NAJWYŻSZA IZBA KONTROLI
Delegatura w Rzeszowie

LRZ.410.020.01.2022

Pan
Władysław Ortyl
Marszałek Województwa Podkarpackiego
ul. Łukasza Cieplińskiego 4
35 – 010 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 Marszałkowski Województwa Podkarpackiego w Rzeszowie, 35-010 Rzeszów ul. Łukasza Cieplińskiego 4 (dalej Urząd).
Kierownik jednostki kontrolowanej	Pan Władysław Ortyl – Marszałek Województwa Podkarpackiego, od 19.11.2018 r. (akta kontroli, t. I str. 1-2)
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 *o Najwyższej Izbie Kontroli*[1].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Rzeszowie
Kontroler	Wilhelm Dmytrów, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LRZ/115/2022 z 20.07.2022 r. (akta kontroli, t. I str. 3-4)

[1]Ustawa z dnia 23.12.1994 r. *o Najwyższej Izbie Kontroli* (Dz.U. z 2022 r. poz. 623).

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie określono ogólne zasady i procedury zarządzania oprogramowaniem komputerowym, dotyczące sprzętu, oprogramowania, sieci i rozwiązań usługowych. Zasady te dotyczyły zarządzania bezpieczeństwem systemów informatycznych i nie obejmowały procedur nabywania licencji na oprogramowanie, nadzoru nad używaniem oprogramowania, a także oceny jego zgodności z warunkami licencji.

Urząd nie posiadał kompletnej i aktualnej wiedzy na temat posiadanego oprogramowania, przez co w ograniczonym zakresie sprawował nadzór nad procesem jego instalowania i wykorzystywania. Wpływ na to miało m.in. nieobjęcie monitoringiem wszystkich urządzeń, brak systematycznych przeglądów (skanowania) urządzeń pod kątem zainstalowanych programów, brak pełnego wykazu licencji, nieprowadzenie ewidencji i niezarządzanie oprogramowaniem działającym pod kontrolą systemów MacOS oraz Android, niemonitorowanie w jakim zakresie posiadane oprogramowanie było wykorzystywane.

Urząd prawidłowo dokonywał wydatków związanych z nabywaniem i utrzymaniem oprogramowania. Wykorzystywano jedno oprogramowanie typu SaaS zakupione z licencją bez limitu stanowisk. W Urzędzie nie określono pisemnych zasad nabywania takiego oprogramowania wynikających ze specyfiki stosowania rozwiązań chmurowych.

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

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym.

Opis stanu faktycznego

1. W Urzędzie, zadania związane z odpowiedzialnością za zarządzanie oprogramowaniem komputerowym realizowane były w następujących komórkach utworzonych w ramach Departamentu Organizacyjno-Prawnego (dalej Departament):

a) sześć stanowisk w Biurze Obsługi Informatycznej, do których należy m.in.:
- realizowanie polityki bezpieczeństwa systemów i sieci informatycznych,
- zapewnienie sprawnego funkcjonowania systemów i programów informatycznych na serwerach,
- prowadzenie ewidencji baz danych zainstalowanych na serwerach,
- zapewnienie sprawnego funkcjonowania serwerowni oraz systemów i aplikacji zainstalowanych na serwerach,
- administrowanie sieciami administracyjnymi,
- wnioskowanie o przeprowadzenie zamówień dotyczących aktualizacji licencji i oprogramowania komputerowego;

b) sześć stanowisk w Oddziale do spraw utrzymania sprzętu teleinformatycznego (UST), do których m.in. należy:
- zapewnienie sprawnego funkcjonowania komputerów stacjonarnych i przenośnych oraz współpracujących z nimi urządzeń peryferyjnych,
- zapewnienie sprawnego funkcjonowania systemów i programów informatycznych na stacjach komputerowych,
- prowadzenie ewidencji baz danych zainstalowanych na stacjach komputerowych;

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

c) dwa stanowiska w Oddziale zarządzania mieniem ruchomym, do którego m.in. należy:
- prowadzenie ewidencji sprzętu informatycznego oraz licencji oprogramowania informatycznego,
- bieżące uzgadnianie stanu ewidencji wyposażenia ze stanem rzeczywistym.

Zasady zarządzania licencjami zawarto w dwóch następujących aktach wewnętrznych:
- instrukcji zarządzania bezpieczeństwem systemów teleinformatycznych[4] (dalej zarządzenie 74), oraz
- zasadach gospodarowania zbędnym mieniem ruchomym[5] (dalej zarządzenie nr 70).

