NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.017.02.2022

Pan
Prof. dr hab. Jacek Majchrowski
Prezydent Miasta Krakowa
pl. Wszystkich Świętych 3-4
31-004 Kraków

WYSTĄPIENIE POKONTROLNE

P/22/082 - Zarządzanie oprogramowaniem komputerowym przez administrację publiczną

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Krakowa, pl. Wszystkich Świętych 3-4,31-004 Kraków (dalej: Urząd, UMK)
Kierownik jednostki kontrolowanej	Jacek Majchrowski, Prezydent Miasta Krakowa, od 2002 r.
Zakres przedmiotowy kontroli	1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym. 2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem.
Okres objęty kontrolą	Lata 2019 – 2022 do dnia zakończenia kontroli, z wykorzystaniem dowodów wytworzonych przed i po tym okresie, jeżeli miały one istotny wpływ dla ustaleń i ocen kontroli.
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 Krakowie
Kontroler	Piotr del Fidali, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/122/2022 z 12 sierpnia 2022 r. oraz nr LKR/144/2022 z 12 października 2022 r.

(akta kontroli str. 1-2)

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Urząd rzetelnie zorganizował proces postępowania z oprogramowaniem, nie był on jednak w pełni skuteczny. NIK ocenia negatywnie zaniechanie w okresie od listopada 2021 r. do kwietnia 2022 r. comiesięcznej weryfikacji legalności zainstalowanego oprogramowania, podczas gdy kontrola przeprowadzona w maju 2022 r. wykazała, że liczba pozycji nieautoryzowanego oprogramowania wzrosła z 11 przypadków na 176 badanych komputerów w październiku 2021 r. do 129 pakietów oprogramowania na stu badanych stacjach roboczych.

NIK ocenia pozytywnie przyjęte w UMK zasady zarządzania oprogramowaniem. Sprzyjały one bieżącej, prawidłowej realizacji zadań publicznych. Zasady te odnosiły się do wszystkich etapów związanych z nabyciem, użytkowaniem oraz likwidacją oprogramowania. W Urzędzie zgromadzono kompletne dane o posiadanych licencjach i oprogramowaniu komputerowym i aktualizowano je na bieżąco. Narzędzia do monitorowania licencji użytkowane w Urzędzie umożliwiały weryfikację instalowanego oprogramowania zarówno dla środowiska stacji roboczych/laptopów, urządzeń mobilnych jak i serwerów.

W Urzędzie określono zasady nabywania oprogramowania, a środki publiczne na zakup i użytkowanie oprogramowania wydatkowane były gospodarnie. Urząd podejmował na ogół skuteczne działania w celu optymalizacji wykorzystania oprogramowania, przy czym nie posiadał narzędzia do bieżącej analizy jego wykorzystania. Analizy możliwych do wdrożenia rozwiązań pozwalających optymalnie wykorzystywać posiadane oprogramowanie przeprowadzane były w Zespole Zarządzania Zmianą, który został utworzony w ramach Centrum Obsługi Informatycznej UMK. NIK zwraca uwagę na nieefektywne wykorzystanie zakupionych w 2021 r. za kwotę 54,3 tys. zł licencji V., z których większość (45 z 48) nie była użytkowana.

NIK zwraca również uwagę, na niezapewnienie pełnej rozliczalności użytkowników Zintegrowanego Systemu Wspomagania Zarządzania Miastem. W przypadku trzech modułów tego systemu nie przechowywano danych o logowaniach użytkowników.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[3] kontrolowanej działalności

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym.

Opis stanu faktycznego

W UMK określono zasady i procedury zarządzania oprogramowaniem komputerowym niezbędne dla bieżącej realizacji zadań publicznych. Obejmowały one kwestie związane z nabywaniem, wdrażaniem, użytkowaniem i bieżącym nadzorowaniem oprogramowania. Procedury regulowały zagadnienia dotyczące m. in. przypisanych ról i odpowiedzialności, nabywania i wycofywania licencji, dowodów, zakup zarządzania bezpieczeństwem nośników instalacyjnych, monitorowania licencji. Urząd nie posiadał jednak narzędzia do bieżącej analizy wykorzystania zakupionych licencji.

(akta kontroli str. 8-11, 345-350)

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej. W niniejszym wystąpieniu zastosowano ocenę opisową.

[3] 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.

Dyrektor Magistratu wyjaśniła że Urząd nie posiadał narzędzia do automatycznej analizy bieżącego/aktywnego wykorzystania zakupionych licencji. Dodała, że 13 grudnia 2018 r. rozpoczęto rozpoznawanie rynku w celu zakupu takiego oprogramowania, jednak koszt takiego zakupu okazał się zbyt wysoki dla UMK. Z tego względu zrezygnowano z wprowadzenia takiego mechanizmu. Koszt wdrożenia systemu zapewniającego bieżące monitorowanie wykorzystania zakupionych licencji wraz z asystą techniczną oszacowano na 704,1 tys. zł.

(akta kontroli str. 37-38, 326-328)

Obowiązujące procedury podlegały regularnym przeglądom i były doskonalone. Wprowadzane, w okresie objętym kontrolą, zmiany wynikały m.in. z wprowadzenia na szeroką skalę pracy zdalnej oraz zmian organizacyjnych. Miały też charakter uszczegóławiający obowiązujące zapisy.

(akta kontroli str. 8-11, 345-350)

W toku kontroli zlecono biegłemu sporządzenie opinii, która obejmowała m.in. sprawy związane z wdrożonymi zasadami zarządzania licencjami na oprogramowanie. W opinii biegłego zarządzenie dotyczące przeglądu legalności oprogramowania nie wskazuje na konieczność:

Zdaniem biegłego brak ustanowienia szczegółowych, kompletnych (w ramach całego cyklu życia oprogramowania i licencji) zasad zarządzania licencjami, w tym związanych z wykonywaniem przeglądów może utrudniać lub uniemożliwiać skuteczne zarządzanie i nadzór nad licencjami. Istnieje ryzyko naruszeń warunków licencji lub naruszeń warunków własności intelektualnej. Możliwe są skutki finansowe (np. konieczność wypłaty odszkodowania i poniesienia kosztów prawnych) oraz skutki niefinansowe (np. utrata reputacji).

