zdalnej, nr 71/2020 z 25 maja 2020 r. w sprawie zmian organizacji pracy w Urzędzie Gminy w Gietrzwałdzie oraz Nr 174/2020 z 4 grudnia 2020 r. w sprawie wykonywania czynności pracy zdalnej w Urzędzie oraz Gminnym Ośrodku Pomocy Społecznej w Gietrzwałdzie.

Wszyscy pracownicy wykonujący pracę zdalną z wykorzystaniem powierzonego sprzętu komputerowego mieli pełny dostęp do systemów teleinformatycznych Urzędu, który był realizowany za pośrednictwem sieci VPN i tzw. pulpitu zdalnego. Rozwiązanie to umożliwiało im korzystanie z programów pakietu biurowego i służbowej poczty elektronicznej zainstalowanych na służbowych komputerach lokalnych znajdujących się w Urzędzie.

(akta kontroli str. 363-399, 405)

2.4 Spośród siedmiu komputerów stanowiących własność Urzędu, na których pracownicy wykonywali w okresie objętym kontrolą pracę zdalną, jeden był fizycznie uszkodzony i wyłączony z eksploatacji, jeden – posiadał niedziałający system operacyjny po próbie jego bezskutecznego przywrócenia, a jeden pozostawał wydany pracownikowi wykonującemu pracę zdalną.

Oględziny pozostałych czterech sprawnych i dostępnych w Urzędzie komputerów[27] oraz serwera Urzędu wykazały, że:

- trzy komputery spełniały wymogi dotyczące bezpieczeństwa danych wskazane w PBI, Instrukcji zarządzania systemem informatycznym oraz POD w zakresie:
  - zabezpieczenia programem antywirusowym – w komputerach tych ustawiona była aktualizacja automatyczna (sprawdzana i instalowana przy każdym uruchomieniu komputera), a ustawienia programu antywirusowego powodowały ciągły nadzór nad systemem plików (ochrona w czasie rzeczywistym),
  - zastosowania wygaszacza ekranu – automatycznie uruchamianego po pięciu minutach bezczynności i wymagającego podania hasła w celu odblokowania systemu,
  - zainstalowania klienta VPN oraz skonfigurowania dostępu do stacji roboczej użytkownika przy pomocy tzw. pulpitu zdalnego,
  - bieżących aktualizacji systemowych,
- jeden komputer posiadał zainstalowanego klienta VPN, bieżące aktualizacje systemowe oraz skonfigurowany dostęp do stacji roboczej za pośrednictwem pulpitu zdalnego, działający wygaszacz ekranu (po pięciu minutach bezczynności) wymagający podania hasła do odblokowania systemu, a także niedziałający system antywirusowy,
- konfiguracja serwera Urzędu dotycząca polityki haseł spełniała wymagania Instrukcji zarządzania systemem informatycznym dotyczące długości hasła (minimum osiem znaków) oraz wymaganego okresu jego zmiany (30 dni). Na serwerze tym nie ustawiono reguły wymuszającej stosowania przez użytkowników obowiązujących wymogów dotyczących złożoności hasła (zagadnienie opisano w sekcji „stwierdzone nieprawidłowości").

  W toku kontroli informatyk Urzędu ustawił na serwerze wymóg stosowania przez użytkowników haseł złożonych z kombinacji małych i wielkich liter, cyfr oraz znaków specjalnych.

(akta kontroli str. 418-468)

2.5 W Urzędzie nie dopuszczono świadczenia pracy zdalnej z wykorzystaniem prywatnych urządzeń komputerowych. Z wyjaśnień pięciu pracowników Urzędu objętych szczegółową analizą wynikało, że czterech spośród nich nie korzystało z komputerów prywatnych, a jeden pomocniczo korzystał z takiego komputera, w celu uzyskania dostępu do ogólnodostępnych stron internetowych.

(akta kontroli str. 398-399, 415, 421-463)

[27] Według stanu na dzień wykonywania oględzin tj. 9 listopada 2021 r. komputery dostępne w Urzędzie nie były wykorzystywane do pracy zdalnej.

2.6 Z wyjaśnień złożonych przez pięciu, objętych próbą pracowników Urzędu[28] wynikało, że nie pobierali oni z Urzędu oryginałów lub kserokopii dokumentów, a także nie wynosili skanów dokumentów na nośnikach danych. Podali oni natomiast, że wykorzystując udostępnione przez Urząd komputery przenośne za pośrednictwem tzw. pulpitu zdalnego łączyli się ze służbowymi komputerami stacjonarnymi, na których dysponowali dostępem do:

- systemów i ewidencji Urzędu, w tym m.in. ewidencji finansowo-księgowej Urzędu, systemów związanych z naliczaniem płac, a także systemu elektronicznego obiegu dokumentów Urzędu (dotyczyło to trzech spośród pięciu pracowników),
- plików, dokumentów elektronicznych, w tym skanów zgromadzonych na komputerach stacjonarnych (dwóch z pięciu pracowników).

