P. J. Bulz
15.11.2022 r.

07 LIS 2022

P. sekretarz
+
01+BK

URZĄD MIASTA RZESZOWA
WYDZIAŁ ORGANIZACYJNO-ADMINISTRACYJNY
Oddział Zarządzania Dokumentacją
DATA WPŁYWU 03. 11. 2022 *
Ldz. 186563 Podpis

NAJWYŻSZA IZBA KONTROLI
Delegatura w Rzeszowie

LRZ.410.020.02.2022

ODA-0.1710.8.2022

09. 11. 2022
01+ODA
P. o. wolno

Pan
Konrad Fijołek
Prezydent Miasta Rzeszowa
ul. Rynek 1
35-064 Rzeszów

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Rzeszowie
ul. Kraszewskiego 8, 35-016 Rzeszów
T +48 17 780 23 00, F +48 17 780 23 06
lrz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Rzeszowa[1], ul. Rynek 1, 35-064 Rzeszów.
Kierownik jednostki kontrolowanej	Konrad Fijołek, Prezydent Miasta Rzeszowa[2] - od czerwca 2021 r. (poprzednio: Tadeusz Ferenc).
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*[3].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Rzeszowie
Kontroler	Wojciech Kajzar, inspektor kontroli państwowej, upoważnienie do kontroli nr LRZ/112/2022 z dnia 15 lipca 2022 r. (akta kontroli: tom I, str. 2-5)

[1] Dalej: „Urząd" lub „Urząd Miasta".
[2] Dalej: „Prezydent" lub „Prezydent Miasta".
[3] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności.

OCENA OGÓLNA I JEJ UZASADNIENIE

W ocenie NIK kontrolowana jednostka posiadała zdolność do zarządzania licencjami i oprogramowaniem komputerowym w ograniczonym zakresie.

Przyjęte w Urzędzie regulacje uwzględniały uprawnienia, odpowiedzialność oraz obowiązki administratorów i użytkowników, a także ogólne zasady dotyczące postępowania z licencjami i oprogramowaniem, przy czym przepisy te nie obejmowały wszystkich kluczowych aspektów niezbędnych w procesie efektywnego i skutecznego zarządzania licencjami. Dodatkowo, pracowników Urzędu nie zapoznano z dokumentacją składającą się na System Zarządzania Bezpieczeństwem Informacji.

Pomimo posiadania przez Urząd narzędzi wspierających zarządzanie licencjami typu *Inventory tool*, (zapewniających skuteczne mechanizmy kontroli i bieżący nadzór nad instalowanym oprogramowaniem), nie zostały one w pełni zasilone danymi, co ograniczało kontrolę nad ogólnym stanem zasobów, ilością, rodzajem oraz datą wygaśnięcia terminowych licencji.

Negatywnie oceniono brak objęcia regularnym monitoringiem części pracujących urządzeń końcowych oraz oprogramowania instalowanego na urządzeniach mobilnych (telefony, tablety).

NIK ocenia pozytywnie działania podjęte przez Urząd polegające na analizie dostępnych na rynku alternatywnych rozwiązań dla dotychczas stosowanego oprogramowania.

Pozytywnie należy ocenić efekty prowadzonego przez Biuro Obsługi Informatycznej i Telekomunikacyjnej[5] monitoringu sieci pod kątem zgodności wykorzystywanego oprogramowania z warunkami licencji. Nie zidentyfikowano licencji specyficznych, które wymagałyby szczególnego monitorowania użycia.

Na pozytywną ocenę zasługują również działania podejmowane przez BOIT w zakresie dążenia do uzyskania zgodności użytkowanego oprogramowania z warunkami licencji w kontekście stwierdzenia przez biegłego istnienia oprogramowania, które nie powinno być zainstalowane na urządzeniach ze względu na brak wsparcia producenta oraz luki w bezpieczeństwie.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności.

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym

Opis stanu faktycznego

1.1

Obowiązujące w dniu wszczęcia kontroli przepisy wewnętrzne w zakresie zarządzania oprogramowaniem komputerowym oraz licencjami zostały ustanowione Zarządzeniem[7] nr 93/2021 Prezydenta Miasta Rzeszowa z dnia 5 listopada 2021 r., którym wprowadzono System Zarządzania Bezpieczeństwem Informacji dla Urzędu

---

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

[5] Dalej także: „BOIT" lub „Biuro" lub „OI".

[6] 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.

[7] Zarządzenie nr 93/2021 Prezydenta Miasta Rzeszowa z dnia 5 listopada 2021 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Miasta Rzeszowa.

Miasta Rzeszowa[8]. SZBI zastąpił poprzednio obowiązujące w tym zakresie zasady, tj: Politykę bezpieczeństwa informacji oraz Instrukcję zarządzania systemem informatycznym w Urzędzie Miasta Rzeszowa[9].
Przyjęte regulacje określały mechanizmy kontrolne w procesie zarządzania oprogramowaniem komputerowym oraz regulowały zasady nabywania i postępowania z licencjami w ramach przygotowania urządzeń do pracy. Ponadto SZBI uwzględniał ogólne obowiązki i uprawnienia administratorów i użytkowników w zakresie postępowania z oprogramowaniem. W ramach SZBI opracowano i wdrożono m.in.:

- Politykę ochrony danych osobowych Urzędu Miasta Rzeszowa (zał. nr 1 do SZBI),
- Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie (zał. nr 2),
- Regulamin korzystania z zasobów Informatycznych Urzędu (zał. nr 7),
- Zasady korzystania z Internetu i poczty elektronicznej Urzędu (zał. nr 8),
- Instrukcję nadawania, zawieszania i cofania (odbierania) upoważnień do przetwarzania danych osobowych oraz uprawnień do systemów informatycznych w Urzędzie (zał. nr 12),
- Aktywa informacyjne Urzędu (zał. nr 15).

(akta kontroli: tom I, str. 89-256)

W badanym okresie zadania z zakresu zarządzania oraz nadzoru nad zasobami informatycznymi (oprogramowaniem oraz licencjami komputerowymi) realizowało Biuro Obsługi Informatycznej i Telekomunikacyjnej, zgodnie z zapisami Regulaminu Organizacyjnego, wprowadzonego Zarządzeniem nr 19/2013 Prezydenta Miasta Rzeszowa z dnia 27 lutego 2013 r.[10]
Na podstawie § 24 ww. regulaminu do zadań Biura należało m.in.:

- opracowywanie oraz zlecanie opracowań programów komputerowych dla potrzeb Urzędu (pkt 4 regulaminu);
- prowadzenie ewidencji praw licencyjnych zakupionego oprogramowania oraz nadzór nad przestrzeganiem praw autorskich przez użytkowników systemów informatycznych w Urzędzie (pkt. 5);
- prowadzenie spraw związanych z zakupami sprzętu informatycznego i oprogramowania (pkt 8);
- prowadzenie ewidencji ilościowo-wartościowej środków trwałych, wartości niematerialnych i prawnych oraz zapasów magazynowych sprzętu komputerowego i telekomunikacyjnego z wykorzystaniem narzędzia informatycznego w postaci oprogramowania dziedzinowego użytkowanego przez Urząd (pkt. 9);
- prowadzenie szkoleń i udzielanie pomocy pracownikom w zakresie podstawowej obsługi sprzętu informatycznego i pracy z zainstalowanymi programami (pkt 10);
- opracowywanie Polityki Bezpieczeństwa Informacji oraz nadzór nad jej przestrzeganiem (pkt. 14);
- wdrażanie, doskonalenie oraz nadzór nad przestrzeganiem Systemu Zarządzania Bezpieczeństwem Informacji (pkt. 15);

---

[8] Dalej: „SZBI"
[9] Wprowadzone Zarządzeniem nr 7/2012 Prezydenta Miasta Rzeszowa z dnia 26 stycznia 2012 r.
[10] Zmienionego Zarządzeniem nr 47/2020 Prezydenta Miasta Rzeszowa z dnia 16 lipca 2020 r. Zmiany (w zakresie zadań BOIT) dotyczyły pkt 14-17 Regulaminu w związku z wdrożeniem przez Urząd Polityki Bezpieczeństwa Informacji.

– zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji (pkt. 17).

W Regulaminie określono odpowiedzialność BOIT w zakresie opracowania „*standardów w zakresie metod, narzędzi informatycznych i telekomunikacyjnych*", a więc też oprogramowania i prowadzenie ewidencji praw licencyjnych zakupionego oprogramowania oraz nadzoru nad przestrzeganiem praw autorskich przez użytkowników systemów informatycznych w Urzędzie.

Zgodnie z wewnętrznymi regulacjami w BOIT prowadzono rejestr[11] programów rozprowadzanych na zasadach darmowych i dopuszczonych do użytkowania w Urzędzie.

(akta kontroli: tom I, str. 16-27)

W ramach Regulaminu korzystania z zasobów informatycznych Urzędu Miasta Rzeszowa opracowano *Standardy oprogramowania dla stacji roboczych w Urzędzie Miasta Rzeszowa* określając zasady oraz dopuszczone do użytkowania w jednostce oprogramowanie.