Zgodnie z zapisami § 22 zarządzenia 74, każde nowe lub zmodernizowane urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek sposób wpływać na bezpieczeństwo przetwarzania informacji, musi zostać zweryfikowane na zgodność z wymaganiami bezpieczeństwa informacji obowiązującymi w Urzędzie przez właściwego w danym obszarze Administratora Systemu (dalej AS).

Procedury te były wykonywane wyłącznie w przypadku komputerów pracujących pod kontrolą systemu Windows i jedynie w momencie wydania nowego komputera. Departament nie zarządzał takimi zasobami sprzętowymi jak np. smartfony, tablety lub komputery pod kontrolą systemu MacOS, ani oprogramowaniem znajdującym się na tych zasobach.

Departament, zgodnie z § 2 zarządzenia 70, prowadzi bieżącą analizę stanu mienia ruchomego Urzędu z uwzględnieniem jego stanu technicznego oraz przydatności do dalszego użytkowania. BOI[6] natomiast odpowiada za techniczne aspekty zarządzania systemem IT, w tym zarządzania aktywami sprzętowymi, siecią i oprogramowaniem.

Postanowienia zarządzenia 74 miały ogólny charakter i nie określały szczegółowych zasad w zakresie instalowania, użytkowania i deinstalowania programów (zarządzanie cyklem życia oprogramowania). Postanowienia nie określały zasad nabywania licencji, sprawowania nadzoru nad działalnością związaną z posiadanym oprogramowaniem (licencjami) komputerowym, inwentaryzacji i przeglądów licencji, monitorowania (stanu użycia, ważności licencji).

Brak było dokumentów potwierdzających, kto jest odpowiedzialny za weryfikację umów licencyjnych i utrzymanie zgodności z przepisami praw autorskich i praw pokrewnych na wszystkich zasobach sprzętowych oraz monitorowanie urządzeń przenośnych.

W Urzędzie nie określono wymogu badania efektywności wykorzystywania licencji. Urząd nie badał efektywności wykorzystywania licencji.
Urząd nie dokonywał oceny w zakresie bezpieczeństwa wykorzystywanych lub wdrażanych aplikacji „darmowych" lub aplikacji dystrybuowanych w modelu „portable[7]".

---

[4] Wdrożonej w formie zarządzenia nr 74/2021 Marszałka Województwa Podkarpackiego z dnia 20.12.2021 r. w sprawie ustalenia Instrukcji zarządzania bezpieczeństwem systemów teleinformatycznych w Urzędzie Marszałkowskim Województwa Podkarpackiego w Rzeszowie, uchylającego zarządzenie nr 76/2019 Marszałka Województwa Podkarpackiego z dnia 25.10.2019 r. wydanego w tej samej sprawie.

[5] Wdrożonej w formie zarządzenia nr 70/2021 Marszałka Województwa Podkarpackiego z dnia 18.11.2021 r. w sprawie określenia zasad gospodarowania zbędnym mieniem ruchomym, będącym w posiadaniu Urzędu Marszałkowskiego Województwa Podkarpackiego, uchylającego zarządzenie nr 9/2012 Marszałka Województwa Podkarpackiego z dnia 31.01.2012 r. z późniejszymi zmianami (w tym z dni: 12.09.2019 r. i 24.02.2020 r.) wydanego w tej samej sprawie.

[6] Biuro Obsługi Informatycznej.

[7] To rodzaj programu, który nie wymaga instalacji, innymi słowy to program „przenośny". Wystarczy kliknąć ikonę programu i od razu się uruchamia.

Urząd nie posiadał narzędzia klasy UEM[8], MDM[9], czy też EMM[10], stanowiącym mechanizm nadzoru i zarządzania urządzeniami mobilnymi, w tym zarządzania ich oprogramowaniem w trybie ciągłym, stąd też nie generował raportu rozliczenia oprogramowania.

W Urzędzie nie było określonych odrębnych zasad nabywania licencji. Ich zakupy dokonywane były na podstawie przepisów[11] ustawy Prawo zamówień publicznych[12] przez Departament oraz przez Departament Społeczeństwa Informacyjnego (dalej SI).

Wprowadzone regulacje uwzględniają mechanizm kontrolny realizowany przez Departament zapewniający, że zapotrzebowanie na licencje jest weryfikowane i oceniane pod kątem zasadności/celowości wykorzystania oprogramowania, przy jednoczesnym uwzględnieniu możliwości finansowych. W przypadku zakupów licencji dokonywanych przez SI dopiero na etapie ich instalacji weryfikowane są np. zapisy licencyjne danej wersji, jej ograniczenia lub informacje zawarte w poszczególnych polach eksploatacji przez osoby odpowiedzialne za IT zatrudnione w Departamencie.

