NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.08.2021

Wiesław Śniecikowski
Burmistrz Pasłęka
Urząd Miejski w Pasłęku,
pl. św. Wojciecha 5
14-400 Pasłęk

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 Miejski w Pasłęku, pl. św. Wojciecha 5, 14-400 Pasłęk, zwany dalej: Urzędem lub Jednostką.

Kierownik jednostki kontrolowanej

Wiesław Śniecikowski, Burmistrz, od 20 listopada 2018 r.

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

Kontroler

Emilia Wasilewska, inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/111/2021 z 15 września 2021 r.

(akta kontroli str. 1-2)

I. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą praca w trybie zdalnym wykonywana była przez pracowników Urzędu głównie przy wykorzystaniu komputerów stanowiących własność tej jednostki. Przy spełnieniu warunków dotyczących bezpieczeństwa informacji dopuszczono również wykonywanie pracy w tej formie przy użyciu sprzętu prywatnego. Obowiązujące w okresie wykonywania pracy zdalnej w Urzędzie regulacje wewnętrzne obejmowały zasady określone dla zapewnienia bezpieczeństwa danych osobowych.

Do 20 czerwca 2021 r. w Urzędzie Miejskim w Pasłęku nie ustanowiono i nie wdrożono systemu zarządzania bezpieczeństwem informacji wymaganego 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] (dalej: KRI), do czego Urząd, jako podmiot realizujący zadania publiczne, był zobligowany. Obowiązująca w Urzędzie Polityka Bezpieczeństwa spełniała część minimalnych wymagań Polskiej Normy PN-ISO/IEC 27001 (dalej: PN-ISO/IEC 27001) w odniesieniu do bezpieczeństwa przetwarzania danych osobowych. W styczniu 2021 r. podjęto działania mające na celu opracowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji w Urzędzie. Wprowadzony zarządzeniem Burmistrza Pasłęka System Zarządzania Bezpieczeństwem Informacji, spełniający wymogi określone w § 20 ust. 1 i 2 ww. rozporządzenia, obowiązywał od 21 czerwca 2021 r.

[1] Tj. do 18 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. 2247.

Pracownicy Urzędu wykonywali swoje zadania w ramach pracy zdalnej z wykorzystaniem rozwiązań technicznych i technologicznych podnoszących poziom bezpieczeństwa informacji ukierunkowanych na ochronę danych osobowych. Dostępu do zasobów Urzędu na potrzeby wykonywania pracy zdalnej udzielano na ogół na podstawie stosownych upoważnień. Pracownicy Urzędu zostali zapoznani z zasadami bezpieczeństwa informacji w pracy na odległość. Zasady te były stosowane w zakresie korzystania z zasobów Urzędu oraz oprogramowania w ramach udzielonych pracownikom upoważnień.

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

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. W Urzędzie, w okresie kontrolowanym, w ramach zapewnienia bezpieczeństwa informacji obowiązywały: Plan ciągłości działania systemu teleinformatycznego[6] (dalej: Plan ciągłości) i Polityka Bezpieczeństwa (dalej: PB) oraz System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI).

Obowiązująca do 20 czerwca 2021 r. PB wprowadzona została Zarządzeniem nr 68/2018 Burmistrza Pasłęka z 8 maja 2018 r. w sprawie: wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Pasłęku". Regulacja PB Urzędu nie była zgodna z zapisami § 20 ust. 1 i 2 KRI. Zgodnie z § 20 ust. 3 ww. rozporządzenia wymagania te można uznać za spełnione w przypadku jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie PN-ISO/IEC 27001. PB spełniała część wymagań ww. Normy[7] i jedynie w odniesieniu do bezpieczeństwa przetwarzania danych osobowych wynikającego z 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; dalej: RODO)[8]. Ww. rozporządzenie stanowi jedyną podstawę prawną zarządzenia wprowadzającego BP.

W ramach obowiązującej do 20 czerwca 2021 r. PB określono, ograniczony do zakresu ochrony danych osobowych, rejestr i zbiory aktywów. Zidentyfikowano m.in. czynności przetwarzania danych osobowych, sprzęt komputerowy, oprogramowanie oraz sieć komputerową. Utrzymano aktualność tych rejestrów i zbiorów, m.in. poprzez wykorzystanie oprogramowania monitorującego oraz zarządzenie przez Inspektora Ochrony Danych Osobowych (dalej: IOD lub Inspektor) analizy rejestru czynności przetwarzania danych osobowych w 2020 r. Urząd identyfikował część zasobów informatycznych. Proces ten został rozpoczęty i nie został zakończony. Urząd nie dysponował listą aktywów w bezpieczeństwie informacji, co nie spełniało wymogów określonych w celu A. 8.1 PN-ISO/IEC 27001[9].

[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] Wprowadzony Zarządzeniem nr 33/18 Burmistrza Pasłęka z 12 lutego 2018 r. w sprawie wdrożenia Planu ciągłości działania systemu teleinformatycznego w Urzędzie Miejskim w Pasłęku.

[7] Informacje na podstawie Raportu z audytu przedwdrożeniowego, weryfikującego poziom spełnienia wymagań określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, minimalnych wymagań dla systemów teleinformatycznych oraz wybranych elementów normy PN-EN ISO/IEC 27001:2017-06 Systemu Zarządzania Bezpieczeństwem Informacji w Gminie Pasłęk – Urzędzie Miejskim w Pasłęku, przeprowadzonego w okresie od 15 lutego do 15 marca 2021 r.

[8] Dz. U. UE. L. z 2016 r., poz. 119.