(akta kontroli: tom II, str. 111-113)

W zakresie nabywania licencji/oprogramowania w Urzędzie obowiązywały ogólne zasady odnoszące się do prowadzenia zamówień publicznych uregulowane w Zarządzeniach Prezydenta Miasta Rzeszowa nr 91/2020[12] oraz nr 86/2020 (ze zm.)[13].

(akta kontroli: tom I, str. 6-13)

Kontrolowana jednostka ustanowiła procedury wewnętrzne określające odpowiedzialność oraz zasady zarządzania licencjami na oprogramowanie. W SZBI wskazano ponadto ogólne obowiązki i uprawnienia administratorów i użytkowników w zakresie postępowania z oprogramowaniem. Regulacje te nie obejmowały jednak wszystkich kluczowych aspektów niezbędnych w procesie efektywnego zarządzania licencjami, co zostało potwierdzone badaniami, które przeprowadził powołany przez Najwyższą Izbę Kontroli biegły z dziedziny audytu systemów informatycznych[14]. Więcej w sekcji: *stwierdzone nieprawidłowości.*

1.2

Pracownicy BOIT wykonywali zadania w obszarze zarządzania/administrowania licencjami/oprogramowaniem komputerowym zgodnie z ustalonymi pisemnie zakresami czynności. Analiza zakresów obowiązków 11 pracowników Biura wykazała, że pracownikom przypisano zadania polegające na pełnieniu funkcji administratorów dedykowanych systemów informatycznych, w tym w szczególności wyznaczonym osobom powierzono odpowiedzialność za:

– instalacje i konfiguracje oprogramowania systemowego (pkt II 1.5 zakresu czynności),
– konfigurację i administrowanie oprogramowaniem systemowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem (pkt II 1.6),

---

[11] O którym mowa w § 37 ust. 4 lit. b) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych w Urzędzie Miasta Rzeszowa. - Załącznik nr 2 do SZBI.

[12] Zarządzenie nr 91/2020 Prezydenta Miasta Rzeszowa z dnia 31 grudnia 2020 r. w sprawie ustalenia Regulaminu udzielania zamówień publicznych dla Urzędu Miasta Rzeszowa.

[13] Zarządzenie nr 86/2020 Prezydenta Miasta Rzeszowa z dnia 30 grudnia 2020 r. w sprawie wprowadzenia Regulaminu udzielania zamówień publicznych w Urzędzie Miasta Rzeszowa, których wartość nie przekracza 130 000 zł netto.

[14] Postanowieniem Dyrektora Delegatury NIK w Rzeszowie z dnia 30 sierpnia 2022 r.

- sporządzanie przynajmniej raz w roku inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania danych dla powierzonych systemów informatycznych (pkt II 1.12),
- przyznawanie na wniosek IOD ściśle określonych praw dostępu do informacji w danym systemie, a przynajmniej raz w roku sprawdzenie zgodności stanu uprawnień każdego z kont w powierzonym systemie informatycznym z prowadzonym przez IOD rejestrem udzielonych upoważnień do przetwarzania danych, a szczególnie danych osobowych. Dokumentowanie w odpowiednim protokole przeprowadzonych czynności kontrolnych (pkt II 1.14),
- zarządzanie licencjami powierzonych systemów informatycznych, procedurami ich dotyczącymi (pkt II 1.20).

W zależności od rodzaju oprogramowania funkcję administratora systemu powierzono jednemu lub dwóm pracownikom Biura.

(akta kontroli: tom I, str. 28-86)

Pracownicy Biura nie przechodzili specjalistycznych szkoleń w dziedzinie zarządzania licencjami komputerowymi. Ze złożonych wyjaśnień wynika, że część pracowników została przeszkolona w zakresie obsługi systemów pośrednio związanych z zarządzaniem oprogramowaniem: system Komadres (1 osoba), Active Directory (4 osoby), Service Desk Plus Helpdesk (2 osoby), Desktop Central (2 osoby), szkolenia online: z zarządzania pakietem biurowym (administratorzy systemu), Menage Engine w ramach asysty technicznej (3 osoby).

Prezydent wyjaśnił, że *przyjęta w Biurze praktyka wygląda tak, że przy zakupie i wdrażaniu systemów informatycznych na etapie ich wdrożenia, przewidziani do administracji danym systemem pracownicy OI uczestniczą przy pracach wykonywanych przez wykonawców. Jednocześnie nabywają wiedzę odnośnie działania danego systemu i nadzorują wykonawcę. Dodatkowo praktykowane są szkolenia przy zakończeniu wdrażania danego systemu w formie warsztatów dotyczących administracji wdrażanym systemem. Przy czym nie jest praktykowany wymóg uzyskiwania certyfikatów, dyplomów z odbytych szkoleń, gdyż nacisk kładziony jest na umiejętności praktyczne.*

(akta kontroli: tom II, str. 10-11)

Przyjęte w jednostce rozwiązania określały role, obowiązki oraz odpowiedzialność poszczególnych osób z zakresu administrowania konkretnym systemem, w tym zarządzaniem jego licencją (pkt II 1.20 analizowanych zakresów czynności).

W okresie objętym kontrolą zasoby kadrowe BOIT zasiliły: w 2019 r. 3 osoby, w 2020 r. 1 osoba, w 2021 r. 7 osób. W 2021 r. BOIT opuściła jedna osoba, z kolei w 2022 r. odnotowano odejście 5 osób.
Łącznie, na przestrzeni 2019-2022 zasoby kadrowe komórki OI zwiększyły się o 5 osób i wynosiły na dzień 30 czerwca 2022 r. 21 osób, w tym Dyrektor oraz Zastępca Dyrektora Biura. Nie odnotowano przestojów w czynnościach w obszarze zarządzania oprogramowaniem z uwagi na braki kadrowe.

(akta kontroli: tom II, str.122-123)

W latach 2019-2022 Urząd nie korzystał z outsourcingu usług w zakresie zarządzania zasobami informatycznymi. Zlecane na zewnątrz prace dotyczyły aktualizacji oraz opieki powdrożeniowej danego produktu/programu komputerowego.

(akta kontroli: tom II, str. 11)

1.3

W kontrolowanym okresie Urząd nie prowadził jednolitego spisu posiadanych licencji. Częściowe wykazy ujęto w rejestrze (prowadzonym w formie papierowej) oraz za pomocą programu Komadres, przy czym żadna z ewidencji nie była kompletna, co zostało potwierdzone w badaniu przeprowadzonym przez biegłego. W toku kontroli jednostka potwierdziła zdolność ustalenia stanu rzeczywistego - zidentyfikowała i zweryfikowała posiadane zasoby oraz przedłożyła jednolity wykaz (w formie papierowej) posiadanych licencji.

(akta kontroli: tom II, str. 243-248)

W procesie nadzoru nad licencjami Urząd wykorzystywał narzędzie *Manage Engine/Endpoint Central*[15], w którym na bieżąco zbierano dane odnośnie zainstalowanego oprogramowania w użytkowanych systemach komputerowych. W wyniku przeprowadzonego badania biegły stwierdził brak kompletności informacji w narzędziu wykorzystywanym do zarządzania i nadzoru nad wykorzystaniem licencji. Narzędzie *Manage Engine/Endpoint Central* umożliwiało monitorowanie zasobów pracujących pod kontrolą wszystkich używanych w Urzędzie systemów operacyjnych (Windows, MacOS oraz Linux).

Prezydent Miasta wyjaśnił, że wszyscy administratorzy mają dostęp do systemu zarządzania stacjami roboczymi (Desktop Central/ Unifield Endpoint Managment) oraz że *głównym zadaniem systemu jest usprawnienie zarządzania stacjami komputerowymi, automatyzacja zarządzania zasobami komputerowymi od konfiguracji systemów operacyjnych poprzez dystrybucję oprogramowania, czy też zdalne wsparcie użytkowników oraz inwentaryzację sprzętu i oprogramowania łącznie z zarządzaniem poprawkami bezpieczeństwa.*

(akta kontroli: tom II, str. 11, 129)

W dniu 30 września 2022 r. przeprowadzono oględziny wybranych 21 stacji roboczych[16] (zlokalizowanych w trzech różnych wydziałach Urzędu). W wyniku oględzin potwierdzono zdalny dostęp za pomocą oprogramowania *Manage Engine/Endpoint Central* do komputerów objętych badaniem. Ponadto wygenerowano raport (bieżący wykaz używanych programów na danej stacji roboczej) oraz potwierdzono fakt ich zainstalowania oraz zgodność z ewidencją systemową i rzeczywiste wykorzystywanie.