Oprogramowania i licencje jako wartości niematerialne i prawne ujmowane były w module środków trwałych w programie Komadres (nie było prowadzonego osobnego wykazu posiadanego i wykorzystywanego oprogramowania/licencji). System ten nie posiada możliwości monitorowania liczby wolnych/wykorzystanych licencji oraz nie zawiera informacji dotyczących daty wygaśnięcia licencji.

Ewidencja środków trwałych pozwala na podstawie ręcznego wprowadzenia numeru inwentarzowego jednostki sprzętu określić jego lokalizację, dane dotyczące zainstalowanego oprogramowania (ale nie dotyczy to urządzeń mobilnych i licencji wielostanowiskowych, obejmujących zbiór stacji roboczych, jak np. oprogramowanie antywirusowe, pakiety oprogramowania biurowego) oraz użytkownika.

W ocenie biegłego[13] w dziedzinie audytu systemów informatycznych (dalej Biegły), powyższe zasady zarządzania licencjami nie określały szczegółowych odpowiedzialności i zadań m.in. w zakresie:
- zasad (listy kontrolnej) nabywania, w tym weryfikacji pod kątem bezpieczeństwa oraz zasad wycofywania licencji,
- inwentaryzacji i przeglądów,
- monitorowania (stanu użycia i legalności licencji),
- działań naprawczych w przypadku wykrycia braku lub nieprawidłowego użycia licencji.

(akta kontroli, t. I str. 5-271, 335-339)

---

[8] Systemy MDM/EMM/UEM, czyli Mobile Device Management (tłum. z ang. - *oprogramowanie do zarządzania nad urządzeniami mobilnymi*)/Enterprise Mobile Management (tłum. z ang. - *zarządzanie urządzeniami przenośnymi*)/Unified Endpoint Management (tłum. z ang. – *zunifikowane zarządzanie punktami końcowymi*), to klasa narzędzi programowych, które umożliwiają konfigurację i zabezpieczenie niemal wszystkich urządzeń wykorzystywanych przez użytkowników.

[9] Jak wyżej.

[10] Jak wyżej.

[11] W tym zarządzeń Marszałka Województwa Podkarpackiego nr:

1) 41/2021 z dnia 17.06.2021 r. w sprawie ustalania zasad przygotowania i prowadzenia postępowań o udzielenie zamówień publicznych w Urzędzie Marszałkowskim Województwa Podkarpackiego w Rzeszowie oraz ustalenia Regulaminu pracy Komisji do przeprowadzenia postępowania o udzielenie zamówienia publicznego, uchylającego zarządzenie nr 30/2021 z dnia 12.05.2021 r. wydane w tej samej sprawie.

2) 35/2022 z dnia 05.05.2022 r. w sprawie określenia zasad udzielania w Urzędzie Marszałkowskim Województwa Podkarpackiego w Rzeszowie zamówień klasycznych o wartości poniżej 130 tys. zł, uchylającego zarządzenie nr 29/2021 z dnia 12.05.2021 r. wydane w tej samej sprawie.

[12] Ustawa z dnia 11.09.2019 r. *Prawo zamówień publicznych* (Dz. U. z 2022 r. poz. 1710, ze zm.).

[13] Powołanego w drodze Postanowienia wydanego w dniu 31.08.2022 r., w trybie art. 49 ust. 1 i 2 ustawy o NIK.

2. W Departamencie zatrudnionych było 14[14] osób, którym przydzielono do realizacji zadania dotyczące postępowania z oprogramowaniem komputerowym. W okresie objętym kontrolą na wymienionych stanowiskach nie było wakatu oraz nie było tzw. ruchu kadrowego (zwolnień/zatrudnień). W katalogu zadań, były m.in. następujące, spośród przydzielonych więcej niż jednej osobie:
- zapewnienie sprawnego funkcjonowania systemów i programów informatycznych na stacjach komputerowych (sześciu osobom),
- prowadzenie ewidencji baz danych zainstalowanych na stacjach komputerowych (sześciu osobom),
- opiniowanie pod względem merytorycznym wniosków o likwidację sprzętu komputerowego i oprogramowania informatycznego, będącego na wyposażeniu stanowisk pracy w Urzędzie (sześciu osobom),
- zapewnienie prawidłowego funkcjonowania systemów bazodanowych Urzędu (dwóm osobom).

Spośród zadań przydzielonych pojedynczym osobom były m.in. następujące:
- administracja systemem antywirusowym,
- administracja serwerami Active Directory,
- administracja serwerami dns[15], www, ftp[16],
- prowadzenie ewidencji sprzętu informatycznego oraz licencji oprogramowania informatycznego wykorzystywanego w Urzędzie.