(akta kontroli str. 148-164)

W Systemie Zarzadzania Bezpieczeństwem Informacji[4], Standardach usług teleinformatycznych w Urzędzie[5] oraz zakresach czynności Administratorów Technicznych określono Zadania związane z:

- dokonywania przeglądu wszystkich wykorzystywanych w Systemie Informatycznym (SI) Urzędu systemów operacyjnych (w tym serwerowych systemów operacyjnych oraz systemów operacyjnych zainstalowanych na urządzeniach typu smartfon/tablet),
- wykonywania dedykowanego przeglądu stacji komputerowych przypisanych do użytkowników posiadających uprawnienia administracyjne (pozwalające na samodzielne instalowanie oprogramowania),
- przedstawiania w raportach pokontrolnych przyczyn pojawienia się nieautoryzowanego oprogramowania,
- przedstawiania w raportach rekomendacji kierunkowych celem minimalizowania zjawiska instalacji nieautoryzowanego oprogramowania (np.: prowadzenie dodatkowych szkoleń użytkowników z przestrzegania obowiązujących zasad, wdrożenie w narzędziach bezpieczeństwa IT blokad pobierania nieautoryzowanego w UMK oprogramowania, odbieranie uprawnień administracyjnych, zgłaszanie incydentów bezpieczeństwa, stosowanie indywidualnych pouczeń),
- dokonywania przeglądu lokalnych i serwerowych zasobów plikowych celem identyfikacji danych multimedialnych i innych plików, których przechowywanie prowadzi do naruszenia praw autorskich.

[4] Zarządzenie Prezydenta Miasta Krakowa nr 958/2010 z 30 kwietnia 2010 r.

[5] Zarządzenie Prezydenta Miasta Krakowa nr 3376/2016 z 9 grudnia 2016 r.

Czynności te wykonywane były w ramach bieżących zadań Administratorów Technicznych, którzy pracują i opiekują się stacjami roboczymi pracowników UMK w różnych lokalizacjach Urzędu.

(akta kontroli str. 236-237, 345-350)

W UMK nie ustanowiono i nie zastosowano procedury regulującej zasady dopuszczania i wykorzystywania w SI UMK oprogramowania narzędziowego. Urząd zdiagnozował ten problem w trakcie przeprowadzonego w grudniu 2021 r. audytu bezpieczeństwa informacji. W wyniku ustaleń z przeprowadzonego audytu podjęto działania doskonalące, które są w trakcie realizacji. Planowana data ich wdrożenia to koniec 2022 r.

(akta kontroli str. 8-11, 125-136, 148-164)

W Urzędzie zapewniono dostępność zasobów kadrowych niezbędnych do realizacji poszczególnych zadań w procesie zarządzania licencjami oprogramowaniem komputerowym. W zakresach czynności pracowników znajdowały się zapisy odnoszące się do zarządzania aplikacjami i bezpieczeństwa systemu informatycznego Urzędu. W okresie objętym kontrolą sprawy obsługi informatycznej Magistratu, elektronicznej obsługi mieszkańców oraz koordynacja działań związanych z objęciem wspólnymi rozwiązaniami informatycznymi Magistratu i jednostek organizacyjnych zostały powierzone Wydziałowi Informatyki. Od 1 czerwca 2020 r. został on przekształcony w Centrum Obsługi Informatycznej (COI). COI działało na podstawie szczegółowych zarządzeń Prezydenta, w których określono jego strukturę organizacyjną oraz zakres zadań i odpowiedzialności poszczególnych komórek organizacyjnych wchodzących w jego skład. Pracownikom przypisano role i obowiązki w zakresach czynności, które były przez nich potwierdzane własnoręcznym podpisem. Zadania związane z zarządzaniem oprogramowaniem w UMK realizowało od 47 osób w 2019 r. do 67 osób w 2022 r.

(akta kontroli str. 36-37, 310-328, 348-350)

Pracownicy posiadali odpowiednie kwalifikacje i byli regularnie szkoleni. W 2019 r. w szkoleniach z pięciu tematów[6] wzięło udział 9 pracowników COI, w 2020 r. w 11[7] szkoleniach udział wzięło 17 pracowników, w 2021 r. w 11[8] szkoleniach udział wzięło 15 pracowników, a w 2022 r. w 14[9] szkoleniach udział wzięło 36 pracowników. Koszty udziału w szkoleniach oraz koszty związanych z nimi podróży służbowych wyniosły 16,2 tys. zł w 2019 r., 36,6 tys. zł w 2020 r., 29,2 tys. zł w 2021 r. oraz 50,8 tys. zł w 2022 r.

(akta kontroli str. 36-37, 317-325)

W COI wydzielono m.in. referat ds. zarządzania aplikacjami oraz referat ds. analiz i utrzymania zasobów stanowiskowych. Zatrudnienie w COI wzrosło z 69 osób na koniec 2019 r. do 118 pracowników na koniec września 2022 r. W referacie ds. zarządzania aplikacjami zatrudnionych było 14 osób a w referacie ds. analiz i utrzymania zasobów stanowiskowych cztery osoby.

(akta kontroli str. 36-37, 332-33, 348-350)

[6]Tematami szkoleń były m.in.: Prawo autorskie i ochrona know-how w umowach IT; Umowy na utrzymanie, serwis i rozwój systemów IT; Umowy IT-projekty realizowane w metodykach zwinnych.

[7]Tematami szkoleń były m.in.: Prawo autorskie w praktyce; Wdrożenia IT-jak przygotować dobrą umowę.

[8]Tematami szkoleń były: Prawo Autorskie i ochrona know-how w umowach IT; Umowy IT-licencje i prawa autorskie; Certyfikowany Manager ds. Licencji Audyt IT-dla średniozaawansowanych.