(akta kontroli: tom II, str. 135-137)

Jednostka przedłożyła listę czterech głównych producentów oprogramowania będącego na stanie Urzędu (biorąc pod uwagę wartość):

1. Microsoft Corporation reprezentowany przez Microsoft Sp. z o.o. – kwota 2 500 724,20 zł – oprogramowanie biurowe Office 365.
2. Ecol-Union Sp. z o.o. – kwota 1 594 603,96 zł – oprogramowanie Bumerang – zarządzanie retencją.
3. VULCAN sp. z o.o. – kwota 1 550 750,00 zł – pakiet oprogramowania zarządzania oświatą.
4. Integrated Solution Sp. z o.o. – kwota 762 721,72 zł – Podkarpacki System Informacji Przestrzennej.

---

[15] Oprogramowanie (typu *Inventory tool)* służące do zarządzania komputerami i urządzeniami przenośnymi, które pozwala zarządzać z jednego miejsca serwerami, laptopami, stacjami roboczymi, smartfonami i tabletami. Narzędzie to w pełni wspiera kompleksowe zarządzanie i nadzór nad licencjami w czasie rzeczywistym umożliwiając sprawdzenie liczby zainstalowanych programów oraz porównanie monitorowanych systemów z dostępną liczbą licencji.

[16] Użytkowanych na stanowiskach pracy zlokalizowanych w Wydziałach: Finansowym, Budżetowym oraz Księgowo-Rachunkowym Urzędu Miasta Rzeszowa.

oraz listę głównych producentów programów najczęściej wykorzystywanych w jednostce:

1. Microsoft Corporation reprezentowany przez Microsoft Sp. z o.o. – kwota 2 500 724,20 zł - oprogramowanie biurowe Office 365.
2. VULCAN sp. z o.o. – kwota 1 550 750,00 zł - pakiet oprogramowania zarządzania oświatą.
3. Integrated Solution Sp. z o.o. – kwota 762 721,72 zł - Podkarpacki system informacji przestrzennej.
4. COIG Centralny Ośrodek Informatyki Górnictwa S.A. – kwota 499 257,00 zł – pakiet oprogramowania KSAT 2000i.

(akta kontroli: tom II, str. 6-7)

Kontrolowana jednostka zakupiła oprogramowanie typu *Inventory tool - Manage Engine/Endpoint Central* w dniu 15 lutego 2018 r. Koszty nabycia wyniosły 128 273, 65 zł. Ze złożonych wyjaśnień wynika, że licencja na oprogramowanie odnawiana była corocznie, dotychczas poniesione na ten cel wydatki wyniosły 490 037,16 zł.

Prezydent wskazał, że *narzędzie wykorzystywane jest w trybie ciągłym, w pełnym zakresie, w celu realizacji obsługi stacji roboczych, w tym zgłoszeń technicznych, awarii oprogramowania i bieżącej kontroli aktualności licencji. Do wykonywania zbiorczych inwentaryzacji oprogramowania komputerów stacjonarnych Manage Engine/Endpoint Central wykorzystywany jest z końcem każdego roku.*

(akta kontroli: tom I, str. 263, tom II, str. 5-6)

W latach 2019-2021, w zaplanowanych odstępach czasu, prowadzono przeglądy oprogramowania za pomocą *Manage Engine/Endpoint Central*. Raporty (audyty) ze skanowania sieci zawierały listę zainstalowanych programów na poszczególnych urządzeniach końcowych objętych monitoringiem. Raporty te nie obejmowały wykorzystywanych w Urzędzie licencji ze środowisk wirtualnych, w tym nie obejmowały całości wykupionych dostępów do programów typu Saas. Z wyjaśnień Prezydenta wynika, że narzędzie *Inventory tool* nie obsługuje w pełni systemów chmurowych. W przypadku systemów chmurowych pracownicy OI wykorzystują moduły do zarządzania tym oprogramowaniem, dostarczone przez producentów (działające w ramach chmury).

Ponadto Prezydent wskazał, m.in. *że jeśli chodzi o oprogramowanie chmurowe, to w przypadku licencji, które nie wymagają instalacji, system Manage Engine/Endpoint Central nie posiada mechanizmów kontroli takich licencji a może stanowić jedynie elektroniczny rejestr zakupionych licencji i terminów jej ważności. Z tych powodów do tej pory system był wykorzystywany do kontroli ilości tylko instalowanego oprogramowania. Natomiast kontrola systemów chmurowych odbywa się w oparciu o rozwiązania zapewniane przez producentów oprogramowania. Planowana jest jednak optymalizacja procesu zarządzania oprogramowaniem i zdublowanie rejestru oprogramowania oprócz prowadzonego w formie tradycyjnej, papierowej, prowadzenia go również w postaci elektronicznej w systemie Manage Engine/Endpoint Central. Co mimo braku prawidłowej obsługi wszystkich typów licencji powinno usprawnić proces zarządzania licencjami w Urzędzie Miasta Rzeszowa.*

Prezydent wyjaśnił, m.in. że po analizie raportów skanowania odnotowano dużo oprogramowania w różnych wersjach. Dyrektor OI zalecił podległym pracownikom weryfikację zainstalowanego oprogramowania pod kątem adekwatności oraz aktualizację jak największej ilości programów do najnowszej wersji.

(akta kontroli: tom II, str. 11, 92, 130)

Funkcjonalność *Manage Engine/Endpoint Central* umożliwiała ustalenie oraz bieżącą kontrolę stanu oraz daty wygaśnięcia wszystkich wprowadzonych do programu terminowych licencji. Pozostające pod kontrolą systemu zasoby były monitorowane przez pracowników BOIT w sposób ciągły, w pozostałym zakresie z uwagi na brak możliwości automatycznej weryfikacji, monitorowanie licencji odbywało się w sposób manualny, przy czym brak pełnego zasilenia *Manage Engine/Endpoint Central* danymi uniemożliwiał skuteczne wykorzystanie narzędzia oraz nadzór nad zasobami licencyjnymi Urzędu.
Dostępy do oprogramowania przydzielano poszczególnym pracownikom za pośrednictwem środowiska teleinformatycznego Active Directory. Nie stwierdzono długotrwałych przestojów w aktywności użytkowników na stacjach roboczych poddanych sprawdzeniu. Z przekazanych przez Z-cę Dyrektora Biura wyjaśnień wynika, że sprawdzenia aktywności stacji roboczych są dokonywane za pomocą oprogramowania *Manage Engine/Endpoint Central*, w przypadku braku aktywności stacji roboczej powyżej 30 dni administratorzy dokonują wizji lokalnej w miejscu pracy stacji roboczej wyjaśniając przyczynę braku aktywności. Bieżące analizy wykorzystania oprogramowania są wykonywane poprzez robocze konsultacje administratorów systemów z użytkownikami tych systemów oraz dyrektorami równorzędnych komórek, w których te systemy pracują. Z powyższych analiz nie sporządzano dokumentacji w postaci raportów oraz notatek.

(akta kontroli: tom II, str. 121, 139-143)

W przebadanej próbie 10 wybranych programów zweryfikowano posiadanie przez jednostkę dowodów (legalności) nabycia licencji na ich użytkowanie. Klucze licencyjne zostały udostępnione administratorom poszczególnych systemów za pośrednictwem poczty elektronicznej Urzędu. Umowy licencyjne (wydruki umów) przechowywano w zabezpieczonych pomieszczeniach BOIT[17], w sposób zapewniający dostęp wyłącznie upoważnionych osób.

Prezydent wyjaśnił m.in., że *dane (klucze licencyjne) przechowywane na służbowych indywidualnych kontach pracowników IT są zabezpieczone mechanizmami uwierzytelniania Active Directory - hasłem oraz tzw. wielopoziomowym uwierzytelnianiem MFA[18].*

(akta kontroli: tom II, str. 141, 274-281)

W kontrolowanej jednostce nie zidentyfikowano programów komputerowych, których twórcami byli pracownicy Urzędu.

(akta kontroli: tom II, str. 123)

Funkcjonalność *Manage Engine/Endpoint Central* pozwalała na identyfikację oraz bieżącą kontrolę liczby aktualnie wykorzystywanych/wolnych licencji (w zakresie w jakim dane te zostały do systemu wprowadzone). Jednocześnie ze złożonych wyjaśnień Prezydenta wynika, że *Manage Engine/Endpoint Central* potrafi sprawdzić jedynie ilość instalacji sieciowych danego oprogramowania i porównać z ilością licencji wprowadzoną do systemu jako zakupione. Niniejsze rozwiązanie pozwala na prawidłową kontrolę tylko części oprogramowania, gdyż system pokazuje nieprawidłowości dla licencji jednoczesnych, dla których można instalować oprogramowanie na większej ilości stacji niż posiadanych licencji.
W wyniku przeprowadzonych badań nie stwierdzono braku instalacji nabywanych przez jednostkę programów.

(akta kontroli: tom II, str. 129)

---

[17] tj. w Rzeszowie przy ul. Króla Kazimierza 9.
[18] Multi Factor Authentication.

1.4

Szczegółowe zasady akceptowanego użycia zasobów służbowych IT zostały określone w Regulaminie korzystania z zasobów informatycznych Urzędu Miasta Rzeszowa[19].