Zakresy zadań i obowiązków pracowników Departamentu nie zawierały zadań w zakresie zarządzania oprogramowaniem:
a) monitorowanie faktycznego wykorzystywania / przydatności danego programu;
b) prowadzenie w zaplanowanych odstępach czasu przeglądów:
- stacji roboczych i udostępnionych udziałów sieciowych użytkowników pod kątem obecności nieautoryzowanego oprogramowania,
- urządzeń mobilnych (laptopy, tablety, smartfony) użytkowników pod kątem obecności nieautoryzowanego oprogramowania,
- środowisk wirtualnych, deweloperskich, testowych, szkoleniowych pod kątem obecności nieautoryzowanego oprogramowania,
- zgodności posiadanych i wykorzystywanych licencji z posiadanymi dowodami zakupu;
c) sporządzanie raportu rozliczenia oprogramowania.

W badanym okresie nie było szkoleń dla pracowników realizujących zadania w procesie zarządzania oprogramowaniem/licencjami. W latach poprzedzających kontrolowany okres pracownicy realizujący zadania w procesie zarządzania oprogramowaniem/licencjami, byli szkoleni m.in. w zakresie: MS-20744-Securing Windows Serwer 2016, MS 20345-1-Administering Microsoft Exchange Serwer 2016, F-Secure Administrator, „*Istotne zmiany w świetle krajowych i unijnych przepisów o ochronie danych osobowych - Rozporządzenie UE 2016/679 z 27 kwietnia 2016 roku*". Zastępca Dyrektora Departamentu podał m.in., że *nikt w Urzędzie nie zgłaszał potrzeb w kontrolowanym okresie, co do realizacji szkoleń wewnętrznych (bądź zewnętrznych)*.

[14] W tym: 6 pracowników BOI, 6 pracowników Oddziału do spraw utrzymania sprzętu teleinformatycznego oraz 2 pracowników Oddziału zarządzania mieniem ruchomym (utworzonym w dniu 17.06.2021 r. na mocy zarządzenia nr 39/2021 Marszałka Województwa Podkarpackiego).

[15] DNS, czyli Domain Name System, to system tłumaczący przeglądarkom nazwy adresów domenowych na adresy IP docelowych serwerów. Jeżeli przeglądarka odbierze tłumaczenie nazwy domenowej, to następuje połączenie i otwierana jest wskazana strona internetowa.

[16] Serwer FTP to serwer umożliwiający wymianę plików z komputerami za pomocą protokołu komunikacyjnego FTP (protokół transferu plików od ang. File Transfer Protocol – to protokół komunikacyjny typu klient-serwer, wykorzystujący protokół sterowania transmisją, umożliwiający dwukierunkowy transfer plików w układzie serwer FTP – klient FTP).

Zgodnie z zasadami zarządzania oprogramowaniem pracownicy Departamentu winni weryfikować zapisy licencyjne. Pracownicy Departamentu podali, że nie byli szkoleni z takiego zakresu, nie posiadają szczegółowych wytycznych, a ich weryfikacja jest pobieżna (weryfikacja strony internetowej licencjodawcy) i może być obarczona błędem.

W Departamencie, w procesie zarządzania oprogramowaniem nie był stosowany outsourcing[17] usług.

(akta kontroli, t. I str.272-330, 335-339)

3a-c i 3g. Posiadane i nabywane licencje ujmowane były w Departamencie w module środków trwałych prowadzonym w oprogramowaniu Komadres[18], natomiast narzędziem służącym do zbierania danych w sposób automatyczny z poszczególnych hostów wykorzystywany był program Lansweeper. Lansweeper nie umożliwiał zaczytania liczby licencji i oceny bieżącego ich wykorzystania, natomiast Komadres zawierał jedynie dane wprowadzone na podstawie dokumentów księgowych i nie umożliwiał weryfikacji ich wykorzystania.
Biegły stwierdził, że nawet próba manualnego porównywania bazy Komadres z bazą Lansweeper nie umożliwi kompletnej weryfikacji licencji, ponieważ w ramach bazy Komadres nie są wprowadzane np. programy na licencjach opensource, a baza Lansweeper nie jest kompletna, ponieważ nie jest wykorzystywany ten program do inwentaryzacji sprzętu i oprogramowania na zasobach sprzętowych pracujących pod kontrolą systemów innych niż Windows, pomimo posiadania funkcjonalności zaczytania danych z systemu MacOS oraz Android.
Agent Lansweepera nie został też zainstalowany na serwerach.