[9]Tematami szkoleń były: Umowy IT w praktyce – case study typowe i najczęstsze problemy oraz praktyczne rozwiązania dotyczące wybranych umów IT; Umowy na korzystanie z oprogramowania w chmurze obliczeniowej – wyzwania, ryzyka i praktyczne aspekty zawierania i negocjowania umów na cloud computing; Umowy wdrożeniowe na systemy IT- aspekty prawne i praktyczne; Praktyczna strona umów IT; Umowy na utrzymanie, serwis i rozwój systemów IT - najlepsze praktyki i sporne kwestie; Prawo autorskie i ochrona know-how w umowach IT – ujęcie praktyczne.

Urząd odnotowywał problemy z pozyskaniem pracowników na stanowiska związane z procesem zarządzania licencjami/oprogramowaniem komputerowym. Wynikały one z braku zgłoszeń kandydatów, niespełnienia przez nich warunków formalnych, niezgłoszeniu się na testy kwalifikacyjne, nieuzyskania minimalnej wymaganej liczby punktów w ramach testu kwalifikacyjnego lub rozmowy kwalifikacyjnej, rezygnacji z udziału w rozmowie kwalifikacyjnej. W okresie objętym kontrolą nie udało się pozyskać pracowników na stanowiska związane z procesem zarządzania licencjami/oprogramowaniem komputerowym w ramach 16 spośród 77 naborów do COI.

(akta kontroli str. 33-34, 332-333, 348-350)

Urząd posługiwał się outsourcingiem usług w obszarach hostingu i administracji technicznej, budowy, wdrażania, aktualizacji i rozwoju oprogramowania, analizy biznesowej oraz audytu oprogramowania. Outsourcing usług stosowano również w zakresie Biuletynu Informacji Publicznej oraz portali internetowych Urzędu.

(akta kontroli str. 19-22)

W UMK prowadzono i aktualizowano informację o posiadanych licencjach i oprogramowaniu komputerowym. Przed zakończeniem aktywności produktu lub w przypadku przedłużania licencji dokonywano przeglądów wykorzystania oprogramowania. Nadzór nad dokumentacją licencyjną i nośnikami oprogramowania prowadzony był w sposób pozwalający na identyfikację posiadanego oprogramowania i ograniczenie dostępu osób nieuprawnionych. Rejestr oprogramowania prowadzony był w aplikacji S., rejestrach wewnętrznych poszczególnych referatów IT odpowiedzialnych za zakup i zarządzanie daną usługą i systemach do zarządzania uprawnieniami udostępnianymi przez producentów oprogramowania i wykazach oprogramowania instalowanego na stacjach roboczych zgodnie z przyjętą procedurą. Ponadto zasoby stanowiące wartości niematerialnoprawne ewidencjonowano w aplikacji Środki Trwałe.

(akta kontroli str. 8-11, 01_348-350, 354, 365)

Czterema głównymi producentami oprogramowania były M., O., A., P. Wartość oprogramowania posiadanego przez UMK wytworzonego przez te firmy stanowiła 45,7% wartości oprogramowania będącego własnością Urzędu.

(akta kontroli str. 348-350)

W Urzędzie wykorzystywano także 29 aplikacji, których autorami byli pracownicy UMK. Aplikacje te tworzone były w ramach zawartych umów o pracę. Kody źródłowe przechowywane były w repozytorium Urzędu.

(akta kontroli str. 22-23, 345-347)

W Urzędzie prowadzono analizy możliwego do wdrożenia tzw. wolnego oprogramowania. W ramach analizy rynkowej realizowanej w projekcie budowy platformy e-learningowej podjęto decyzję o wdrożeniu platformy M. W Procedurze D-07 określającej standardy oprogramowania instalowanego na urządzeniach komputerowych również dopuszczono korzystanie z tzw. wolnego oprogramowania.

(akta kontroli str. 17-18, 344)

Prowadzone w Urzędzie rejestry oprogramowania pozwalały na identyfikację liczby wykorzystywanych/wolnych licencji wraz z datą ich wygaśnięcia. Prowadzone rejestry były aktualne i kompletne. Pozwalały ustalić użytkowników danego oprogramowania oraz zawierały informacje o przeniesieniu licencji między stanowiskami Dyrektor Wydziału Kontroli Wewnętrznej i Ewidencji Mienia zwracał się również do dyrektorów komórek organizacyjnych o dokonanie przeglądu wartości niematerialnych i prawnych

pod kątem faktycznego użytkowania oraz aktualności, w szczególności czy autorskie prawo majątkowe lub licencja w dalszym ciągu obowiązuje.

(akta kontroli str. 8-11, 345-350, 354,365)

Urząd wykorzystywał do inwentaryzacji oprogramowania narzędzie typu inventory tool, które zakupiono w lipcu 2019 r. Wydatki związane z opłatami licencyjnymi za możliwość korzystania z tego oprogramowania wyniosły w okresie objętym kontrolą 201,0 tys. zł. Narzędzie to było jednak wykorzystywane w mniejszym zakresie niż zakładano (Zagadnienie szerzej opisane w sekcji stwierdzone nieprawidłowości). Ponadto sposób postępowania Urzędu związany z wykorzystaniem tego narzędzia nie był wystarczająco skuteczny dla ograniczenia użytkowania na stacjach roboczych nieautoryzowanego oprogramowania. Zagadnienie szerzej opisane w sekcji *stwierdzone nieprawidłowości.* Ponadto sposób postępowania Urzędu związany z wykorzystaniem tego narzędzia nie był wystarczająco skuteczny dla wyeliminowania/zminimalizowania/ograniczenia użytkowania na stacjach roboczych nieautoryzowanego oprogramowania. Zagadnienie szerzej opisane w sekcji *stwierdzone nieprawidłowości.*

(akta kontroli str. 12, 16, 148-164, 345-350)

7 września 2022 r. stwierdzono, że pięć komputerów Urzędu nie było nigdy skanowanych z wykorzystaniem narzędzia typu inventory tool. Kierownik Referatu ds. cyberbezpieczeństwa Systemu Informatycznego wyjaśnił, że do przeprowadzenia skanowania niezbędne jest włączenie urządzenia do sieci wewnętrznej Urzędu. Komputery te nie były włączane do sieci UMK z uwagi na przekazanie czterech z nich radom dzielnicy. Jeden komputer był komputerem szkoleniowym. Komputery te nie należały do sieci Urzędu.