Od pracowników nie odebrano oświadczeń o zapoznaniu się z ww. procedurami, określonymi w wewnętrznej procedurze SZBI, co szerzej opisano w sekcji *stwierdzone nieprawidłowości.*

W badanym okresie pracownicy BOIT corocznie przeprowadzali automatyczne (za pomocą skanowania sieci) przeglądy infrastruktury IT pod kątem zainstalowanego oprogramowania. Monitoring ten nie obejmował jednak całości zasobów. Pomimo posiadania odpowiednich mechanizmów nie była możliwa automatyczna weryfikacja, a część urządzeń monitorowano w sposób manualny.

Prezydent wyjaśnił, że wykaz urządzeń niemonitorowanych przez Manage Engine/Endpoint Central składa się głównie z urządzeń, które zostały wycofane z pracy produkcyjnej a także z urządzeń, które nie mają jeszcze zainstalowanego agenta Manage Engine/Endpoint Central.

(akta kontroli: tom II, str. 130)

Ponadto monitorowaniem nie objęto urządzeń mobilnych typu telefony oraz tablety. W wyniku badań biegły stwierdził, że Urząd posiada licencję na użytkowanie dedykowanego narzędzia FAMOC[20] służącego m.in. do zarządzania i monitorowania urządzeniami mobilnymi, zawierającego systemy klasy MDM (Mobile Device Menagement), którego nie wykorzystuje. W opinii biegłego kontrolowana jednostka posiadała skuteczne mechanizmy nadzoru, monitorowania instalowania i użycia oprogramowania na urządzeniach mobilnych w czasie rzeczywistym i w trybie ciągłym lecz z nich nie korzystała.

Prezydent wyjaśnił m.in. że *system FAMOC został dostarczony jako dodatkowa, czasowa usługa zewnętrzna i jest wykorzystywany do zabezpieczenia danych na służbowych telefonach pracowników w przypadku zagubienia czy kradzieży telefonu. Oprogramowanie to wykorzystywane jest także do wykonywania kopii kontaktów użytkowników przechowywyanych na służbowych telefonach.*

(akta kontroli: tom I, str. 130, 185-208)

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemu teleinformatycznego oraz wyeliminowania możliwości instalowania nieautoryzowanego oprogramowania pracownicy Urzędu Miasta nie mieli możliwości instalowania oprogramowania.

Prezydent wyjaśnił, że *wszelkie instalacje oprogramowania realizowane są przez pracowników OI. Mimo tego za pomocą systemu Manage Engine/Endpoint Central wykonywane jest automatyczne skanowanie systemów (na chwilę obecną bez telefonów i tabletów), również w zakresie zainstalowanego oprogramowania. Administratorzy na bieżąco sprawdzają jakie oprogramowanie zostało zainstalowane na stacjach roboczych.*

(akta kontroli: tom II, str. 21)

W badanej próbie nie stwierdzono wykorzystywania oprogramowania, dla którego licencje wygasły lub utraciły ważność.

(akta kontroli: tom II, str. 92-93, 141, 185-204, 249-259)

W badanym okresie nie odnotowano nałożenia na Urząd kar i grzywien w związku z nielegalnym lub nieprawnie użytkowanym oprogramowaniem. W badanej próbie

---

[19] Stanowiące załącznik nr 7 do SZBI.

[20] Oprogramowanie umożliwiające zdalne kontrolowanie, zarządzanie i zabezpieczanie różnorodnej infrastruktury mobilnej.

przekazanego przez Urząd sprzętu komputerowego nie wystąpiła konieczność usuwania danych z nośników pamięci. Analiza protokołów przekazania sprzętu IT (na rzecz szkół oraz uczniów) wykazała, że sprzęt nie był używany i został przekazany wraz z dyskami z zainstalowanym system operacyjnym na licencji OEM[21]. W związku z powyższym nie wystąpiła konieczność deinstalacji lub nadpisywania danych.

Prezydent wyjaśnił, że *praktyka w Urzędzie jest taka, że przed zbyciem/ przekazaniem sprzętu jest on sprawdzany przez pracowników OI, wszelkie nośniki danych są czyszczone za pomocą darmowych narzędzi dostępnych w Internecie lub fizycznie niszczone. W przypadku przekazania sprzętu po wyczyszczeniu nośników danych wykonywana jest reinstalacja systemu operacyjnego i tak przygotowany sprzęt jest przekazywany zgodnie z zarządzeniem nr 71/2010 Prezydenta Miasta Rzeszowa*[22]. W uzupełnieniu do powyższych wyjaśnień Z-ca Dyrektora Biura wskazał, że do bezpiecznego usuwania danych z dysków Urząd korzysta z darmowego oprogramowania Eraser. Skuteczność wykorzystywanego narzędzia potwierdzono poddając sprawdzeniu (za pomocą skanowania sieci) trzy przypadki deinstalacji wycofanego przez Urząd oprogramowania.

Biegły, po analizie ustanowionych w tym zakresie zasad stwierdził, że działania, które mogą determinować wycofanie licencji i odinstalowanie oprogramowania z urządzenia, były efektem realizacji procedury związanej z przygotowaniem komputera użytkownikowi, wycofania i likwidacji sprzętu z użycia lub w ramach procedury postępowania z dyskami twardymi. W ocenie biegłego zasady nie odnosiły się do postępowania w przypadkach takich jak upłynięcie terminu ważności dla licencji czasowych lub wycofanie licencji z użycia np. ze względu na brak wsparcia bezpieczeństwa i konieczności użycia właściwego dla danego oprogramowania narzędzia deinstalacji.

(akta kontroli: tom II, str. 22-86, 185-204, 271)

1.5

W badanej próbie (10 licencji) nie wystąpiły przypadki wykorzystania większej ilości instalacji niż możliwa. Biegły nie stwierdził również licencji specyficznych, które wymagałyby szczególnego monitorowania użycia. W zakresie zgodności użytkowanego oprogramowania z warunkami licencji nie stwierdzono nieprawidłowości.

(akta kontroli: tom I, str. 185-204)

Stwierdzone nieprawidłowości

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

1.

Obowiązujące w jednostce zasady nie ustanawiały istotnych mechanizmów kontrolnych, koniecznych do zapewnienia skutecznego i efektywnego zarządzania oprogramowaniem i licencjami. Regulacje te nie obejmowały następujących procedur (w odniesieniu do całego cyklu życia licencji i oprogramowania):

- zakresu koniecznej weryfikacji pod kątem wymagań bezpieczeństwa w ramach nabywania licencji,
- ustanowienia zasad przechowywania i zabezpieczania dostępu do nośników instalacyjnych, kluczy licencyjnych i innych dokumentów licencyjnych (w tym utrzymywanych w środowiskach chmurowych),

[21] Licencja przypisana do danego komputera.

[22] Z dnia 9 sierpnia 2010 r. w sprawie zasad i trybu likwidacji aktywów trwałych i druków ścisłego zarachowania oraz innych składników majątku w ewidencji ilościowej Urzędu Miasta Rzeszowa.

- ewidencjonowania wszystkich posiadanych i używanych licencji, w tym oprogramowania nabywanego w modelu Saas[23],
- dystrybucji i redystrybucji licencji,
- monitorowania (stanu użycia i legalności licencji) oraz zasad wykonywania cyklicznych przeglądów licencji (określenie cyklu, monitorowania poziomu wykorzystania i daty ważności - szczególnie w przypadkach czasowych subskrypcji, wymagany sposób i elementy raportowania),
- dokonywania przeglądów na wszystkich wykorzystywanych w jednostce kontrolowanej urządzeniach (serwery, stacje robocze, laptopy, smartfony/tablety) oraz objęcia szczególnym nadzorem hostów użytkowników posiadających uprawnienia administracyjne,
- dokonywania cyklicznego skanowania środowiska IT (stacje robocze, serwery, urządzenia mobilne) pod kątem identyfikacji nieautoryzowanego oprogramowania, a w przypadku jego identyfikacji przedstawiania w raportach pokontrolnych przyczyn takich sytuacji oraz (jeśli konieczne) wskazywania rekomendacji systemowych,
- dokonywania przeglądów lokalnych i serwerowych zasobów plikowych pod kątem przechowywania danych multimedialnych i innych plików, których przechowywanie prowadzi do naruszenia praw do własności intelektualnej oraz innych treści nielegalnych.

Brak ustanowienia w Urzędzie powyższych zasad potwierdził również biegły po przeprowadzeniu badań w jednostce.

(akta kontroli: tom II, str. 185-204)

Prezydent wyjaśnił, że wprowadzony zarządzeniem nr 93/2021 SZBI służy do regulacji spraw dotyczących ochrony danych zawartych w systemie informatycznym Urzędu, a także zasad użytkowania programów komputerowych i baz danych. SZBI określa m.in. procesy dotyczące zarządzania systemami i sieciami jak również pozyskiwanie, rozwój i utrzymanie systemów informatycznych.