Zastępca Dyrektora Departamentu, w wyjaśnieniu będącym odpowiedzią na pytanie jakie dodatkowe warunki musi spełnić Urząd by zapewnić pełną i aktualną ewidencję wszystkich programów komputerowych, podał m.in. *stworzenie wyspecjalizowanego stanowiska pracy, przeszkolenie pracownika z zakresu zarządzania oprogramowaniem i licencjami, gromadzenie w jednej komórce wszelkiej dokumentacji dotyczącej praw do użytkowania zakupionego lub nabytego nieodpłatnie oprogramowania.*

W wyniku oględzin stwierdzono m.in. następujące przypadki:
- braku aktualizacji programów na hostach użytkowników (np. różne wersje przeglądarek, itp.),
- wykorzystywania na hostach rozwiązań cloud storage[19] (Xiaomi Cloud, Dropbox), które niosą zwiększone ryzyko naruszenia ochrony informacji, w tym danych osobowych,
- instalacji komunikatorów internetowych, które mogą posłużyć do nienamierzalnego (ze względu na szyfrowanie end-to-end) wyprowadzenia informacji (np. Signal[20], Telegram Desktop[21], Whatsapp),
- funkcjonowanie programów, które nie są już wykorzystywane w Urzędzie, zostały formalnie wycofane, a dotychczas są zainstalowane na hostach (e-audytor v3[22]),

[17] Skrót z ang. outside-resource-using, to wydzielenie ze struktury organizacyjnej przedsiębiorstwa niektórych realizowanych przez nie samodzielnie funkcji i przekazanie ich do wykonania innym podmiotom.

[18] System finansowo-księgowy funkcjonujący w Urzędzie od 2008 r., w którym prowadzona jest m.in. ewidencja środków trwałych.

[19] Cloud – chmura, obłok. Storage – przechowywanie, magazynowanie, zapamiętywanie. Microsoft Azure definiuje chmurę obliczeniową jako dostarczanie usług obliczeniowych (w tym serwerów, pamięci masowej, baz danych i oprogramowania) przez Internet.

[20] To otwartoźródłowa, niekomercyjna, szyfrowana aplikacja komunikacyjna dla systemów Android i iOS.

[21] To komunikator internetowy, który pozwala na wysyłanie wiadomości tekstowych, zdjęć, filmów oraz plików zapisanych w rozmaitych formatach (doc, zip, mp3, itp.), jak również umożliwia tworzenie grup składających się z 200 użytkowników.

[22] Aplikacja online do automatycznej analizy plików JPK (Jednolity Plik Kontrolny, to zestaw danych o operacjach gospodarczych firmy, dotyczący konkretnego okresu podatkowego).

- telefonów, które mimo zawartych tam informacji (w postaci np. danych osobowych, zdjęć z kontroli, poczty elektronicznej, plików chronionych, wysyłania backupu do zewnętrznego usługodawcy w chmurze) nie były zabezpieczone w jakikolwiek sposób (np. brak zabezpieczenia blokady ekranu po wybudzeniu),

Urząd posiadał 118 programów instalowanych na serwerach, w tym: 7 serwerów pocztowych, 28 serwerów obiegu dokumentów i zintegrowany FK OTAGO, 19 serwerów WWW, 4 serwery plików, 47 serwerów aplikacji, 9 serwerów baz danych i 4 serwery wydruku.
W wyniku oględzin stwierdzono przypadek braku aktualizacji serwerowych systemów operacyjnych (np. Windows 7 na serwerze monitorującym z zainstalowanym oprogramowaniem do monitorowania sieci – PRTG, Windows 2003 Server na serwerze VRCP, Ubuntu 14.0.4 LTS na serwerze Graylog, openSuse Leap 15.2 na serwerze PI-WWW).

(akta kontroli, t.I str. 174-191, 273-275, 323-393, 475-505 oraz t. II str. 1-18)

3d. W zbadanej próbie kontrolnej przypadków[23] odejścia pracowników z zajmowanego stanowiska (wskutek np. rozwiązania stosunku pracy, bądź przeniesienia na inne stanowisko), zwalniane oprogramowanie było przydzielane innym osobom.

(akta kontroli, t. I str. 394-411)

3e. Dla wybranej próby dziesięciu oprogramowań zróżnicowanych pod względem typu licencji, w każdym przypadku dostępne były dowody ich zakupu.

W wyniku oględzin miejsca przechowywania nośników/plików instalacyjnych, stwierdzono, że nośniki/pliki instalacyjne znajdowały się w pomieszczeniu biblioteki programów komputerowych Departamentu. Pomieszczenie jest zamykane na klucz, do którego dostęp ma dwoje pracowników Oddziału zarządzania mieniem ruchomym.