Z wyjaśnień tych pracowników, wynikało ponadto, że w trakcie świadczenia pracy zdalnej nie wystąpiły przypadki braku dostępu do dokumentów niezbędnych do jej wykonywania.

Jeden z pracowników Urzędu zatrudniony w Referacie Rozwoju Społecznego i Promocji w złożonych wyjaśnieniach podał, że w trakcie pracy zdalnej korzystał ze służbowych nośników danych (płyty CD), zawierających wnioski o dofinansowanie oraz studia wykonalności projektów, co do których Urząd ubiegał się o dofinansowanie ze źródeł zewnętrznych.

Informatyk Urzędu podał, że płyty te zawierały informacje publiczne, więc nie kwalifikowały się do wykazania ich w rejestrze nośników danych.

(akta kontroli str. 421-463, 548)

2.7 Na próbie obejmującej pięciu pracowników, którzy wykonywali pracę zdalną w latach 2020-2021 ustalono, że w przypadku trzech z nich monitorowanie i nadzór nad ich pracą sprawowany był poprzez system e-mailowego raportowania o wykonanych czynnościach oraz kontakt telefoniczny z przełożonymi, a w przypadku dwóch pozostałych pracowników – poprzez kontakt telefoniczny.

Wójt podał, że obowiązek weryfikacji przestrzegania zasad i reguł dotyczących bezpieczeństwa informacji został powierzony kierownikom referatów oraz osobom na samodzielnych stanowiskach Urzędu. Każda z powyższych osób miała obowiązek przekazywania informacji o aktualnym stanie pracy zdalnej w podległym referacie lub na swoim stanowisku pracy. Według jego wyjaśnień w trakcie pracy zdalnej nie był on informowany o nieprawidłowościach, czy też problemach wynikających z tej formy pracy, a obowiązki nałożone na Urząd Gminy były wykonywane.

(akta kontroli str. 421-463, 469-494, 546-547)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Do 9 listopada 2021 r. (tj. dnia przeprowadzenia oględzin przez NIK) na serwerze Urzędu nie skonfigurowano ustawień wymuszających od użytkowników systemu stosowania haseł zawierających, wymagane Instrukcją zarządzania systemem informatycznym, małe i wielkie litery, cyfry oraz znaki specjalne, pomimo tego, że dokonanie takiej konfiguracji serwera było możliwe. Brak takiej konfiguracji nie dawał rękojmi rzetelnego wywiązywania się użytkowników systemu z przyjętych ww. Instrukcją standardów w zakresie polityki haseł, której celem było zapewnienie dostępu do systemów informatycznych jedynie osób upoważnionych.

[28] Doboru dokonano spośród pracowników zatrudnionych na stanowiskach w różnych komórkach organizacyjnych Urzędu, którzy w okresie objętym kontrolą wykonywali pracę zdalną.

Według wyjaśnień Informatyka przyczyną zaistniałej sytuacji było przeoczenie, spowodowane natłokiem wykonywanych obowiązków.

(akta kontroli str. 418-422)

OCENA CZĄSTKOWA

W Urzędzie prawidłowo wdrożono i stosowano większość określonych w SZBI rozwiązań organizacyjnych i technicznych mających na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej. Zasady pracy zdalnej określono w zarządzeniach Wójta, a przyjęte rozwiązania techniczne i informatyczne umożliwiały jej sprawne wykonywanie. Wykonywanie pracy zdalnej poprzedzono podjęciem działań w celu przekazania pracownikom informacji w zakresie bezpiecznego łączenia się z siecią wewnętrzną Urzędu. W celu udostępnienia informacji i systemów niezbędnych do realizacji powierzonych zadań, przy jednoczesnym zapewnieniu bezpieczeństwa danych, zastosowano sieć VPN i tzw. pulpit zdalny. Niemniej jednak nie wykorzystano w pełni możliwości skonfigurowania serwera Urzędu w zakresie ustawień wymuszających od użytkowników stosowanie haseł o stopniu złożoności zgodnym z wymogami obowiązujących regulacji wewnętrznych.

IV. Uwagi i wnioski

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

Wnioski

1. Przeprowadzanie corocznych audytów wewnętrznych w zakresie bezpieczeństwa informacji, a także okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji.
2. Zapewnienie szkoleń pracowników Urzędu zaangażowanych w proces przetwarzania informacji.
3. Podjęcie działań w celu zapewnienia spójności regulacji zawartych w dokumentach składających się na SZBI.
4. Zapewnienie bieżącej realizacji obowiązku pisemnego potwierdzenia zapoznania się z dokumentacją SZBI.
5. Bieżące nadawanie pracownikom Urzędu upoważnień do przetwarzania danych osobowych i prowadzenie ewidencji osób upoważnionych do przetwarzania tych danych.
6. Zaktualizowanie Polityki Bezpieczeństwa Informacji.

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 Olsztynie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę 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.

Olsztyn, 29 listopada 2021 r.

Kontrolerzy

Marcin Wójcik
Inspektor kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up.
Piotr Wanic
Wicedyrektor

.....
podpis

Adam Rączkiewicz
Główny specjalista kontroli państwowej

.....
podpis