(akta kontroli: tom I, str. 4)

2.

Pracowników Urzędu nie zapoznano z regulacjami wynikającymi z wprowadzonego w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji, w tym m.in. z następującymi zasadami i regulaminami:

- Regulaminem korzystania z zasobów informatycznych Urzędu Miasta Rzeszowa (zał. nr 7 do SZBI),
- Zasadami korzystania z Internetu oraz poczty elektronicznej Urzędu Miasta Rzeszowa (zał. nr 8 do SZBI),
- Regulaminem użytkowania urządzeń mobilnych w Urzędzie Miasta Rzeszowa (zał. nr 9 do SZBI).

Dyrektorzy poszczególnych komórek organizacyjnych Urzędu byli zobligowani przepisem § 2 zarządzenia nr 93/2021 Prezydenta Miasta Rzeszowa do zapoznania podległych pracowników z zasadami wynikającymi z SZBI oraz zapewnienia ich przestrzegania. Ponadto od pracowników nie odebrano oświadczeń (zgodnie z wzorem określonym w załączniku nr 13 do SZBI) o zapoznaniu się z ww. zarządzeniem w sprawie określenia Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Rzeszowa.

---

[23] SaaS - (ang. Software as a Service, SaaS) - oprogramowanie jako usługa.

Ze złożonych przez Prezydenta wyjaśnień wynika m.in., że załączniki do zarządzenia nr 93/2021 Prezydenta Miasta Rzeszowa są dostępne na portalu intranetowym QSystem. Ponadto wyjaśniono, że do czasu wdrożenia systemu Microsoft Office 365 postanowiono wstrzymać się z odebraniem oświadczeń od pracowników (załącznik nr 13 do SZBI), aby umożliwić ewentualne dostosowanie SZBI do wdrożenia systemu i wykorzystać jego mechanizmy do dystrybucji ww. oświadczeń drogą elektroniczną wraz z elektronicznym potwierdzeniem zapoznania się z jego zapisami. Prezydent wskazał, że w IV kwartale planuje się ewaluację zapisów SZBI oraz ich zmianę, uwzględniając wdrożone systemy informatyczne, przeprowadzenie szkoleń pracowników dotyczących zapisów SZBI oraz odebranie elektronicznych oświadczeń potwierdzających zapoznanie się pracowników z zapisami SZBI.

(akta kontroli: tom I, str. 89, tom II, str. 128-129)

3.

Nie przestrzegano procedury wewnętrznej określonej w Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania Danych Osobowych w Urzędzie Miasta Rzeszowa[24]. W § 37 pkt 4 ww. Instrukcji, wprowadzono wymóg stosowania *procedury akceptacyjnej dopuszczającej oprogramowanie rozprowadzane na zasadach darmowych*, jak również zdefiniowano sposób ich wprowadzania: *Oprogramowanie takie może być instalowane i wykorzystywane jedynie po wypełnieniu następujących warunków określonych jako procedura akceptacyjna:*

a) *analizie prawnej postanowień licencyjnych przeprowadzonej przez Biuro Obsługi Prawnej Urzędu;*
b) *zgłoszeniu zapotrzebowania na program do komórki IT i uzyskaniu akceptacji ASI, który dopuszcza program do użytkowania w Urzędzie.*

W wyniku czynności kontrolnych nie zidentyfikowano stosowania w Urzędzie ww. procedury, co potwierdziło również badanie przeprowadzone przez biegłego.

Prezydent wyjaśnił, że *zgodnie z przyjętą praktyką (dotyczy to jeszcze okresu sprzed SZBI), konsultacje powinny być zasięgane w sytuacjach, w których służby informatyczne miały wątpliwości co do interpretacji zapisów licencyjnych lub ich jednoznaczności wskazujących na uprawnienie do wykorzystania takiego oprogramowania. W ramach ewaluacji w IV kwartale 2022 r. planowana jest modyfikacja zapisów SZBI m.in. w powyższym zakresie, polegająca na doprecyzowaniu sytuacji, w których niezbędne jest sporządzenie opinii prawnej. Zmiana ma sprowadzić takie sytuacje tylko do wątpliwych a nie do wszystkich przypadków wykorzystania oprogramowania jak wyżej – ponieważ obecne zapisy zdają się sugerować nieodzowność takiej opinii we wszystkich przypadkach, co nie odpowiada intencjom twórców SZBI i stosowanych ogólnie dobrych praktyk.*

(akta kontroli: tom I, str. 163-164, tom II, str. 92)

4.

Urząd nie monitorował urządzeń mobilnych (telefony, tablety). Pomimo posiadania dedykowanego narzędzia FAMOC zawierającego system klasy MDM (Mobile Device Management) oraz podpięcia pod ten system służbowych smartfonów, nie objęto monitorowaniem oprogramowania instalowanego na tych urządzeniach.

Prezydent wyjaśnił, że *urządzenia mobilne typu smartfony i tablety były głównie wykorzystywane do prowadzenia rozmów głosowych oraz ewentualnego mobilnego dostępu do Internetu i nie były wykorzystywane do pracy z systemami teleinformatycznymi Urzędu, w związku z czym nie prowadzono inwentaryzacji*

[24] Określonej w Załączniku nr 2 do SZBI.

oprogramowania na tego typu urządzeniach. Ponadto Prezydent wyjaśnił, iż *obecnie trwają testy funkcjonalności modułu do zarządzania urządzeniami mobilnymi smartfonami i tabletami systemu Manage Engine/Endpoint Central, które powinny zakończyć się wdrożeniem rozwiązania w IV kwartale br. Testy mają na celu sprawdzenie funkcjonalności zarządzania w jednolitym narzędziu całością infrastruktury IT. Po zakończeniu testów modułu Manage Engine/Endpoint Central zostanie wykonana analiza porównawcza funkcjonalności systemu FAMOC (pracownik zostanie skierowany na dodatkowe szkolenie, aby w pełni zapoznał się z aktualnymi możliwościami systemu FAMOC). Jeśli w wyniku analizy porównawczej okaże się, że rozwiązanie Manage Engine/Endpoint Central posiada wszystkie potrzebne funkcjonalności do kompleksowego zarządzania urządzeniami mobilnymi to Urząd wypowie umowę na dostęp do oprogramowania FAMOC i będzie korzystał z jednego jednolitego narzędzia. W przypadku gdy w wyniku analizy porównawczej okaże się, że FAMOC posiada dodatkowe funkcjonalności, ponad te dostępne w Manage Engine/Endpoint Central i będą one pomocne w zarządzaniu urządzeniami mobilnymi, wówczas Urząd będzie korzystał z obydwu narzędzi jako wzajemnie się uzupełniających.*

(akta kontroli: tom II, str. 11, 130-131, 185-204)

5.

W wyniku badań przeprowadzonych przez biegłego ujawniono przypadki instalacji oprogramowania w wersji określonej jako EOL[25] (dot. oprogramowania TrueCrypt) czyli takiego, które zostało oficjalnie wycofane ze względu na luki w bezpieczeństwie. Zidentyfikowano również użycie programów np.: Total Commander zainstalowany na zbyt dużej liczbie stacji, Winrar. Ponadto wystąpiły przypadki braku aktualizacji serwerów (w tym poprawek krytycznych) oraz używania starych wersji aplikacji (bez najnowszych poprawek (np. Firefox). Biegły stwierdził również przypadki użycia aplikacji portable[26], a także brak zdefiniowania zasad blokowania na poziomie *Manage Engine/Endpoint Central.*

Prezydent wyjaśnił, że nadmierna ilość licencji (o trzy więcej niż zakupionych dla Total Commander oraz Winrar) wynikała z błędnych wskazań Manage Engine/Endpoint Central, gdyż system uwzględnił oprogramowanie już usunięte razem z agentem Endpoint Central, a nie zostało to automatycznie odwzorowane w systemie. Po wykonaniu synchronizacji statusu agentów Endpoint Central liczba licencji wskazywana przez system jest pokazywana prawidłowo. Ponadto wyjaśniono, że: *oprogramowanie TrueCrypt pozostało zainstalowane w celu zapewnienia odtworzenia nośników, które zostały zabezpieczone właśnie tym oprogramowaniem i w obecnej formie nie służy jako narzędzie zabezpieczania danych, a jedynie jako element odtworzenia zabezpieczonych wcześniej danych na nośnikach zewnętrznych (pendrive).* Prezydent wskazał, że w ostatnim czasie wdrożono system EDR – aktywnej ochrony przed cyberzagrożeniami – umożliwiający m.in. wykrywanie w czasie rzeczywistym wersji aplikacji komunikujących się poprzez sieć i dokonywanie weryfikacji podatności tych aplikacji, a także reagowania na wykryte w nich podatności przez odcięcie tej aplikacji od komunikacji internetowej. Oprogramowanie EDR umożliwia również blokowanie na bieżąco (w trybie on-line) instalacji aplikacji typu portable z nośników zewnętrznych.