[9] Informacje na podstawie Raportu z audytu przedwdrożeniowego, przeprowadzonego w Urzędzie w dniach od 15 lutego do 15 marca 2021 r.

Jednocześnie w Jednostce nie zostały wdrożone procedury klasyfikacji informacji w odniesieniu do wymogów punktu A. 8.2 Normy.

(akta kontroli str. 56-58, 68-75, 80-110, 140-141, 375-379, 389-390, 472-475, 472-492)

Obowiązujący od 21 czerwca 2021 r. SZBI został wprowadzony Zarządzeniem nr 68/21 Burmistrza Pasłęka z dnia 11 czerwca 2021 roku w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pasłęku, którego podstawę prawną stanowił m.in. § 20 KRI. SZBI opracowano, zatwierdzono i wdrożono zgodnie z wymogami PN-ISO/IEC 27001[10]. W celu ich spełnienia sklasyfikowano wszystkie aktywa wchodzące w skład SZBI oraz określono procedury m.in.: wykonywania pracy na odległość i zarządzania nośnikami wymiennymi zgodnie ze schematem klasyfikacji przyjętym w Urzędzie. Regulacja SZBI Urzędu określona została zgodnie z zapisami § 20 ust. 1, 2 i 3 KRI.

W zakresie obowiązującego od 21 czerwca 2021 r. SZBI określono informacje i aktywa z nimi związane. Były to np. sprzęt komputerowy, oprogramowanie i zbiory danych. Sporządzono listy aktywów w bezpieczeństwie informacji, a odpowiedzialność za te aktywa przypisano kierownikom referatów.

(akta kontroli str. 76-88, 375-376, 419, 412-426)

Kierownictwo Urzędu, pracownicy zatrudnieni w okresie wdrażania i obowiązywania regulacji, jak również osoby przyjmowane do pracy oraz na staż do Urzędu, byli zapoznawani z ww. przepisami głównie w ramach samokształcenia, a fakt ten potwierdzali złożonymi podpisami.

(akta kontroli str. 17-32, 58, 81-86, 104-110, 113, 188)

1.2. Urząd w okresie kontrolowanym funkcjonował na podstawie Regulaminu Organizacyjnego[11], w którym zadania z zakresu organizacji bezpieczeństwa określone zostały w zadaniach Referatu Organizacyjnego.

W ramach PB przypisano odpowiedzialność za bezpieczeństwo informacji w odniesieniu do przetwarzania danych osobowych. Odpowiedzialność ta w zakresie sprawowania nadzoru nas przestrzeganiem zasad przetwarzania i ochrony danych osobowych spoczywała na IOD. Na pracownikach zatrudnionych na stanowisku informatyka - w ramach bieżącego nadzoru nad systemem informatycznym, w którym przetwarzane były dane osobowe. Kierownicy referatów nadzorowali przestrzeganie zasad przetwarzania i ochrony danych osobowych przez podległy personel.

Odpowiedzialność za bezpieczeństwo informacji w ramach SZBI przypisano: na poziomie stanowisk Burmistrza, Zastępcy Burmistrza, Sekretarza Gminy, Radcy Prawnego i innych stanowisk podległych bezpośrednio Burmistrzowi - osobom zatrudnionym na tych stanowiskach przy współpracy m.in. z IOD, Koordynatorem SZBI (dalej: KSZBI) oraz Koordynatorem Bezpieczeństwa Teleinformatycznego (dalej: KBT), a na poziomie referatów - kierownikom.

Zadania z zakresu bezpieczeństwa informacji przypisano w zakresach czynności pracującym w Urzędzie dwóm informatykom. Do zadań tych należało m.in. wykonywanie kopii bezpieczeństwa systemów komputerowych

[10] Informacje na podstawie Raportu z audytu powdrożeniowego, w zakresie spełnienia wymagań określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, minimalnych wymagań dla systemów teleinformatycznych oraz wybranych elementów normy PN-EN ISO/IEC 27001:2017-06 Systemu Zarządzania Bezpieczeństwem Informacji w Gminie Pasłęk – Urzędzie Miejskim w Pasłęku, przeprowadzonego 16 czerwca 2021 r.

[11] Zarządzenie nr 82/18 Burmistrza Pasłęka z 25 maja 2018 r. w sprawie ogłoszenia tekstu jednolitego Regulaminu Organizacyjnego Urzędu Miejskiego w Pasłęku, ze zm.

i oprogramowania, nadawanie uprawnień do systemów oraz prowadzenie spraw dotyczących legalności stosowanego w Urzędzie oprogramowania.

Obowiązki z zakresu bezpieczeństwa informacji pozostałych pracowników regulowane były w zarządzeniach Burmistrza, tj. m.in. w ramach PB w Zarządzeniu nr 33/18 Burmistrza Pasłęka z 12 lutego 2018 r. w sprawie wdrożenia Planu ciągłości działania systemu teleinformatycznego w Urzędzie Miejskim w Pasłęku, powołującym w Urzędzie zespoły antykryzysowy i odtworzeniowy oraz w ramach SZBI w Zarządzeniu nr 69/21 Burmistrza Pasłęka z 11 czerwca 2021 r. w sprawie powołania Koordynatora Systemu Zarządzania Bezpieczeństwem Informacji i jego zastępcy, Koordynatora Bezpieczeństwa Teleinformatycznego i jego zastępcy oraz zespołu audytorów wewnętrznych w ramach Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pasłęku.