(akta kontroli, str. t. I 412-425, 433-434)

3f. Urząd posiadał łącznie trzy następujące programy, których autorami są dwaj pracownicy Urzędu:
- system informatyczny do obsługi Programu Rozwoju Obszarów Wiejskich 2014-2020,
- portal zamówień Regionalnego Programu Operacyjnego,
- Intranetowe serwisy Regionalnego Programu Operacyjnego.

Programy komputerowe były tworzone przez pracowników w ramach wykonywania obowiązków ze stosunku pracy[24].

(akta kontroli, t. I str. 426-432)

4a-c i e. Zarządzenie 74 w § 22 ust. 1 określa, że każde nowe lub zmodernizowane urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek sposób wpływać na bezpieczeństwo przetwarzania informacji musi zostać zweryfikowane na zgodność z wymaganiami bezpieczeństwa informacji obowiązującymi w Urzędzie przez właściwego w danym obszarze AS, gdzie wszelkie uchybienia AS zgłasza Kierownikowi BOI.
W Urzędzie nie było (nie określono) wypracowanych wymagań w zakresie dopuszczonego oprogramowania zarówno na komputerach jak i na urządzeniach mobilnych.

(akta kontroli, t. I str. 262-271, 323-330, 350-357 oraz t. II str. 49-186)

[23] Nie wystąpił przypadek likwidacji stanowiska pracy albo przestoju powyżej sześciu miesięcy.

[24] W badanym okresie Urząd nie zawierał umów cywilno-prawnych z tymi pracownikami oraz nie poniósł wydatków w związku z tworzeniem przez pracowników oprogramowań.

4d. Przypadki programów, które nie zostały wycofane z użycia, dla których licencje już wygasły przedstawiono w pkt 3a-c i 3g niniejszego wystąpienia pokontrolnego.

4f. W okresie objętym kontrolą Urząd nie ponosił kar w związku z nielegalnym lub nieprawnie użytkowanym oprogramowaniem.
Sprawdzanie legalności oprogramowania w Urzędzie nie było przedmiotem kontroli skarbowej ani producentów oprogramowań.

W zarządzeniu 74 § 28 ust. 4-5 uregulowano, że w przypadku trwałego przekazywania sprzętu komputerowego wraz z nośnikami danych typu dysk twardy lub dysk flash, dane na nich zawarte muszą być trwale usunięte za pomocą specjalistycznego narzędzia wykonującego operacje wielokrotnego zapisywania całego obszaru nośnika losowym ciągiem binarnym. Za usunięcie wszelkich danych przed przekazaniem sprzętu komputerowego podmiotom zewnętrznym odpowiada Oddział do spraw utrzymania sprzętu teleinformatycznego w Departamencie.

W badanym okresie, Urząd przekazywał jednostki sprzętu wraz z systemem operacyjnym podmiotom zewnętrznym (m.in. szkołom publicznym, ośrodkom kultury, Fundacji Pomocy Młodzieży, Stowarzyszeniu Peregrini w Leżajsku, Fundacji Aprobata, i innym). Stosowanie powyższej procedury dokumentowane było naklejoną etykietą na wycofywanych stacjach roboczych, zawierającą informacje o wykonanych czynnościach w zakresie usuwania oprogramowania, dacie wykonania operacji oraz podpisana była przez osobę dokonującą czynności.

(akta kontroli, t. I str. 350-357, 427-432, 435-448)

5. W wybranej próbie 10 zróżnicowanych rodzajowo umów licencyjnych (gdzie nie było licencji darmowej), nabytych w latach 2019 – 2021, stwierdzono, że liczba nabytych licencji odpowiadała liczbie zainstalowanych licencji. Próba obejmowała osiem licencji jednostanowiskowych, jedną licencję czterostanowiskową i jedną licencję siedmiostanowiskową.

(akta kontroli, t. I str. 332-334, 433-434)

Stwierdzone nieprawidłowości

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

1. Urząd nie zarządzał oprogramowaniem zainstalowanym na takich zasobach sprzętowych jak np. smartfony, tablety lub komputery pod kontrolą systemu MacOS.

Zastępca Dyrektora Departamentu wyjaśnił, że *Urząd w chwili obecnej nie dysponuje oprogramowaniem właściwym do zarządzania innymi niż Windows systemami operacyjnymi.*

(akta kontroli, t. I str. 5-271)

2. Urząd nie posiadał kompletnego wykazu licencji, którego prowadzenie należało do obowiązków Kierownika Oddziału zarządzania mieniem ruchomym.