(akta kontroli str. 148-164, 362-364, 366)

W toku kontroli zlecono biegłemu sporządzenie opinii, która obejmowała m.in. rzetelność, efektywność i funkcjonalność stosowanego narzędzia do monitorowania licencji. W opinii biegłego UMK posiada adekwatne oprogramowanie pozwalające na monitorowanie wykorzystania licencji zarówno dla środowiska stacji roboczych/laptopów, urządzeń mobilnych jak i serwerów.

(akta kontroli str. 148-164)

Biegły wskazał jednak na konieczność wzmocnienia wykorzystania oprogramowania do monitorowania środowisk mobilnych oraz na niewykonywanie cyklicznych przeglądów legalności oprogramowania zainstalowanego na służbowych telefonach komórkowych pracowników. Było to spowodowane trudnościami w instalacji takiego oprogramowania na służbowych telefonach. W trakcie kontroli NIK rozpoczęto akcję uświadamiającą pracowników o konieczności instalacji tego oprogramowania. W komunikacie w intranecie UMK poinformowano ich, że w przypadku nie przeprowadzenia instalacji do 15 września 2022 r. zostaną zgłoszone incydenty bezpieczeństwa informacji.

Zdaniem biegłego brak kompletnej i aktualnej wiedzy na temat posiadanego i wykorzystywanego oprogramowania i licencji w środowisku urządzeń mobilnych może prowadzić do naruszenia przepisów prawa. Niewykonywanie przeglądów może utrudniać lub uniemożliwiać skuteczne zarządzanie i nadzór nad licencjami. Biegły wskazał na ryzyko naruszeń warunków licencji lub naruszeń warunków własności intelektualnej. Wskazał że możliwe są skutki finansowe (np. konieczność wypłaty odszkodowania i poniesienia kosztów prawnych) oraz skutki niefinansowe (np. utrata reputacji).

(akta kontroli str. 125-136, 148-164, 355-356)

Urząd posiadał 1343 karty SIM przeznaczone do połączeń głosowych oraz 225 kart SIM przeznaczonych do transmisji danych. W grudniu 2022 r. Urząd zakupił za 157,3 tys. zł 1416 licencji narzędzia do zarządzania urządzeniami mobilnymi. W lutym 2022 r. poinformowano pracowników o konieczności jego instalacji.

(akta kontroli str. 161, 355-361, 367)

Dyrektor COI wyjaśnił, że proces rozpoznania i wyboru tego typu narzędzia, z uwagi na ogromne zróżnicowanie dotyczące funkcjonalności oraz cen istniejących rozwiązań, był bardzo złożony i długotrwały. Dyrektor COI wskazał, że po wyborze rozwiązania pozwalającego zabezpieczyć urządzenia mobilne oraz zarządzać nimi konieczne było pozyskanie środków finansowych oraz przeprowadzenie procedury zakupowej. Podkreślił on, że przed rozpoczęciem masowego wdrożenia konieczne było przeprowadzenie testów które umożliwiło przygotowanie i konfigurację całego środowiska po stronie serwerowej. Dopiero w kolejnym etapie wdrożenia rozpoczęto proces instalacji oprogramowania na urządzeniach użytkowników. Dyrektor COI wskazał, że proces instalacji obejmuje coraz większą liczbę urządzeń, niestety na części urządzeń nie można zainstalować oprogramowania bądź po jego zainstalowaniu urządzenie przestaje dać się używać ze względu na zbyt ograniczone zasoby. Dyrektor poinformował, że liczba urządzeń zarejestrowanych w usłudze wynosiła 6 października 2022 r. 895.

(akta kontroli str. 245-246, 355-361)

W toku kontroli zlecono biegłemu sporządzenie opinii, która obejmowała m.in. zakup licencji na oprogramowanie. W opinii biegłego wymagane jest wzmocnienie mechanizmu corocznego przeglądu posiadanych zasobów. Biegły zwrócił uwagę na wykorzystanie zakupionych w formie subskrypcji na:

- P. (spośród zakupionych 140 licencji wykorzystywano108),
- C. (spośród zakupionych 200 licencji wykorzystywano 87),
- S. (N. spośród zakupionych 500 wykorzystywano 275; S. spośród zakupionych 2500, wykorzystywano 1390; W. spośród zakupionych 100 wykorzystywano 51),

zakupionych w formie licencji wieczystej:

- D. (spośród zakupionych 264 instalacje a wykorzystano126,
- V. (wykorzystywano trzy licencje spośród 48 zakupionych). Zagadnienie szerzej opisane w sekcji *stwierdzone nieprawidłowości.*

(akta kontroli str. 148-164, 148-150)

Dyrektor COI wyjaśnił, że system B. został wdrożony w 2020 r. a na podstawie analizy wymagań liczbę licencji oszacowano na 125. Dyrektor COI wyjaśnił, że liczba wykorzystywanych licencji zmienia się w czasie, w zależności od przetwarzanych danych i generowanych raportów. Dyrektor COI poinformował, że liczba licencji dla B. została zwiększona 1 czerwca 2022 r. i że nie wszystkie licencje zostały do tej pory rozdysponowane. Odnośnie C. Dyrektor COI wyjaśnił, że 200 licencji jest minimalną ilością możliwą do zakupu. W zakresie W. Dyrektor wyjaśnił, że w okresie 2021/22 Urząd posiadał 50 licencji, z których wszystkie były używane, dlatego zdecydowano o zwiększeniu liczby licencji do kolejnego progu jaki ustalił producent. Dyrektor wyjaśnił, że S. jest modułem który zapewnia monitorowanie serwerów i aplikacji, w razie awarii 2500 licencji jest w pełni wykorzystywane, z uwagi na przygotowywane dedykowane opcje monitoringu.