(akta kontroli str. 5-15, 42-43, 54-60, 68, 76)

1.3. W Urzędzie wyznaczono IOD[12], a jego zadania określał zakres czynności oraz uregulowania wewnętrzne Urzędu. Osoba wyznaczona na IOD była jednocześnie Kierownikiem Urzędu Stanu Cywilnego w Pasłęku (dalej: Kierownik USC). Analiza przebiegu dotychczasowego zatrudnienia[13], zdobytego wykształcenia oraz odbytych szkoleń i kursów osoby wyznaczonej na IOD wskazała, iż posiada ona fachową wiedzę w zakresie prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności umożliwiające pełnienie zadań.

(akta kontroli str. 61-67)

1.4. W ramach procedur PB zawartych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji[14] określono m.in. sposób postępowania z nośnikami w przypadku przekazania sprzętu do naprawy podmiotowi zewnętrznemu oraz sposób postępowania z nośnikami zawierającymi dane osobowe w celu ich zaszyfrowania. W PB określono procedurę przechowywania i zabezpieczania dokumentów zawierających dane osobowe w pomieszczeniach Urzędu. Ww. rozwiązania nie odpowiadały warunkom zapobiegającym nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach celem opisanych w punkcie A.8.3 PN-ISO/IEC 27001[15].

Zapisy SZBI określały typowe nośniki informacji, tj. przenośne twarde dyski, laptopy, pendrive, płyty CD, telefony komórkowe oraz dokumentację papierową. Określono również sposób postępowania z tymi nośnikami w zakresie m.in.: rozpoczęcia, zawieszenia i zakończenia pracy w celu uniemożliwienia dostępu do informacji osobom nieupoważnionym. Określono sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków. W ramach SZBI sporządzono listy aktywów i zbiorów danych osobowych w bezpieczeństwie informacji uwzględniającą nośniki informacji. Przypisano je do Referatów Urzędu oraz wyszczególniono kierowników referatów jako ich właścicieli. Określono również zakaz wynoszenia poza Urząd nośników informacji, w tym dokumentacji papierowej bez wcześniejszego uzyskania upoważnienia, zgodnie z zapisami PN-ISO/IEC 27001 w punkcie A.8.3[16].

(akta kontroli str. 70-71, 78, 80-86, 121, 389-391)

[12] Zarządzenie nr 123/18 Burmistrza Pasłęka z 29 sierpnia 2018 r. w sprawie wyznaczenia inspektora ochrony danych w Urzędzie Miejskim w Pasłęku.
[13] W tym m.in. pełnienie funkcji administratora bezpieczeństwa informacji oraz inspektora bezpieczeństwa teleinformatycznego.
[14] Załącznik nr 6 do PB Urzędu.
[15] Informacje na podstawie Raportu z audytu przedwdrożeniowego, przeprowadzonego w Urzędzie w dniach od 15 lutego do 15 marca 2021 r.
[16] Informacje na podstawie Raportu z audytu powdrożeniowego, przeprowadzonego w Urzędzie 16 czerwca 2021 r.

1.5. W okresie wykonywania pracy zdalnej zasady wynoszenia sprzętów i nośników informacji były określone w PB, Zarządzeniu nr 40/20 Burmistrza Pasłęka z 13 marca 2020 r. w sprawie sposobu organizacji pracy zdalnej pracowników Urzędu Miejskiego w Pasłęku w związku z przeciwdziałaniem COVID-19 (dalej: Zarządzenie 40/20) oraz indywidualnych pisemnych poleceniach wykonywania pracy zdalnej.

PB określała odpowiedzialność osób upoważnionych do przetwarzania informacji w zakresie danych osobowych za naruszenie zasad ich ochrony. Określono m.in. sposób postępowania z nośnikami informacji w przypadku przekazania sprzętu do naprawy dla firmy zewnętrznej oraz warunki nadawania uprawnień do zdalnego dostępu do zasobów sieci Urzędu. W zakresie zapewnienia bezpieczeństwa sprzętu i nośników informacji poza siedzibą obowiązywały procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu oraz zasady szyfrowania informacji zawierających dane osobowe. Z analizy raportu z audytu[17] wynika, iż w ramach PB nie określono zasad zabezpieczenia sprzętu i nośników informacji wynoszonych poza siedzibę Urzędu przed skutkami wynikającymi z materializacji niektórych ryzyk związanych z pracą poza siedzibą Jednostki.

Zarządzenie 40/20 stanowiło, iż w celu przeciwdziałania rozprzestrzenianiu się choroby zakaźnej wywołanej wirusem SARS-CoV-2, pracownikowi Urzędu może zostać wydane polecenie wykonywania, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania, tj. tzw. pracy zdalnej. Polecenie to mogło zostać wydane w formie pisemnej lub ustnej.

Pisemne indywidualne polecenia wykonywania pracy zdalnej zawierały warunki jej wykonywania, m.in. w zakresie udostępniania sprzętu służbowego, jego rodzaju, jak również potwierdzenie powierzenia tego sprzętu.

W dokumentacji obowiązującego od 21 czerwca 2021 r. SZBI, w punkcie „Praca zdalna" Instrukcji zarządzania systemem teleinformatycznym[18] określono warunki wykonywania pracy zdalnej i wskazano m.in., iż wykonywanie pracy zdalnej mogło odbywać się wyłącznie ze sprzętu udostępnionego pracownikowi przez Urząd. W ramach SZBI, zgodnie z listą aktywów, opracowano zabezpieczenia dla poufności, dostępności oraz dla integralności, w tym zabezpieczenia przed wystąpieniem różnych ryzyk związanych z pracą zdalną.