---

[25] Oprogramowanie typu End of life – oprogramowanie, dla którego producent zakończył wsparcie techniczne.
[26] Oprogramowanie nie wymagające instalacji.

OCENA CZĄSTKOWA

W Urzędzie została opracowana dokumentacja składająca się na System Zarządzania Bezpieczeństwem Informacji, który określał mechanizmy kontrolne w procesie zarządzania oprogramowaniem komputerowym, w tym szczegółowe procedury i instrukcje. Kontrolowana jednostka wdrożyła regulacje, które wspierały nadzór nad oprogramowaniem i licencjami, przy czym zasady te nie obejmowały wszystkich kluczowych aspektów niezbędnych do efektywnego zarządzania tym procesem. Ustanowiony wewnętrzną procedurą przegląd użytkowanego oprogramowania był realizowany, jednak monitoring ten nie obejmował wszystkich pracujących urządzeń, w tym aplikacji instalowanych na służbowych telefonach i tabletach. Ponadto raporty (audyty) z przeglądów nie zawierały kryteriów oraz rekomendacji i ograniczały się jedynie do zinwentaryzowania zasobów danej stacji roboczej.

W Urzędzie nie stosowano wewnętrznej procedury akceptacyjnej dopuszczającej oprogramowanie rozprowadzane na zasadach darmowych oraz nie odebrano od pracowników oświadczeń potwierdzających zapoznanie się z ustanowionymi regułami SZBI. Prowadzone w jednostce spisy licencji nie były kompletne, co ograniczało kontrolę stanu zasobów. Należy jednak nadmienić, że w toku kontroli jednostka potwierdziła zdolność ustalenia stanu rzeczywistego weryfikując posiadane zasoby oraz przedkładając jednolity wykaz posiadanych licencji.

Nieefektywnie wykorzystywano posiadane narzędzia *Inventory tool* wspierające zarządzanie licencjami – oprogramowanie nie zostało w pełni zasilone danymi, a części pracujących urządzeń końcowych oraz aplikacji instalowanych na urządzeniach mobilnych nie monitorowano. Brak odpowiedniego korzystania z wszystkich funkcjonalności automatyzujących pracę dedykowanych narzędzi zapewniających bieżącą, kompletną i aktualną wiedzę na temat użytkowanego oprogramowania oraz stopnia wykorzystania licencji, znacznie ograniczało prowadzenie skutecznego nadzoru w całym cyklu życia licencji.

NIK pozytywnie ocenia korzystanie przez Urząd z udzielonych praw licencyjnych do użytkowanego oprogramowania. Pozytywna ocena dotyczy także skuteczności podejmowanych przez BOIT działań naprawczych w celu utrzymania zgodności oprogramowania z warunkami licencji. Ujawnione przez biegłego pojedyncze zdarzenia nadmiarowych instalacji zostały niezwłocznie wyjaśnione oraz doprowadzone do stanu zgodności. Nie ujawniono przypadków nabycia zbędnego oprogramowania, którego nie instalowano, jak również nie stwierdzono wykorzystywania oprogramowania, dla którego licencje wygasły lub utraciły ważność.

OBSZAR

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

2.1

Opis stanu faktycznego

Przyjmowaniem i analizą sygnalizowanych potrzeb w zakresie zakupu oraz instalacji oprogramowania zajmowali się pracownicy BOIT. Informacje w tym zakresie wpływały bezpośrednio od kierujących poszczególnymi komórkami Urzędu. Ponadto jednostka wykorzystywała platformę HelpDesk, gdzie poszczególni użytkownicy mieli możliwość indywidualnego zgłaszania potrzeb w zakresie instalacji, obsługi oraz aktualizacji oprogramowania. Jednostka nie prowadziła rejestru wpływających potrzeb, a realizacją zgłoszeń zajmowali się pracownicy BOIT na bieżąco.

Prezydent wyjaśnił, że *wnioski z zapotrzebowaniem na zakup licencji/oprogramowania składają Dyrektorzy/ Kierownicy wydziałów po dokonaniu uprzedniej analizy zasadności i celowości zakupu, po uzgodnieniu z bezpośrednimi*

przełożonymi (Prezydent, Zastępcy Prezydenta, Sekretarz) i uzyskaniu ich akceptacji do dalszego procedowania. Kolejno wnioski kierowane są do OI, gdzie dokonywana jest techniczna analiza zgłoszonego zapotrzebowania pod kątem dostępnych na rynku rozwiązań optymalnych dla stosowanej w Urzędzie infrastruktury teleinformatycznej wraz z dostępnymi sposobami licencjonowania, spełniającymi wymagania z wniosku. OI w porozumieniu z wnioskodawcą ustala optymalną potrzebną ilość licencji. OI dokonuje szacunku kosztów, a następnie konsultuje ze Skarbnikiem Miasta i jego służbami budżetowymi sposoby i możliwości sfinansowania zakupu.

(akta kontroli: tom II, str. 21)

Proces nabywania licencji/oprogramowania odbywał się zgodnie z ogólnymi zasadami w zakresie prowadzenia zamówień publicznych.

Ze złożonych wyjaśnień wynika, że *za każdym razem procedura zakupu była poprzedzona szczegółową analizą rynku, prowadzoną przez Dyrektora oraz Zastępcę Dyrektora BOIT, przy współudziale osoby, której planowane jest powierzenie roli administratora nowego systemu. Nadzór nad poprawną pracą systemu prowadzi jego administrator m.in. w oparciu o zgłoszenie użytkowników przez Help Desk. Jeżeli w trakcie pracy w systemie administrator dostrzega wyczerpywanie się limitu licencji – zgłasza to Dyrektorowi Biura, który po konsultacjach z Dyrektorem wydziału merytorycznego proponuje zakup dodatkowych licencji zgodnie ze ścieżką opisaną przy zakupie nowego oprogramowania/licencji.*

(akta kontroli: tom II, str. 4)

W latach 2019-2021 w Urzędzie kilkukrotnie zwiększano[27] planowane wydatki budżetowe przeznaczone na nabycie licencji/oprogramowania.

W złożonych wyjaśnieniach Prezydent miasta przyznał, że w okresie objętym kontrolą wydatkowano środki na licencje i oprogramowanie, które nie były pierwotnie planowane. Budżet zwiększono w 2019 r. (trzykrotnie) o kwoty: 36 900 zł, 11 500 zł, 70 000 zł; w 2020 r. o kwotę 220 000 zł; w 2021 r.(dwukrotnie) o kwoty: 1 500 000, zł, 950 000 zł. W powyższych kwotach zawierały się zwiększenia dotyczące nabycia oprogramowania: e-sesja, Moduł PIT-R Simple, System Zarządzania Treścią, Cisco Meeting Server, Desktop Central Endpoint, Security Addon, ADAudit, System aktywnych formularzy, Moduł Elektroniczne Archiwum Zakładowe, Pakiet oprogramowania biurowego Office 365 dla Urzędu Miasta, Chmura Azure.

Prezydent wyjaśnił m.in. że *w projekcie budżetu zabezpieczane są środki na zadania, na które zaciągnięte zostały zobowiązania finansowe, podpisane umowy i wszczęte procedury przetargowe oraz zadania przyjęte do realizacji. W planie finansowym nie tworzy się rezerw na pozostałe zakupy.* Ponadto wskazano, że *jeżeli sytuacja finansowa Miasta w trakcie roku budżetowego na to pozwala i zapadną decyzje o zakupie nowych licencji, wówczas zmienia się plan finansowy Biura poprzez zwiększenie środków na takie zadanie.*

W badanej próbie (10 zakupionych licencji) oprogramowanie zostało zainstalowane na stacjach roboczych pracowników i pozostawało w użyciu. Nie stwierdzono nabycia oprogramowania, którego Urząd nie wykorzystywał.

---

[27] Na podstawie uchwał Rady Miasta Rzeszowa: Nr XVII/328/2019 z dnia 27 sierpnia 2019 r., Nr XLII/870/2021 z dnia 26 stycznia 2021 r., Nr LII/1089/2021 z dnia 28 września 2021 r. oraz Zarządzeń Prezydenta Miasta Rzeszowa: Nr VIII/276/2019 z dnia 21 maja 2019 r., Nr VIII/463/2019 z dnia 30 września 2019 r., Nr VIII/917/2020 z dnia 31 lipca 2020 r.

W analizowanej próbie zakupionych przez Urząd 10 licencji nie stwierdzono rozbieżności pomiędzy liczbą deklarowanego zapotrzebowania w porównaniu z liczbą nabytych licencji.

(akta kontroli: tom II, str. 131-132, 143, 260-261)

2.2

Kontrolowana jednostka nie przedstawiła dowodów w zakresie prowadzenia pomiarów efektywności wykorzystywanych zasobów IT (oprogramowania). Ze złożonych wyjaśnień wynika, że prowadzono jedynie monitoring wskaźników wdrożenia usług w odniesieniu do oprogramowania Microsoft w ramach pakietu Microsoft Office 365 oraz statystyk poczty elektronicznej Urzędu.