Zwiększenie zapotrzebowanie na licencje D. Dyrektor COI wyjaśnił utworzeniem COI i zwiększenia liczby pracowników COI oraz obsługi winnych komórek organizacyjnych UMK. Dyrektor COI wskazał, że większa niż wykorzystywana liczba licencji jest konieczna w celu zapewnienia dostępność usługi.

W jednostce wdrożono mechanizmy służące przestrzeganiu zasad prawidłowego użytkowania oprogramowania oraz prowadzono audyty legalności oprogramowania.

(akta kontroli str. 239-245)

W okresie objętym kontrolą nie wystąpiły przypadki nałożenia ani zapłaty przez UMK kar z tytułu nieuprawnionego użytkowania oprogramowania.

(akta kontroli str. 35, 145-147, 341-343)

Przed zbyciem lub przekazaniem sprzętu do ponownego użycia licencjonowane produkty były usuwane, a uszkodzone nośniki były niszczone zgodnie z przyjętymi procedurami. W Urzędzie wprowadzono i stosowano instrukcję postępowania przy wykupie laptopów. W przypadku zbywania laptopów dyski twarde były formatowane oraz instalowano dostarczony pierwotnie z laptopem system operacyjny[10].

(akta kontroli str. 35, 348-350, 334-339, 353)

Stwierdzone nieprawidłowości

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

1. W Urzędzie nie przeprowadzano kontroli legalności oprogramowania w listopadzie 2021 r., grudniu 2021 r., styczniu 2022 r., lutym 2022 r., marcu 2022 r. oraz kwietniu 2022 r. co było niezgodne z §1 ust.1 lit a procedury przeglądu legalności oprogramowania. Procedura została wprowadzona zarządzeniem wewnętrznym nr 4/2021 Dyrektora Centrum Obsługi Informatycznej z dnia 1 marca 2021 r. Wskazano w niej, że praktyczną kontrolę legalności zainstalowanego oprogramowania poprzez identyfikację zainstalowanych aplikacji należy przeprowadzić u około 50 osób miesięcznie.

   (akta kontroli str. 51-52, 125-136, 148-164, 345-347)

   Dyrektor COI wyjaśnił, że w związku z wprowadzeniem stopni alarmowych Alfa-CRP, Bravo-CRP i Charlie-CRP oraz sytuacją na granicy z Białorusią podjęto decyzję o ograniczeniu operacji skanujących wewnątrz SI UMK, w celu sprawdzenia aktualnego stanu bezpieczeństwa systemów i ocenienia wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.

   (akta kontroli str. 250)

   NIK zwraca uwagę, że pierwszy stopień alarmowy ALFA-CRP dotyczący zagrożeń w cyberprzestrzeni został wprowadzony 15 lutego 2022 r., a kontroli legalności oprogramowania nie przeprowadzano już od listopada 2021 r., tj. trzy i pół miesiąca przed jego wprowadzeniem. Należy podkreślić, że po wznowieniu testowania liczba pozycji oprogramowania do usunięcia wzrosła z 11 przypadków na 176 badanych komputerów w październiku 2021 r. do 129 pakietów oprogramowania na stu badanych stacjach w maju 2022 r. Ponadto okres obowiązywania stopni alarmowych nie jest właściwym czasem na ograniczanie funkcjonowania mechanizmów kontrolnych dotyczących użytkowanego oprogramowania.

2. 7 września 2022 r. stwierdzono na komputerach w SI Urzędu kilkadziesiąt pozycji nieautoryzowanego (niedopuszczonego do użytku w UMK) oprogramowania.

   Narzędzie typu inventory tool wykryło obecność na komputerach Urzędu m.in. wielokrotnie wykrywanego podczas wcześniejszych skanowań c. oraz inne programy, takie jak m.in. F., W., G., F., M., S., W., C. Było to niezgodne z podrozdziałem 5.2.5 Zasad Zarządzania Bezpieczeństwem Informacji UMK, zgodnie z którym użytkownicy nie mogą instalować oraz uruchamiać żadnych

[10] Analizie poddano 5 spośród 40 sprzedanych urządzeń.

aplikacji, które nie zostały wcześniej formalnie dopuszczone do użytkowania, zgodnie ze standardem oprogramowania instalowanego na stacji roboczej w UMK opisanego w D-7.

(akta kontroli str. 125-136, 148-164, 345-350)

Dyrektor COI poinformował, że wykryte aplikacje zostały odinstalowane na komputerach podłączonych do sieci Urzędu. Osoby, które posiadały wykryte oprogramowanie na komputerach przenośnych zostały zobowiązane do zgłoszenia się do AT. Nie można było odinstalować zdalnie trzech aplikacji.
Jako przyczyny obecności nieautoryzowanego oprogramowania Dyrektor COI wskazał daleko posuniętą ingerencje systemu W. w zawartość komputera, który często przy aktualizacjach instaluje dodatkowe oprogramowanie. Dyrektor COI podkreślił, że często są to programy M., promujące w ten sposób swoje dodatkowe narzędzia lub gry. Podkreślił również, że najczęściej są to śmieciowe „darmówki".
Jako przyczynę wykrywania nieautoryzowanego oprogramowania Dyrektor COI wskazał również sposób deinstalacji oprogramowania w systemie W., który często pozostawia wpisy w rejestrze systemu lub resztki plików. Podkreślił, że ręczne usuwanie takich wpisów może spowodować uszkodzenie systemu operacyjnego.

(akta kontroli str. 246-249, 331-332)

3. 45 spośród 48 zakupionych licencji V. za kwotę 57,9 tys. zł nie było wykorzystywane, pomimo upływy prawie roku od ich nabycia (11 października 2021 r.), co było działaniem niegospodarnym.