(akta kontroli str. 68, 70-71, 79, 187, 230-235, 241-262, 287-300, 309-323, 386, 412-426)

1.6. Obowiązująca do 20 czerwca 2021 r. PB określała zasady przesyłania informacji głównie w zakresie ochrony danych osobowych. Jako szczególne środki zapewnienia bezpieczeństwa informacji w ww. zakresie wskazano m.in. stosowanie mechanizmów szyfrowania informacji zawierających dane osobowe.

Regulacje SZBI, obowiązujące od 21 czerwca 2021 r. określały zasady przesyłania informacji, w tym m.in. możliwość monitorowania pracy urządzeń znajdujących się w sieci informatycznej Urzędu pod kątem przesyłania i przetwarzania informacji oraz rejestracji zdarzeń związanych z przesyłaniem informacji w oprogramowaniu. W celu zabezpieczenia przesyłanych informacji, danych osobowych pocztą elektroniczną dla określonych kategorii informacji wymagano szyfrowania lub zabezpieczenia hasłem.

[17] Informacje na podstawie Raportu z audytu przedwdrożeniowego, przeprowadzonego w Urzędzie w dniach od 15 lutego do 15 marca 2021 r.

[18] Załącznik nr 9 do Polityki Bezpieczeństwa Informacji Urzędu Miejskiego w Pasłęku.

W regulacjach wewnętrznych Urzędu w zakresie komunikacji w ramach pracy zdalnej:

- określono warunki i możliwość zdalnego dostępu do zasobów i systemów informacyjnych Jednostki poprzez dostęp do oprogramowania elektronicznego obiegu dokumentów,
- dozwolone było korzystanie ze służbowej poczty elektronicznej z komputerów innych niż służbowe, a warunki jakie powinien spełniać dopuszczony komputer oraz sposób postępowania z przesyłanymi informacjami zostały określone w pisemnych poleceniach wykonywania pracy zdalnej,
- zarządzono zabezpieczenia oraz wprowadzono rozwiązania mające na celu zminimalizowanie ryzyka korzystania z prywatnego konta e-mail, tj. m.in. monitoring aktywności użytkowników stanowisk komputerowych,
- określono przypadki wymagające dodatkowego zabezpieczenia wiadomości przekazywanych w formie elektronicznej oraz sposoby realizacji tych zabezpieczeń.

(akta kontroli str. 7-8, 79, 112, 120-121, 209-210, 230-235, 241-262, 287-300, 309-323)

1.7. W dokumentacji PB określono procedurę zarządzania incydentami w przypadku naruszenia ochrony danych osobowych oraz postępowanie w przypadku wystąpienia tych incydentów. Procedura polegała m.in. na każdorazowej weryfikacji przez IOD czy zdarzenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych oraz określała sposób postępowania IOD w sytuacji, gdy takie ryzyko występowało. Sposób postępowania w sytuacji naruszenia ochrony danych osobowych zawarty był w Instrukcji[19], która określała m.in. podstawy stwierdzenia naruszenia systemu ochrony danych osobowych oraz typowe zagrożenia bezpieczeństwa tych danych. Instrukcja ta określała również sposób postępowania w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych pracowników Urzędu i IOD, procedurę działań korygujących i zapobiegawczych oraz opis czynności. W ramach Planu ciągłości opracowano procedury sygnalizowania i reagowania na incydenty związane z bezpieczeństwem informacji przypisane zespołowi antykryzysowemu. Do jego zadań należała m.in. analiza stanu bezpieczeństwa oraz wpływu zaistniałego incydentu na działalność jednostki.

W dokumentacji SZBI opracowano procedury sygnalizowania i reagowania na incydenty związane z bezpieczeństwem informacji. W ramach tej regulacji przypisano określonym pracownikom Urzędu odpowiedzialność w zakresie tych procedur, tj. KSZBI i KBT oraz IOD.

W okresie kontrolowanym odnotowano dwa zdarzenia związane z zagrożeniem bezpieczeństwa danych osobowych. Miały one miejsce w lutym 2021 r., tj. w czasie obowiązywania PB. Związane były one z próbą podjęcia nieuprawnionego dostępu do zasobów dyskowych oraz możliwością zainstalowania niezatwierdzonego oprogramowania. Incydenty nie dotyczyły pracy zdalnej i zostały zidentyfikowane w związku z pracą wykonywaną w budynku Urzędu. Zastosowano środki eliminujące niebezpieczeństwo, a IOD sfomułował rekomendacje w zakresie przeciwdziałania podobnym zagrożeniom.

(akta kontroli str. 56-57, 69-70, 77, 120-121, 151-159)

1.8. W Urzędzie nie opracowano oddzielnego regulaminu dotyczącego świadczenia pracy w trybie zdalnym. Odbywała się ona na podstawie regulacji opisanych w punkcie 1.5. niniejszego wystąpienia. Polecenia wykonywania pracy zdalnej zawierały: warunki jej podjęcia, sposoby powierzania zadań do wykonania, sposoby

[19] Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych stanowiącą załącznik nr 8 do PB Urzędu.

komunikacji na odległość, zapis o powierzeniu sprzętu, zakres udzielonego upoważnienia, określenie miejsca wykonywania pracy zdalnej oraz okres jej wykonywania. Polecenia wykonywania pracy zdalnej z wykorzystaniem sprzętu prywatnego zawierały dodatkowo udzielenie zgody pracodawcy na korzystanie ze sprzętu będącego własnością pracownika oraz zobowiązanie pracownika do zabezpieczenia sprzętu poprzez m.in. ograniczenie dostępu do plików tylko dla pracownika oraz zainstalowanie zaakceptowanego przez informatyka aktualnego oprogramowania antywirusowego. W poleceniach tych określono również wymagania, jakie musi spełniać sprzęt co do systemów operacyjnych.