Kierownik Oddziału zarządzania mieniem ruchomym wyjaśnił, że *po przyjęciu obowiązków kierownika oddziału zarządzania mieniem ruchomym kontynuowałem dotychczas stosowaną praktykę dotyczącą zarządzania licencjami. Prowadzona przeze mnie ewidencja środków trwałych zawiera również sprzęt informatyczny i licencje oprogramowania.*

(akta kontroli, t. I str. 273-275, 331)

3. Urząd nie planował i nie prowadził przeglądów oprogramowania i licencji mających na celu sporządzenie i aktualizację spisu oprogramowania, a także ocenę że posiada licencje na każde zainstalowane oprogramowanie. Urząd nie planował i nie prowadził przeglądów stacji roboczych i udostępnionych udziałów sieciowych użytkowników pod kątem obecności nieautoryzowanego oprogramowania.

Odnosząc się do przyczyn nieplanowania i nierealizowania przeglądów (skanowania) pod kątem obecności m.in. nieautoryzowanego oprogramowania, Zastępca Dyrektora Departamentu, podał, że przypadki niedozwolonego oprogramowania nie należą do częstych zjawisk, ponieważ użytkownicy komputerów są pozbawieni możliwości instalacyjnych i jedynie oprogramowanie typu portable mogłoby stanowić takie ryzyko. Jednak jest to zjawisko marginalne i nie odnotowano takiego incydentu w badanym okresie.

(akta kontroli, t. I str. 262-271, 323-330, 350-357)

4. W wyniku oględzin stwierdzono zainstalowaną wersję oprogramowania firmy Oracle Java w wersji wyższej niż 8u211 (update 331), na które Urząd nie posiadał licencji. To licencjonowanie przez firmę Oracle zostało zmienione, w efekcie przestała być darmową do użytku komercyjnego od 16.04.2019 r. (od wersji Oracle Java 8 SE o numerze 211 (8u211, 1.8.0_211-b12)).

Zastępca Dyrektora Departamentu wyjaśnił, że po zdiagnozowaniu problemu podjęto już szereg działań mających na celu poprawę sytuacji. Podjęto już działania mające na celu przegląd i aktualizację systemów operacyjnych (znaczna ich część już została zaktualizowana, a pozostałe zostały zaplanowane do aktualizacji) oraz podjęto decyzję o stworzeniu nowego stanowiska odpowiedzialnego całościowo za zarządzanie oprogramowaniem.

(akta kontroli, str. 174-191, 273-275, 323-357)

OCENA CZĄSTKOWA

Urząd w określił zadania dla komórek organizacyjnych, w procesie zarządzania bezpieczeństwem oprogramowania komputerowego. Zasady te w części obejmowały także zarządzanie oprogramowaniem. Nie określono procedur nabywania licencji na oprogramowanie, nadzoru nad używaniem oprogramowania, a także oceny jego zgodności z warunkami licencji.
W ocenie NIK brak kompletnego wykazu posiadanych licencji, a także niemonitorowanie faktycznie używanych programów, istotnie utrudniał skuteczne zarządzanie oprogramowaniem.

OBSZAR

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

Opis stanu faktycznego

1. W Urzędzie nie było dokumentacji planistycznej dotyczącej potrzeb w zakresie oprogramowania.
Zastępca Dyrektora Departamentu podał, że *wszelkie zapotrzebowania w zakresie oprogramowania powinny być zgłaszane do planu zamówień publicznych.*
W wyniku analizy planów zamówień publicznych nie stwierdzono zmian dotyczących oprogramowania komputerowego/licencji.
Zastępca Dyrektora Departamentu podał, że *plan zamówień publicznych nie był konfrontowany z rzeczywistym stanem zasobów. Decyzje dotyczące wydatków podejmowane były m.in. na podstawie wiedzy co do stanu posiadania oprogramowania w komórce zajmującej się jego zakupami (tj. Departamentu, czy SI).*

W wyniku badania planowania wydatków dotyczących nabycia oprogramowania/licencji, na podstawie wybranej próby 10 zróżnicowanych licencji nabytych w okresie objętym kontrolą stwierdzono, że liczba nabytych licencji odpowiadała liczbie licencji zgłoszonych w zapotrzebowaniach (tzw. liczbie niezbędnych licencji).