(akta kontroli str. 307, 348-350)

Dyrektor COI wyjaśnił, że licencje V. zostały zakupione na potrzeby wykonywania schematów przez COI i inne komórki organizacyjne w październiku 2021 roku. Podkreślił, że licencje są wieczyste i będą wykorzystywane w zależności od zgłoszonych potrzeb. Dyrektor podkreślił, że nawet jeśli w chwili obecnej liczba instalacji jest mniejsza niż wynika z zakupionej liczby to spodziewa się zgłoszeń na bieżąco a dostępna pula (48 szt. na ponad 3 tyś użytkowników) jest minimalną rezerwą w celu zapewnienia dostępności do tego typu oprogramowania.

(akta kontroli str. 245)

OCENA CZĄSTKOWA

Urząd rzetelnie zorganizował proces postępowania z oprogramowaniem, jednak nie był on w pełni skuteczny. NIK negatywnie ocenia zaprzestanie prowadzenia kontroli legalności zainstalowanego oprogramowania w okresie od listopada 2021 r. do kwietnia 2022 r. Kontrola przeprowadzona w maju 2022 r. wykazała znaczny wzrost liczby nieautoryzowanych aplikacji zainstalowanych na stacjach roboczych pracowników. Wykryte w trakcie kontroli nieautoryzowane aplikacje zostały odinstalowane.
NIK ocenia pozytywnie przyjęte w UMK zasady zarządzania oprogramowaniem, ponieważ sprzyjały bieżącej, prawidłowej realizacji zadań publicznych. Obejmowały one kwestie związane z jego nabywaniem, wdrażaniem, użytkowaniem i bieżącym nadzorowaniem. Informacje o posiadanych licencjach i oprogramowaniu komputerowym były na bieżąco aktualizowane. W UMK używano programów pozwalających na monitorowanie instalacji licencji zarówno dla środowiska stacji roboczych/laptopów, urządzeń mobilnych jak i serwerów, jednak narzędzia te nie umożliwiały bieżącej analizy faktycznego wykorzystania zakupionych licencji.

NIK zwraca jednak uwagę, że z zakupionych w 2021 r. za kwotę 54,3 tys. zł licencji V. wykorzystywanych było tylko 6,3%.

OBSZAR

2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem.

Opis stanu faktycznego

Potrzeby UMK w zakresie nabywania i utrzymywania licencji komputerowych były określane na podstawie zgłoszeń zapotrzebowania składanych przez użytkowników składanych do COI. Komórki organizacyjne odpowiedzialne za obsługę określonego zadania, do którego realizacji niezbędne było dane oprogramowanie określały m.in. liczbę użytkowników oprogramowania oraz liczbę niezbędnych do zakupu licencji. Administratorzy Techniczni analizowali wykorzystanie posiadanego oprogramowania i w uzgodnieniu z Gospodarzem lub samodzielnie w zależności od posiadanych kompetencji określali liczbę niezbędnych licencji.

Na podstawie zgłoszonych zapotrzebowań COI opracowywało projekt budżetu. W przypadku zadań wieloletnich środki na realizację były planowane w ramach Wieloletniej Prognozy Finansowej. Plany budżetowe po uchwaleniu budżetu były aktualizowane w zakresie otrzymanych środków. Stosowano priorytetyzację zadań. Za zarządzanie planowaniem budżetowym oraz późniejszą realizacją wydatków odpowiadał Referat ds. Finansów i Kontrolingu IT. Na podstawie planów budżetowych powstawały plany zamówień publicznych, które podległy kwartalnym aktualizacjom. Zmiany w zakresie zadań budżetowych realizowane poza corocznym planowaniem budżetu były realizowane poprzez wnioski budżetowe składane przez członków zespołu zakupowego.

Analiza dziesięciu licencji zakupionych w okresie 2019-2022 wykazała, że liczba nabytych licencji była zgodna ze zgłoszonym zapotrzebowaniem komórek merytorycznych.

(akta kontroli str. 37, 348-350)

W Urzędzie prowadzono analizy możliwych do wdrożenia rozwiązań dotyczących oprogramowania. W Urzędzie wdrożenia dużych systemów realizowane były w oparciu o metodykę PRINCE2[11]. Dyrektor Magistratu podkreśliła, że stosowanie tej metodyki zapewnia lepszą kontrolę nad zarządzaniem zasobami, harmonogramem, zakresem, ryzykiem oraz pozostałymi parametrami projektu. Uruchomienie projektu poprzedzane było przygotowaniem dokumentacji inicjowania projektu, w ramach której przyszły Kierownik Projektu przygotowywał m.in. diagnozę potrzeb, analizę rozwiązań wraz z opisem produktu końcowego projektu z uwzględnieniem: opcji zaniechania, opcji minimum oraz opcji ponad minimum. W dokumencie tym wskazywano również uzasadnienie biznesowe oraz analizowano interesariuszy oraz struktury zespołu projektowego wraz z szacowaniem nakładu pracy. W razie konieczności prowadzono inne analizy zasadności realizacji projektu m.in. za pomocą analizy SWOT.

Zadanie zgłaszane do COI podlegały analizie przez Zespół Zarządzania Zmianą. Spotkania tego zespołu organizowano raz w tygodniu. W trakcie ich trwania omawiane były spływające z komórek organizacyjnych UMK wnioski i podejmowano decyzje o sposobie ich realizacji oraz koniecznym zaangażowaniu zasobów osobowych IT.

Analiza i weryfikacja zasobów aplikacyjnych oraz sprzętowych, prowadzona była w sposób ciągły przez administratorów aplikacji, serwerów oraz przez pracowników referatu ds. cyberbezpieczeństwa systemu informatycznego. Wykorzystywano do tego celu dedykowane narzędzia do monitorowania.

(akta kontroli str. 37-38, 348-350)

[11] Projects In Controlled Environments – Projekty w sterowanym środowisku.