Procedury zawierające sposoby zapewnienia bezpieczeństwa danych osobowych przy realizacji zadań wykonywanych w pracy zdalnej określone zostały w PB. Pracownicy Urzędu zapoznali się z zapisami tej Polityki, co potwierdzone było podpisanymi oświadczeniami. W ramach pisemnego polecenia wykonywania pracy zdalnej z wykorzystaniem sprzętu służbowego wydawano pracownikowi upoważnienie do zdalnego dostępu do komputera używanego w ramach zadań realizowanych w Urzędzie. Pracownik przyjmując polecenie pracy zdalnej podpisywał jednocześnie oświadczenie o przyjęciu warunków tej pracy. Polecenia pracy zdalnej wykonywanej z wykorzystaniem sprzętu niebędącego własnością pracodawcy zawierały zobowiązanie pracownika do stosowania określonych zabezpieczeń.

Praca w formie zdalnej świadczona była w Urzędzie w okresie od 18 marca 2020 r. do 20 maja 2021 r., tj. w okresie obowiązywania PB.

W ustanowionym i wdrożonym 21 czerwca 2021 r. SZBI określono zasady dotyczące bezpieczeństwa informacji w pracy świadczonej na odległość, w tym zasady korzystania z Internetu oraz urządzeń służących do pracy zdalnej (wyłącznie sprzęt służbowy), sposób postępowania z dokumentami w formie papierowej, metody zabezpieczenia przekazywanych informacji, a także procedury postępowania w szczególnych sytuacjach (np. awarie sprzętu lub oprogramowania, utrata sprzętu, dokumentów lub nośników informacji).

W regulacjach dotyczących organizacji pracy zdalnej w Urzędzie nie określono warunków BHP, jakie musi spełniać miejsce jej świadczenia. Z wyjaśnień Burmistrza wynika, iż Zarządzenie nr 40/20 wskazywało, że miejsce wykonywania pracy zdalnej wyznaczone było w porozumieniu z pracownikiem. Porozumienie to polegało m.in. na ustnym ustaleniu z pracownikiem, czy miejsce pracy spełnia podstawowe warunki bezpieczeństwa pracy. Z wyjaśnień Burmistrza wynika również, iż podstawowe zasady dotyczące bezpieczeństwa pracy zdalnej w zakresie BHP regulowane były przez ogólnie obowiązujące akty prawne, tj. Kodeks Pracy oraz Regulamin pracy Urzędu Miejskiego w Pasłęku, z którymi pracownicy byli zapoznawani w trakcie wstępnych i okresowych szkoleń z zakresu BHP.

(akta kontroli str. 17-32, 122-135, 230-235, 241-262, 287-300, 309-323)

1.9. W okresie kontrolowanym pracownicy Urzędu byli zapoznawani z zagrożeniami dotyczącymi bezpieczeństwa informacji. W zakresie skutków naruszania zasad bezpieczeństwa informacji oraz stosowania środków zapewniających bezpieczeństwo informacji określonych w § 20 ust. 2 pkt 6 KRI w 2021 r. odbyły się dwa szkolenia on-line, w którym uczestniczyło 10 osób, tj. audytorzy wewnętrzni SZBI oraz kierownicy referatów Urzędu. Główną formą szkolenia w zakresie bezpieczeństwa informacji w Urzędzie było samokształcenie pracowników w ramach regulacji wewnętrznych Jednostki. Zapoznanie z regulacjami potwierdzane było przez pracowników podpisami. Szkolenie on-line w zakresie SZBI w 2021 r. odbyły cztery osoby wdrażające system. W ramach przeprowadzonych w okresie kontrolowanym kontroli wewnętrznych w zakresie

bezpieczeństwa informacji prowadzony był instruktaż informatyka. Inspektor prowadził również instruktaż nowych pracowników Urzędu w zakresie RODO.

(akta kontroli str. 17-32, 150)

1.10. W okresie obowiązywania w Urzędzie PB, dokumentacja ta nie była aktualizowana, w tym w związku z zarządzeniem organizacji pracy zdalnej w Urzędzie. Przeglądu aktualności dokumentacji dokonano w 2020 r. przez IOD, w ramach audytu wewnętrznego[20] oraz w poszczególnych referatach Urzędu.

Z wyjaśnień Burmistrza wynika, iż wprowadzone w ramach PB rozwiązania i procedury, tj. m.in. umożliwienie dostępu zdalnego do systemów Urzędu, zabezpieczenia sprzętu, sposób rozpoczęcia i zakończenia pracy, procedura haseł, szyfrowanie nośników i połączeń z siecią w całości pozwalały na realizację pracy pracowników poza główną siedzibą Urzędu. W ocenie Burmistrza nie doszło do zmian w prawie wymagających aktualizacji Polityki bezpieczeństwa, czy też innych znaczących zmian w funkcjonowaniu Urzędu. Wszelkie procedury przygotowane w PB przewidywały możliwość pracy zdalnej.

W styczniu 2021 r. zawarto umowę z podmiotem zewnętrznym, w wyniku której przeprowadzono audyt przedwdrożeniowy weryfikujący poziom spełnienia wymagań określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, minimalnych wymagań dla systemów teleinformatycznych oraz wybranych elementów PN-EN ISO/IEC 27001:2017-06 Systemu Zarządzania Bezpieczeństwem Informacji w Gminie Pasłęk – Urzędzie Miejskim w Pasłęku. W ramach tej umowy podmiot zewnętrzny stworzył dokumentację SZBI (wprowadzona Zarządzeniem nr 68/21 Burmistrza Pasłęka z 11 czerwca 2020 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Pasłęku) oraz przeprowadził audyt powdrożeniowy w dniu 16 czerwca 2021 r.