W Urzędzie Miasta Rzeszowa wykorzystywano rozbudowane oprogramowanie wielomodułowe KSAT 2000i[28] (Producent: COIG S.A., oprogramowanie jest stosowane w Urzędzie od 2003 r.) oraz system OTAGO[29] (RATUSZ, użytkowany od 1994 r.) W okresie objętym kontrolą nie nabywano dodatkowych modułów dla ww. systemów, przy czym zawierano umowy na świadczenie usług związanych z obsługą serwisową, asystą techniczną i konserwacją systemów. Wartości usług zawartych w badanym okresie każdorazowo wynosiły poniżej progu 130 000 zł netto. Z zawartych umów[30] na dostawę ww. oprogramowania wynika, że Urząd nie jest w posiadaniu majątkowych praw autorskich do ww. programów w tym do kodu źródłowego. Ponadto Spółki ASSECO Data Systems S.A. oraz COIG S.A. nie wyrażają zgody na powierzenie innemu podmiotowi dokonywania jakichkolwiek modyfikacji systemu.
W ramach opracowania wniosku o przeprowadzenie zamówienia publicznego Urząd przeprowadził w 2022 r. analizę rynku pod kątem możliwości zastosowania alternatywnego rozwiązania polegającego na zakupie i wdrożeniu systemu porównywalnego do oprogramowania OTAGO (RATUSZ). Dokonana analiza doprowadziła do wniosku, iż zakup i wdrożenie alternatywnego rozwiązania dostępnego na rynku nie było (na dzień badania) dla Urzędu korzystne.

Prezydent wyjaśnił, że *do tej pory renegocjowane były koszty utrzymania obu systemów. Zakup odrębnych systemów spowodowany był posiadanymi specyficznymi funkcjonalnościami i możliwościami organizacji pracy w ramach struktury Urzędu. Każdy z nich miał lepiej przystosowane rozwiązania do specyfiki pracy wydziałów je wykorzystujących. Obie firmy, zdając sobie sprawę z wzajemnej konkurencyjności posiadanych rozwiązań, chcąc utrzymać bądź zastąpić swoim rozwiązaniem oprogramowanie konkurencji, stosowały politykę proponowania miastu skalkulowanych cen utrzymania/konserwacji własnego systemu. Ostatni okres przyniósł jednak skokowy wzrost kosztów usług w zakresie informatyki, co miało odzwierciedlenie w waloryzacji cen asysty technicznej oprogramowania, a szczególnie OTAGO. W konsekwencji - ze względu na pogarszającą się sytuację finansową Urzędu oraz rosnące wymagania związane ze zmianą przepisów prawnych powodujących konieczność zakupu nowych systemów lub dodatkowych funkcjonalności posiadanego oprogramowania, przeprowadzone zostanie szersze badanie rynkowe uwzględniające możliwości zakupu pełnej funkcjonalności jednego*

---

[28] Oprogramowanie KSAT2000i (Producent: Centralny Ośrodek Informatyki Górnictwa S.A. (COIG S.A.)), to zintegrowany system zarządzania dla jednostek samorządu terytorialnego, którego zadaniem jest wspomaganie całości procesów administracyjnych realizowanych w jednostkach samorządowych. System posiada strukturę modułową, którą można implementować do działania w danej jednostce w zależności od jej potrzeb.

[29] Oprogramowanie OTAGO (Producent: Asseco Data Systems S.A. - System OTAGO, dawniej System RATUSZ) to zintegrowany system wspomagania zarządzania miastem składający się z współpracujących ze sobą wielu aplikacji/modułów, które są konfigurowane w zintegrowany system przeznaczony dla jednostek administracji samorządowej, poszczególne moduły mogą również pracować niezależnie od siebie.

[30] Umowa z dnia 18 listopada 1994 r. na dostawę oprogramowania OTAGO oraz Umowa nr AE II 342/1/03 z dnia 3 lutego 2003 r. na dostawę oprogramowania KSAT 2000i.

z posiadanych systemów (OTAGO, KSAT) lub zakup nowego systemu umożliwiającego obsługę możliwie największej liczby wydziałów Urzędu z uwzględnieniem automatycznej wymiany danych pomiędzy systemami oraz modernizację zasobów serwerowych. W ramach tych działań odbyło się spotkanie z udziałem Prezydenta Miasta i dyrektorów Wydziałów użytkujących dotychczas oba systemy. W trakcie dyskusji potwierdzono konieczność wykonania pogłębionej analizy zaistniałej sytuacji i na tej podstawie dokonanie wyboru docelowego rozwiązania.

Z wyjaśnień złożonych przez Prezydenta wynika, że *nie dokonywano pełnej analizy funkcjonalności poszczególnych modułów. Równocześnie w systemie Helpdesk, tak jak dla innych systemów, użytkownicy zgłaszają problemy, które są rozwiązywane osobiście lub w konsultacji z serwerem producenta.*
Na podstawie rejestrów zgłoszeń w systemie Helpdesk potwierdzono zgłoszenia użytkowników dotyczące obsługi modułów działających w systemach KSAT2000i oraz Ratusz (OTAGO).
Prezydent wyjaśnił, że moduły są używane na bieżąco przez użytkowników i są wykorzystywane w zakresie funkcjonalności potrzebnych do pracy wydziałów oraz że użytkowane moduły zabezpieczają potrzeby korzystających z nich wydziałów. Ze względu na znaczący wzrost kosztów utrzymania systemów obserwowany zwłaszcza w bieżącym roku – szczególnie systemu OTAGO – w chwili obecnej planowana jest analiza dotycząca wyboru jednego zintegrowanego systemu z wbudowaną w ten system w pełni funkcjonalną szyną ESB[31].

(akta kontroli: tom II, str. 120, 142-143, 171-172, 205-235)

Przeprowadzone oględziny wybranych stacji roboczych Wydziału Finansowego (FN) potwierdziły korzystanie przez pracowników (po zalogowaniu do usługi Active Directory) z oprogramowania sieciowego KSAT 2000i[32] oraz z modułów oprogramowania OTAGO[33].

Koszty związane z utrzymaniem, obsługą serwisową i aktualizacją systemów KSAT 2000i oraz OTAGO wyniosły: system KSAT 2000i: 126 321,00 zł w 2019 r., 141 081,00 zł w 2020 r., 139 605,00 zł w 2021 r.; system OTAGO (odpowiednio): 99 184,04 zł; 101 704,04 zł; 152 350, 82 zł.

(akta kontroli: tom II, str. 125, 135-137)

W Urzędzie nie prowadzono analiz faktycznego wykorzystania oprogramowania typu Saas.

Prezydent wyjaśnił, że *dotychczas nie prowadzono analiz jak często osoby, którym przyznano dostęp do danego programu, faktycznie z niego korzystały. Obecnie trwają testy funkcjonalności Manage Engine/Endpoint Central, których celem jest sprawdzenie możliwości automatycznego wykrywania wykorzystania danego oprogramowania (ile razy dana aplikacja była używana otwierana i zamykana na wszystkich monitorowanych stacjach roboczych) oraz czasu użytkowania*

---

[31] (Ang. Enterprise Service Bus) – korporacyjna magistrala usług.
[32] Z wykorzystaniem modułu obsługi Podatków (POD), który umożliwia ewidencję i obsługę podatków i opłat lokalnych oraz modułu Gospodarka Odpadami (GOP), służącym do rejestracji, ewidencji i rozliczania deklaracji w zakresie gospodarowania odpadami komunalnymi, w ramach modułów wykorzystywano dodatkowe funkcjonalności programu: Centralna Kartoteka Kontrahentów (CKK), Egzekucja (EGZ), Księga Główna (KG), Repozytorium Systemu (RP), Należności i Zobowiązania (NZ).
[33] W Wydziałach Budżetowym oraz Księgowo-Rachunkowym potwierdzono dostęp oraz wykorzystanie modułów: FKORG – finansowo księgowy do obsługi urzędu jako organu, FKJB – do obsługi Urzędu jako jednostki budżetowej, EWYCIĄG – do obsługi wyciągów elektronicznych dla modułów FKJB i FKORG, PLZ – umożliwiający tworzenie planów, GRU – do obsługi rejestru umów, WPBUD – do obsługi dochodów niepodatkowych i opłat lokalnych w zakresie wymiaru i windykacji, WYBUD – do obsługi likwidatury.

oprogramowania (dotyczy informacji o długości używania aplikacji) pod kątem sprawdzenia wykorzystywania oprogramowania subskrypcyjnego instalowanego na stacjach roboczych.

W toku kontroli (przy pomocy narzędzia Endpoint Central) przeprowadzono badanie[34] porównując liczbę aktualnie zalogowanych użytkowników (wykorzystanych dostępów) z liczbą wykupionych dostępów. Nie stwierdzono przypadków przekroczenia liczby dostępów niż możliwa w ramach posiadanych licencji.