Za adekwatność przydzielonych użytkownikom narzędzi informatycznych odpowiadali kierownicy komórek organizacyjnych UMK, którzy wnioskowali za pośrednictwem koordynatorów PBI o uruchomienie procesów nadania uprawnień do SI UMK niezbędnych do realizacji zakresu czynności danego pracownika. Odbywało się to w oparciu o procedurę D-01 *proces zarządzania upoważnieniami i uprawnieniami.*

Ponadto zgodnie z §38 Instrukcji określającej zasady ewidencjonowania składników mienia UMK Dyrektorzy wydziałów na potrzeby których dokonano nabycia wartości niematerialnych i prawnych zobowiązani są do corocznego przeglądu posiadanych stanów wartości niematerialnych i prawnych.

(akta kontroli str. 26-27, 345-350)

UMK nie posiadał automatycznego oprogramowania do analizy wykorzystania oprogramowania typu SaaS[12]. Administratorzy wykorzystywali do tego funkcjonalności administracyjne udostępnionych usług tam, gdzie były dostępne lub opracowywali własne narzędzia (dedykowane raporty, skrypty, zestawienia).

W wyniku analiz zmniejszono liczbę subskrypcji oprogramowania do wideokonferencji z 50 do 35 sztuk.

(akta kontroli str. 25-26, 345-347)

Urząd jako beneficjent realizował projekt finansowany ze środków Unii Europejskiej nr RPMP.02.01.04-12-0063/16-00-XVII/46/FE/16, w ramach którego zakupiono i wdrożono system Elektronicznego Centrum Obsługi Zintegrowanego Systemu Obsługi Zasobu stanowiący element całego projektu. Okres trwałości tego projektu liczony jest od 22 listopada 2021 r.

(akta kontroli str. 35)

W 2019 r. Urząd dokonał wydatków związanych z nabyciem i korzystaniem z oprogramowania komputerowego, w tym związanych m.in. z dostosowaniem lub zaktualizowaniem programów komputerowych, przedłużeniem umów licencyjnych, subskrypcją licencji, instruktażami i szkoleniami związanymi z nabytymi licencjami, opłatami za wsparcie i asysty techniczne w wysokości 17 560,8 tys. zł. W 2020 r. było to 21 360,3 tys. zł, w 2021 r. 25 165,1 tys. zł, a w pierwszym półroczu 2022 r. 9 117,9 tys. zł. Na oprogramowanie typu SaaS wydatkowano w 2019 r. 374,9 tys. zł, w 2020 r. 326,1 tys. zł, w 2021 r. 494,4 tys. zł, w pierwszym półroczu 2022 r. 134,7 tys. zł.

(akta kontroli 348-350)

W Urzędzie wykorzystywano Zintegrowany System Wspomagania Zarządzania Miastem O. (System). Został on zakupiony w 1993 r. W umowie zastrzeżono, że prawa autorskie pozostają przy Wykonawcy systemu.

(akta kontroli str.170-171, 385-306)

Zamówienia publiczne na asystę techniczną i konserwację aplikacji i modułów Systemu udzielane były w trybie zamówienia z wolnej ręki[13].

(akta kontroli str. 165)

Dyrektor Magistratu wyjaśniła, że w trakcie wieloletniej współpracy z Wykonawcą Systemu, prowadzone były rozmowy na temat możliwości pozyskania prawa do modyfikacji jego kodu źródłowego. Jednakże wykonawca informował, że polityka sprzedażowa firmy oraz ochrona know-how nie przewidują możliwości udostępnienia zamawiającym kodu źródłowego systemu.

(akta kontroli str. 176-179)

[12] Oprogramowanie jako usługa (Software as a Service, SaaS.

[13] OR-10.271.113.2018, OR-10.271.87.2020, OR-10.271.31.2021 oraz IT-03-2271.13.2022.

W 2019 r. sporządzono *koncepcję i szacunkową wycenę migracji modułów Systemu O. do modelu usługowego GMK*. Z analizy tej wynikało, że koszt całkowitej migracji modułów do modelu usługowego GMK wyniósłby w okresie 2020-2030 43 330 tys. zł, w tym nakłady inwestycyjne 30 002 tys. zł, a koszty utrzymania 13 328 tys. zł.

(akta kontroli str. 252-269)

W celu integracji z Systemem oprogramowania podmiotów trzecich w 2020 r. zrealizowany został projekt wdrożenia szyny danych w Systemie Informatycznym UMK w celu budowy infrastruktury technicznej pozwalającej na systemową integrację aplikacji zgodnie z architekturą opartą o usługi (SOA). W Urzędzie realizowany był program R., w ramach którego realizowano wymianę technologiczna Systemu na nowe wersje aplikacji działające zgodnie z architekturą usługową SOA. Pozwoli to w przyszłości na łatwiejszą niż do tej pory wymianę poszczególnych aplikacji na jej odpowiedniki pochodzące od niezależnych dostawców. W ramach tego programu planowane jest wdrożenie Platformy wirtualizacji danych, S. oraz wdrożono w Urzędzie jako podstawowego systemu wykonywania czynności kancelaryjnych E. (od stycznia 2022 r.).

W 2022 r. zakończony został projekt budowy Referencyjnej Bazy Osób Fizycznych i Prawnych i Centralnego Systemu Słowników, które są zintegrowane z Systemem poprzez szynę danych.

(akta kontroli str. 176-179, 348-350)

W ramach Systemu w UMK wykorzystywano 37 modułów i aplikacji Systemu. Aplikacje ewidencja działalności gospodarczych oraz ewidencja były aplikacjami archiwalnymi i Urząd nie ponosił kosztów związanych z ich funkcjonowaniem. Aplikacje i moduły Systemu były wykorzystywanie w pracy Urzędu. System nie generował jednak danych o logowaniach do generalnego rejestru informacji pracownika, jednolitego pliku kontrolnego oraz modułu integracyjnego. Zagadnienie szerzej opisane w sekcji *stwierdzone nieprawidłowości.*

(akta kontroli str. 170-171)

UMK wykorzystywał w swojej działalności również Zintegrowany System Zarządzania Oświatą. W 2020 r. zakupiono dwa nowe moduły tego systemu: portal pracowniczy oraz Hurtownię Danych/Business Intelligence. Zamówienia publicznego na te moduły udzielono w trybie przetargu nieograniczonego.