(akta kontroli str. 111, 114-119, 136-141, 144, 160-169, 191-202, 360-430, 469-471)

Stwierdzone nieprawidłowości

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

Obowiązująca do 20 czerwca 2021 r. PB nie była zgodna z zapisami § 20 ust. 1 i 2 rozporządzenia KRI, bowiem zgodnie z § 20 ust. 3 rozporządzenia wymagania te można uznać za spełnione w przypadku jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie PN-ISO/IEC 27001. PB nie spełniała minimalnych wymagań w odniesieniu m.in. do punktów A. 8.1, A.8.2 i A.8.3 Normy. Nie zawierała m.in. klasyfikacji informacji, uwzględniającej wymagania prawne, wartość, krytyczność i wrażliwość na nieuprawnione ujawnienie lub modyfikację, która jest jednym z zabezpieczeń wskazanych w Normie (A.8.2.1), zapewniających przypisanie informacjom odpowiedniego poziomu ochrony.

Z wyjaśnień Burmistrza wynika, iż regulacje obejmujące zagadnienia bezpieczeństwa informacji, które funkcjonowały w Urzędzie przed 21 czerwca 2021 r., spełniały wymogi określone w przepisach KRI, w tym szczególnie te określone w § 20 ust. 1 i 2 ww. rozporządzenia, co potwierdziły audyty przeprowadzone przez audytora wewnętrznego oraz raport z audytu przedwdrożeniowego przeprowadzonego przez podmiot zewnętrzny w Urzędzie w dniach od 15 lutego 2021 r. do 15 marca 2021 r.

[20] Sprawozdanie z audytu wewnętrznego, nr zadania audytowanego: 3/2020, z 21 grudnia 2020 r.; temat zadania: „Organizacja Urzędu Miejskiego – Bezpieczeństwo Informacji wewnętrznej oraz zabezpieczenie mienia".

Analiza wyników ww. audytu przedwdrożeniowego wykazała, że ocena ogólna audytu zawierała stwierdzenie, iż część minimalnych wymagań obowiązujących regulacji KRI została określona i jest w procesie wdrażania, ale jedynie dla przetwarzania danych osobowych. Jednocześnie ustalenia audytu wewnętrznego wskazują, iż jedyną podstawą prawną dla wdrożenia i stosowania PB było RODO. Zdaniem Najwyższej Izby Kontroli nie można zatem uznać, że PB spełniała wymagania rozporządzenia KRI w pełnym zakresie bezpieczeństwa informacji.

(akta kontroli str. 122-130, 365-366, 369-411)

OCENA CZĄSTKOWA

W Urzędzie w 2018 r. wprowadzono PB, która odnosiła się do jednego z obszarów bezpieczeństwa informacji, tj. przetwarzania danych osobowych określonego w RODO i w zakresie tego rodzaju informacji częściowo spełniała minimalne wymagania PN-ISO/IEC 27001. Dokumentacja ta w 2020 r. została poddana przeglądowi. Nie była aktualizowana, m.in. w zakresie zmian związanych z wprowadzaniem w Urzędzie pracy zdalnej w związku z pandemią wirusa SARS-CoV-2, niemniej regulacje w niej zawarte przewidywały rozwiązania umożliwiające wykonywanie pracy na odległość. W styczniu 2021 r. podjęto współpracę z podmiotem zewnętrznym, w wyniku której opracowano i dopiero 21 czerwca 2021 r. wdrożono w Urzędzie SZBI zgodny z wymogami KRI.

Organizacja pracy zdalnej w Urzędzie w zakresie zapewnienia bezpieczeństwa informacji odbywała się na podstawie PB, Zarządzenia nr 40/20 Burmistrza Pasłęka z 13 marca 2020 r. w sprawie sposobu organizacji pracy zdalnej pracowników Urzędu Miejskiego w Pasłęku oraz indywidualnie wydawanego pisemnego polecenia wykonywania pracy zdalnej.

Pracownicy Urzędu zapoznawani byli z obowiązującymi zasadami bezpieczeństwa informacji, a kadra wdrażająca SZBI odbyła odpowiednie szkolenia.

W Urzędzie powołano IOD, który posiadał odpowiednie kwalifikacje i doświadczenie z zakresu prawa i praktyk w dziedzinie ochrony danych osobowych, a jego obowiązki określone zostały w wewnętrznych uregulowaniach Jednostki.

OBSZAR

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

Opis stanu faktycznego

2.1. Praca zdalna wykonywana była przez pracowników Urzędu w okresie od 18 marca 2020 r. do 20 maja 2021 r. W 2020 r. wykonywało ją 44 spośród 71 zatrudnionych w Urzędzie pracowników, a w 2021 r.- 4 z 69. Polecenia wykonywania pracy w tej formie wydawane były w głównej mierze z inicjatywy pracodawcy i miały na celu przeciwdziałanie rozprzestrzeniania się wirusa SARS-CoV-2[21] oraz zapewnienie ciągłości pracy Urzędu. Praca zdalna wykonywana była naprzemiennie ze sposobem stacjonarnym.

(akta kontroli str. 191, 195-202)

2.2. W okresie wykonywania przez pracowników Urzędu pracy zdalnej obowiązywały zasady w zakresie bezpieczeństwa informacji, dotyczące w głównej mierze danych osobowych, w ramach PB. Zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna oraz sposoby stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowań minimalizujących ryzyko błędów ludzkich zawarte były w tej dokumentacji. Pracownicy zapoznawali się z tymi zasadami w głównej mierze poprzez samokształcenie (opisano w punkcie 1.1.