(akta kontroli: tom II, str. 121)

Prezydent wyjaśnił, że *kontrola adekwatności przyznanych dostępów jest realizowana na bieżąco oraz przebiega wieloetapowo. Głównym systemem autoryzacji jest usługa Active Directory, którego administratorzy na bieżąco sprawdzają aktywność użytkowników i przyznane im dostępy. Dyrektorzy komórek decydując o przyznawaniu i odbieraniu uprawnień do systemów informatycznych dla swoich pracowników dokonują analizy adekwatności przydzielania uprawnień. Zgłoszenia dotyczące uprawnień odbywają się za pomocą systemu Help Desk i są realizowane przez pracowników OI – administratorów systemów, którzy podczas realizacji zgłoszeń weryfikują logi systemów dziedzinowych we współpracy z IOD.*

(akta kontroli: tom II, str. 120-121)

W ramach 3 projektów finansowanych ze środków pochodzących z UE (których trwałość zakończyła się w okresie objętym kontrolą), zakupiono łącznie 18 programów komputerowych na licencji bezterminowej. Realizacje ww. projektów zakończyły się w 2015 r. Do 2020 r. (okres trwałości projektu) zakupione w ramach projektów oprogramowanie było użytkowane. Zgodnie ze złożonymi wyjaśnieniami, obecnie zaprzestano użytkowania ośmiu programów z uwagi na: zakończenie wsparcia przez producenta systemu i przeniesieniu funkcjonalności do innych (nowocześniejszych) systemów (w czterech przypadkach), wycofanie oprogramowania przez producenta i migracji do środowisk wirtualnych (dwa przypadki), zintegrowanie wykorzystywanego rozwiązania z obecnymi systemami Windows (dwa przypadki). W pozostałych dziesięciu przypadkach zakupione oprogramowanie jest nadal użytkowane.

(akta kontroli: tom II, str. 121-122, 132-134)

2.3

W badanych latach 2019-2022 Urząd ponosił wydatki związane z nabyciem i utrzymaniem oprogramowania komputerowego, w tym m.in. z dostosowaniem lub zaktualizowaniem programów komputerowych, przedłużeniem umów licencyjnych, subskrypcją licencji, instruktażami oraz szkoleniami i opłatami za wsparcie oraz asysty techniczne. Poniesione na te cele łączne wydatki w poszczególnych latach wyniosły: 1 798 480,29 zł w 2019 r., 5 123 309,17 zł w 2020 r., 5 201 166,12 zł w 2021 r., 1 875 147,34 zł do 30 czerwca 2022 r.

Dane odnośnie wydatków na oprogramowanie odpowiadały informacji o posiadanych zasobach ujętych w spisie prowadzonych licencji.

(akta kontroli: tom I, str. 124-125)

2.4

Nie zidentyfikowano przypadków użycia oprogramowania w modelu Saas niespełniającego wymagań w zakresie bezpieczeństwa, SLA[35] oraz zgodności z przepisami prawa. Biegły potwierdził, że proces nabywania oprogramowania typu Saas odbywał się zgodnie z ogólną procedurą zakupów, a wymagania

---

[34] Sprawdzeniu poddano próbę sześciu wykorzystywanych programów typu Saas.

[35] SLA (ang. Service Level Agreement) umowy dotyczące poziomu oraz warunków świadczonych usług w zakresie IT.

i oczekiwania kontrolowanej jednostki w zakresie SLA, bezpieczeństwa i zgodności z przepisami prawa były wskazywane w opisie przedmiotu zamówienia.

(akta kontroli: tom II, str. 22, 185-204)

2.5

Badanie przeprowadzone przez biegłego wykazało brak istnienia w Urzędzie mechanizmu kontrolnego zapewniającego, że w procesie pozyskiwania oprogramowania Saas uwzględnia się adekwatną weryfikację oraz ocenę dostawcy i oprogramowania. Biegły stwierdził, że ustanowione przez Urząd zasady związane z nabywaniem oprogramowania typu Saas, nie określały szczegółowych zadań i odpowiedzialności w zakresie:

- wiarygodności dostawcy, w tym pod kątem zapewnienia wsparcia technicznego i bezpieczeństwa,
- spełnienia wymagań bezpieczeństwa,
- dostępności umowy SLA i spełnienia oczekiwań kontrolowanej jednostki,
- spełnienia wymagań związanych z zarządzaniem danymi (śledzenie zmian na poziomie rekordów bazy danych, zapewnienia możliwości eksportu danych w popularnych formatach, zasady rozdzielania danych (multi-teanancy),
- zapewnienia szyfrowania data-in-transit w oparciu o bezpieczne protokoły i algorytmy,
- polityki kopii zapasowej, w tym częstotliwości wykonywania kopii i okresu retencji oraz przechowywania,
- spełnienia wymagań kontroli dostępu,
- spełnienia wymagań RODO (i innych wymagań wynikających z określonych przepisów prawa).

Prezydent wyjaśnił m.in., że *użytkowane w Urzędzie oprogramowanie Saas jest preferowane jako tzw. oprogramowanie typu COTS[36] gotowe i powszechnie używane na rynku pochodzące od renomowanych producentów, gwarantujących jego odpowiedni standard i wysoką jakość, zgodność z polskimi wymogami prawa, w tym KRI, RODO oraz ISO w zakresie bezpieczeństwa systemów informatycznych. Dotychczas mimo braku wewnętrznych regulacji w tym zakresie przy procedurze zakupu tego typu oprogramowania zawierane są w opisie przedmiotu zamówienia odpowiednie zapisy odnośnie wymagań zgodności z KRI, RODO oraz normami ISO.*

Ponadto Prezydent wyjaśnił, iż w związku ze wzrastającym udziałem rozwiązań typu Saas na rynku oprogramowania podczas planowanej ewaluacji zapisów systemu SZBI planowane jest wprowadzenie wewnętrznych regulacji obejmujących ww. zagadnienia.

(akta kontroli: tom II, str.143-144, 185-204)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Komórka BOIT prowadziła stały nadzór nad użytkowanym oprogramowaniem analizując na bieżąco zgłaszane potrzeby w zakresie instalacji oraz możliwych dostępów do oprogramowania. Nie zidentyfikowano prowadzenia pomiarów przydatności, w tym systematycznych analiz funkcjonalności oraz efektywności wykorzystania zasobów. Jednocześnie nie stwierdzono przypadków przekroczenia liczby dostępów niż możliwa w ramach posiadanych licencji Saas.

W Urzędzie nie wdrożono strategii (polityki), która określałaby plany zaspokojenia potrzeb jednostki w zakresie rozwoju zasobów związanych z oprogramowaniem. Budżet IT (wydatki na oprogramowanie), w każdym z badanych lat, był

[36] COTS (ang. Commercial of the shelf) komercyjne spółki.

niedoszacowany i nie uwzględniał wszystkich wydatków, w konsekwencji czego był wielokrotnie zwiększany. Decyzje w zakresie pozyskiwania i rozwijania infrastruktury podejmowano po analizie dostępnych na rynku rozwiązań, przy czym brak kompleksowej wiedzy w zakresie stopnia użycia i stanu posiadania utrudniał optymalne zaplanowanie wydatków.

Pomimo braku istnienia w Urzędzie mechanizmu kontrolnego zapewniającego, że w procesie pozyskiwania oprogramowania Saas uwzględnia się adekwatną weryfikację oraz ocenę dostawcy i oprogramowania, przeprowadzone przez biegłego badania potwierdziły zgodność z ogólną procedurą zakupów oraz że wymagania i oczekiwania kontrolowanej jednostki w zakresie SLA, bezpieczeństwa i zgodności z przepisami wskazywano w opisie przedmiotu zamówienia.

Pozytywnie należy ocenić podjęte przez Urząd działania polegające na analizie (opłacalności) dostępnych na rynku alternatywnych rozwiązań w zakresie możliwości zmiany dotychczas użytkowanego oprogramowania.

IV. Wnioski

Wnioski

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

1. Ustanowienie dodatkowych mechanizmów kontrolnych oraz uzupełnienie wewnętrznych procedur i zasad dotyczących zarządzania licencjami/oprogramowaniem komputerowym.
2. Zapoznanie pracowników (użytkowników) z regulacjami wynikającymi z przepisów określonych w SZBI Urzędu Miasta Rzeszowa.
3. Wdrożenie skutecznego nadzoru nad oprogramowaniem instalowanym na wszystkich pracujących w Urzędzie urządzeniach końcowych, przy efektywnym wykorzystaniu dostępnych narzędzi *Inventory tool*.
4. Modyfikacja wewnętrznej *procedury akceptacyjnej dopuszczającej oprogramowanie rozprowadzane na zasadach darmowych*, umożliwiająca jej stosowanie w praktyce.

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 Rzeszowie. 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 wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 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.

Rzeszów, dnia 28 października 2022 r.

Kontroler

Wojciech Kajzar
inspektor kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura w Rzeszowie
Dyrektor
Wiesław Motyka

.....
podpis