(akta kontroli str. 180)

Proces pozyskiwani licencji i oprogramowania uwzględniał ocenę pod względem bezpieczeństw i poufności danych. Zasady weryfikacji planowanego do nabycia oprogramowania określone zostały w procedurze D-6 *Procedura wdrażania nowych Aplikacji oraz nowych modułów lub funkcjonalności do istniejących Aplikacji*. Ponadto każde nowe oprogramowanie wdrażane w Urzędzie musiało być zgodne ze *Standardami usług teleinformatycznych w UMK*. Informacja na temat standardów była dołączana do opisu wymagań przygotowywanego przez Analityka IT. Zgodność ze standardami IT była weryfikowana w projektach umów wdrożenia nowych aplikacji i modyfikacji istniejących aplikacji oraz potwierdzana w trakcie procedur odbiorowych zgodnie z zapisami umów.

Weryfikacja oprogramowania w trakcie odbiorów odbywała się zgodnie z opracowanymi procedurami odbiorowymi opisanymi w umowach oraz zaprojektowanymi w trakcie realizacji umowy testami odbiorowymi w oparciu o zdefiniowane scenariusze akceptacyjne.

(akta kontroli str. 28-29, 345-350)

Zapisy w umowach uwzględniały aspekty bezpieczeństwa informacji i poufności danych. W UMK kupowane były licencjonowane dostępy do usług chmurowych. Referat ds. cyberbezpieczeństwa dokonywał oceny planowanego wdrożenia oprogramowania oraz wydawał rekomendacje do zaproponowanych rozwiązań. W razie wątpliwości co do postanowień umownych wykorzystywano analizy i opinie Zespołu Radców Prawnych UMK.

(akta kontroli str. 28, 125-136, 148-164)

W toku kontroli zlecono biegłemu sporządzenie opinii, która obejmowała m.in. ocenę nabywania i użytkowania SaaS. W opinii biegłego w tym obszarze nie zidentyfikowano nieprawidłowości i istotnych słabości.

(akta kontroli str. 148-164)

Stwierdzone nieprawidłowości

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

Zintegrowany System Wspomagania Zarządzania Miastem nie generował danych o logowaniach do: *generalnego rejestru informacji pracownika (GRIP), jednolitego pliku kontrolnego (JPK) oraz modułu integracyjnego (MINT)*. tym samym system ten nie posiadał atrybutu rozliczalności. Było to niezgodne z § 20 ust. 1 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[14], który nakłada na podmioty publiczne obowiązek wdrożenia i eksploatacje systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

(akta kontroli str. 170-171)

Dyrektor COI wyjaśnił, że Moduł MINT to konsola administracyjna, która jest rozwiązaniem dedykowanym dla administratorów szyny danych O., korzysta ona z własnego rozwiązania w zakresie uwierzytelniania użytkowników i w aktualnej wersji zapisuje datę ostatniego logowania użytkownika do systemu. System ten nie zapisuje pełnej historii logowań użytkowników. Odnośnie do modułu GRIP dyrektor COI wyjaśnił, że posiada on własne rozwiązanie w zakresie uwierzytelniania użytkowników na podstawie przydzielonych uprawnień w module KADRY i nie jest zintegrowany z mechanizmem rejestrowania zdarzeń logowania użytkownika. Potwierdził również, że moduł JPK w aktualnej wersji nie prowadzi rejestru logowań użytkowników i nie jest zintegrowany z ogólnym mechanizmem rejestrowania zdarzeń logowania użytkowników.

Dyrektor poinformował, że Trwają prace w zakresie modyfikacji modułów MINT oraz JPK mające na celu zapis i udostępnienie historii logowania użytkowników. Wskazał również, że wykonawca zadeklarował termin wdrożenia modyfikacji do 28 października 2022 r.

(akta kontroli str. 310-328, 331-333)

25 października 2022 r. Dyrektor COI poinformował o naprawie błędu dotyczącego braku zapisywania historii logowań użytkowników w aplikacji GRIP.

(akta kontroli str. 351-352)

OCENA CZĄSTKOWA

NIK ocenia pozytywnie określenie i stosowanie w Urzędzie zasad nabywania oprogramowania oraz działanie Zespołu Zarządzania Zmianą, który analizował

[14] Dz. U. z 2017 r., poz. 2247.

potrzeby UMK dotyczące licencji komputerowych. Zespół ten prowadził także analizy możliwych do wdrożenia rozwiązań pozwalających optymalnie wykorzystywać posiadane oprogramowanie.
W ocenie NIK Urząd podejmował na ogół skuteczne działania w celu optymalizacji wykorzystania oprogramowania, a środki publiczne związane z jego nabyciem i użytkowaniem były wydatkowane gospodarnie. NIK zwraca jednak uwagę, że trzy z wykorzystywanych przez Urząd modułów Zintegrowanego Systemu Wspomagania Zarządzania Miastem nie zapewniały pełnej rozliczalności użytkowników.

IV. Uwagi i wnioski

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

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

Wnioski

1. Uzupełnienie procedury weryfikacji legalności oprogramowania o wymóg potwierdzenia faktycznego usunięcia nieautoryzowanego oprogramowania.
2. Rozważenie wykorzystania *narzędzia dystrybucji aktualizacji oraz poprawek* do aktualizowania oprogramowania zainstalowanego na stacjach roboczych.

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 Krakowie. 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.

Kraków, października 2022 r.

Kontroler
Piotr del Fidali
Główny specjalista kontroli państwowej

.....
podpis