[21] W okresie kontrolowanym w okresie izolacji i w czasie kwarantanny w sumie pracowało sześciu pracowników. W jednym przypadku wydano polecenie pracy zdalnej z wniosku pracownika.

wystąpienia). W podpisywanych indywidualnych poleceniach wykonywania pracy zdalnej zawarte były wymagania i warunki jej wykonywania (opisano w punkcie 1.8. wystąpienia).

(akta kontroli str. 17-32, 68-81, 150)

2.3. Na potrzeby wykonywania pracy zdalnej użytkowano 19 komputerów przenośnych. Ze sprzętu tego korzystało 29 pracowników Urzędu w 2020 r. i jeden w 2021 r. Z komputera prywatnego - sześciu w 2020 r., spośród których jeden również w 2021 r. Wszyscy pracownicy skierowani do pracy zdalnej korzystali z prywatnych telefonów komórkowych w celu komunikacji głosowej.

Analiza dokumentacji dotyczącej wykonywania pracy zdalnej przez pięciu pracowników Urzędu wykazała m.in., iż:

- pisemne polecenia wykonywania pracy zdalnej zawierały powierzenie określonego sprzętu komputerowego,
- wydawano upoważnienie do zdalnego dostępu do komputera używanego przez pracownika w ramach zadań realizowanych w Urzędzie,
- zadania wyznaczone pracownikom dotyczyły prowadzenia bieżących spraw w obrębie referatu,
- nadawano i odbierano dostęp do sieci VPN Urzędu zgodnie z wyznaczonymi w poleceniach terminami,
- usługi dostępne w sieci VPN umożliwiały wykonywanie wyznaczonych pracownikom zadań,
- pracownicy na potrzeby wykonywania wyznaczonych zadań korzystali wyłącznie z poczty służbowej,
- informacje przesyłane za pośrednictwem poczty elektronicznej zawierające dane osobowe były szyfrowane,
- komputery przenośnie wykorzystywane w pracy zdalnej miały zablokowany dostęp nośników USB.

(akta kontroli str. 189-190, 309-359)

2.4. W Jednostce stosowano środki służące ochronie przetwarzanych danych w pracy zdalnej. Były to m.in. weryfikacja przez informatyka zakresu uprawnień w celu nadania dostępu do sieci VPN Urzędu i dostępu do specjalistycznego oprogramowania, stosowanie szyfrowania dysku, stosowanie hasłowanego dostępu do konta pracownika na poziomie użytkownika oraz udostępniono możliwość korzystania z serwera plików.

(akta kontroli str. 145-149, 203-208, 324-359)

2.5. Obowiązująca w okresie wykonywania przez pracowników Urzędu pracy zdalnej PB dopuszczała możliwość korzystania z prywatnych komputerów. Pracę zdalną z wykorzystaniem sprzętu niebędącego własnością pracodawcy (laptopy) wykonywało sześciu pracowników w całym okresie jej świadczenia w Urzędzie. Główną przyczyną wydania polecenia w tym zakresie był brak sprzętu służbowego z uwagi na wykorzystanie go przez innych pracowników w tym czasie.

Na podstawie analizy dokumentacji dotyczącej wykonywania pracy zdalnej przez sześciu pracowników Urzędu, którym polecono wykonywanie jej z wykorzystaniem prywatnych laptopów ustalono m.in., iż:

- pracownicy ci w indywidualnych poleceniach wykonywania pracy zdalnej zostali zobowiązani do przestrzegania bezpieczeństwa poprzez zabezpieczenie sprzętu,
- wszystkie pisemne polecenia wykonywania pracy zdalnej wydawane w ww. zakresie zawierały oznaczenie sprzętu,

- sprzęt ten był weryfikowany przez informatyka zgodnie z określonymi wymogami, a fakt ten był potwierdzany w Rejestrze przydzielonych dostępów VPN do sieci Urzędu,
- zadania wyznaczone pracownikom dotyczyły prowadzenia bieżących spraw w obrębie referatu,
- nadawano i odbierano dostęp do sieci VPN Urzędu zgodnie z wyznaczonymi w poleceniach terminami,
- każdy z ww. pracowników uzyskał dostęp do usług udostępnionych w sieci VPN Urzędu, które umożliwiały wykonywanie wyznaczonych zadań,
- korespondencja elektroniczna między pracownikami Urzędu zawierająca dane osobowe była szyfrowana.

(akta kontroli str. 230-286, 145, 148-149)

W toku czynności kontrolnych stwierdzono również, iż w przypadku trzech pracowników, w pisemnych poleceniach wykonywania pracy zdalnej nie zawarto informacji o powierzeniu sprzętu służbowego ani zgody pracodawcy na korzystanie ze sprzętu będącego własnością pracownika, wymagając jednocześnie, żeby kontakt z przełożonymi realizowany był m.in. za pośrednictwem poczty elektronicznej. Dwojgu spośród ww. pracowników w okresie od 25 marca do 14 grudnia 2020 r. (dla pracy zdalnej wykonywanej w okresie od 26 marca do 24 grudnia 2020 r.) zostały przydzielone uprawnienia dostępu do sieci VPN Urzędu. Nadano je kolejno dla 7 spośród 12 wszystkich wydanych poleceń pierwszemu pracownikowi i 10 – drugiemu, zgodnie z datami okresów wykonywania pracy zdalnej wyznaczonymi w pisemnych poleceniach. Polecenia te, z wyłączeniem dwóch pierwszych dla każdego z ww. pracowników nie zawierały upoważnień do zdalnego dostępu do usług udostępnianych przez Urząd.

Ustalono również, iż zadania przydzielone w ramach pracy zdalnej wszystkim trzem ww. pracownikom nie wymagały dostępu do sieci VPN Urzędu.

Informatyk Urzędu wyjaśnił, iż w okresie od 25 marca do 14 grudnia 2020 r. nadał upoważnienia dostępu do sieci VPN Urzędu dwóm pracownikom, po uzyskaniu ustnej informacji od Kierownika Referatu Organizacyjnego o skierowaniu tych osób na pracę zdalną. Natomiast z otrzymanych pisemnych poleceń wykonywania pracy zdalnej wynikało, iż osoby te będą wykonywały pracę zdalną bez sprzętu. Po uzyskaniu takiej informacji Informatyk nie aktywował profilu pracownika, co uniemożliwiło połączenie z siecią VPN. Nie przekazywał on loginu i hasła tym pracownikom.

Z wyjaśnień ww. dwóch pracowników wynika, iż podczas wykonywanych przez nich zadań w ramach pracy zdalnej z wykorzystaniem komputerów prywatnych, spośród usług udostępnianych przez Urząd korzystali wyłącznie z poczty służbowej.

(akta kontroli str. 239-286)

2.6. W okresie wykonywania pracy zdalnej nie udzielano pracownikom Urzędu upoważnień w zakresie pobierania oryginałów dokumentów. Skany dokumentów na potrzeby prowadzenia bieżących spraw przekazywano za pośrednictwem służbowej poczty e-mail, a także innych usług i zasobów dostępnych za pomocą połączenia VPN.

(akta kontroli str. 112-113, 145, 148-149, 194, 324-359)

2.7. Pisemne polecenia wykonywania pracy zdalnej zobowiązywały pracownika m.in. do potwierdzania gotowości do podjęcia pracy bezpośredniemu przełożonemu oraz do przedstawiania mu skróconej informacji o wykonanych zadaniach. Zakres zadań przekazywany był pisemnie za pośrednictwem poczty e-mail oraz poprzez kontakt telefoniczny, a poziom zaawansowania wykonania wyznaczonych zadań był

monitorowany i nadzorowany. Nadzór ten pełnili kierownicy referatów oraz Burmistrz w zakresie pracy kierowników.

W okresie wykonywania pracy zdalnej przez pracowników Urzędu nie odnotowano sytuacji niewykonania wyznaczonych zadań, ani nie odwołano żadnego polecenia w związku z niewywiązywaniem się pracownika z wyznaczonych mu zadań. Nie zgłoszono incydentów związanych z bezpieczeństwem informacji w związku z wykonywaniem pracy zdalnej przez pracowników Urzędu.

Monitorowanie i nadzorowanie wykonywania pracy zdalnej w zakresie bezpieczeństwa informacji odbywało się m.in. poprzez monitorowanie przez Informatyka logowań pracowników w programach dziedzinowych oraz w programie obsługującym elektroniczny obieg dokumentów oraz weryfikowanie upoważnień pracowników w celu nadania dostępu do sieci VPN Urzędu.

(akta kontroli str. 203-229, 230-235, 241-262, 287-300, 309-323)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

NIK pozytywnie ocenia działania Burmistrza w zakresie wdrażania i stosowania przyjętych w Urzędzie rozwiązań organizacyjnych i technicznych mających na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej. Praca ta wykonywana była w głównej mierze z inicjatywy pracodawcy i miała na celu przeciwdziałanie rozprzestrzenianiu się wirusa SARS-CoV-2 oraz zapewnienie ciągłości funkcjonowania Urzędu.

W okresie wykonywania pracy zdalnej w Urzędzie stosowano rozwiązania organizacyjne zapewniały odpowiedni poziom bezpieczeństwa informacji głównie w zakresie ochrony danych osobowych.

Pracownicy, którym polecono wykonywanie pracy w formie zdalnej stosowali obowiązujące rozwiązania techniczne i technologiczne podnoszące poziom bezpieczeństwa informacji. W celu wykonywania pracy zdalnej korzystano w głównej mierze ze sprzętu służbowego. Dopuszczona możliwość korzystania przez pracowników z komputerów prywatnych (laptopów), stanowiła niewielki udział w skali wszystkich poleceń wykonywania pracy w formie zdalnej. W przypadku trzech pracowników stwierdzono, iż polecono im wykonywanie pracy zdalnej bez sprzętu komputerowego, wymagając jednocześnie, żeby kontakt z przełożonymi realizowany był m.in. za pośrednictwem poczty elektronicznej. Dwojgu spośród ww. pracowników na przestrzeni 2020 r. przydzielono dostęp do sieci VPN Urzędu mimo, iż nie udzielono im stosownych upoważnień. Zdarzenia te jednak nie miały znaczącego wpływu na realizację zadań w ramach pracy zdalnej, w tym również w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie.

Wszyscy pracownicy zostali zapoznani z zasadami dotyczącymi bezpieczeństwa informacji w wykonywaniu pracy zdalnej.

IV. Uwagi i wnioski

W związku z wyeliminowaniem stwierdzonej nieprawidłowości polegającej na tym, że do 20 czerwca 2021 r. obowiązująca PB nie była zgodna z zapisami § 20 ust. 1, 2 i 3 rozporządzenia KRI, Najwyższa Izba Kontroli nie formułuje wniosków ani 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 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.

Olsztyn, 29 listopada 2021 r.

Kontroler
Emilia Wasilewska
Inspektor kontroli państwowej

.....
podpis

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

.....
podpis