(akta kontroli, t. I str. 433-434, 449-453)

2a. W Urzędzie nie planowano pomiaru efektywności wykorzystywanych zasobów IT. Zastępca Dyrektora Departamentu podał, że *dotychczas nie zostały przyjęte miary, wskaźniki*.
Urząd nie dokonywał analiz efektywności posiadanego oprogramowania (jego faktycznego wykorzystania). Zastępca Dyrektora Departamentu podał, że w badanym okresie komórki organizacyjne nie zgłaszały problemów z zasadniczą funkcjonalnością danego oprogramowania oraz nie występowały długotrwałe przerwy w korzystaniu z oprogramowania.
W Urzędzie występował jeden zasadniczy zintegrowany system (modułowy) – Komadres, który posiadał moduły: finanse i księgowość, klienci – sprzedaż, ewidencja majątku, logistyka i pracownicy. Corocznie Urząd dokonywał zakupu tzw. usługi wsparcia eksploatacji systemu finansowo-księgowego Komadres w zakresie:
- dostosowania programów do zmieniających się przepisów polskiego prawa z wyłączeniem prawa miejscowego,
- udostępnianie modyfikacji systemu podnoszących jego jakość oraz zwiększających funkcjonalność wykorzystywaną przez klientów,
- udostępnianie nowych wersji systemu, oraz
- udzielanie konsultacji i wsparcia użytkownikom systemu.

W roku 2019, miesięczna opłata ryczałtowa wynosiła 6 250 zł netto, w roku 2021 ta sama opłata wynosiła 6 850 zł netto, natomiast w roku 2022 – 8 700 zł netto.
Urząd dokonywał zakupu w trybie zapytania ofertowego. We „wniosku o wyrażenie zgody na realizację zamówienia publicznego o wartości szacunkowej nieprzekraczającej równowartości 30 tys. euro" z lat 2019-2020, w cz. IV pt.: „Inne ważne informacje dotyczące zamówienia" podano m.in.: kontynuacja licencji z roku ubiegłego, jedyny oferent, jedna oferta.
Kierownik BOI w Departamencie podał m.in., że co roku w wyniku zapytania ofertowego wysyłanego do jedynego wykonawcy przedłużana jest umowa na usługi wsparcia eksploatacji systemu Komadres. Oferta cenowa jest podstawą do dokonania analizy kosztów przed dokonaniem zakupów. Komadres jest programem autorskim firmy Etob-Res i nikt poza nią nie ma praw autorskich do kodu programu.

W wyniku sprawdzenia (w dniu 10.10.2022 r.) faktycznego wykorzystania jego poszczególnych modułów, stwierdzono następujący rezultat: finanse i księgowość (UMWP) – 31 użytkowników, finanse i księgowość (ORGAN) – 9 użytkowników, kadry – 6 użytkowników, płace – 6 użytkowników, logistyka – 8 użytkowników, ewidencja majątku – 3 użytkowników, administrowanie aplikacją – 5 użytkowników.

Kierownik BOI podał, że od 2018 r. w Urzędzie jest wdrażane zintegrowane oprogramowanie OTAGO, przez firmę Asseco DS. z Gdańska, w ramach którego znajduje się również oprogramowanie finansowo-księgowe. Jego wdrożenie jest procesem bardzo skomplikowanym i czasochłonnym (co pokazuje jego dotychczasowy okres czterech lat) i przy takich wdrożeniach przynajmniej przez 12 miesięcy wymagana jest praca w dwóch systemach równocześnie. W związku z powyższym Urząd nie jest zainteresowany zakupem ewentualnego, kolejnego oprogramowania.
Zastępca Dyrektora Departamentu podał, że w roku 2017 zdecydowano o zastąpieniu programu Komadres, programem Otago, którego proces wdrażania rozpoczęty w roku 2018, trwa do chwili obecnej. Jest to typowo modułowy program (43 moduły) zintegrowany, do zarządzania całym przedsiębiorstwem.

(akta kontroli, t. I str. 358-393, 449-458)

2b. W Urzędzie było jedno oprogramowanie typu SaaS, tj. systemu informacji prawnej LEX wydawnictwa Wolters Kluwer, które zostało zakupione w wersji bez limitu stanowisk.

Zastępca Dyrektora Departamentu podał, że w związku z tym, że program został zakupiony bez limitu stanowisk, to nie wymagał *sprawdzania faktycznego wykorzystania oprogramowania*.

(akta kontroli, t. I str. 449-452)

2c. Urząd nie przedłożył dokumentów potwierdzających dokonywanie weryfikacji adekwatności przydzielonych użytkownikom narzędzi informatycznych (dostępu do odpowiednich programów komputerowych) pod kątem ich niezbędności do realizacji zadań. W wyjaśnieniu udzielonym w tej sprawie Zastępca Dyrektora Departamentu podał, że *Około 95% oprogramowań przydzielonych użytkownikom narzędzi informatycznych stanowią: system operacyjny + pakiet office i program antywirusowy, których przydatność nie podlega weryfikacji. Pozostałe programy były weryfikowane pod względem adekwatności.*

(akta kontroli, t. I str. 449-452)

2d. W Urzędzie było 16 programów finansowanych ze środków UE (z lat 2015-2017), których trwałość zakończyła się w okresie objętym kontrolą. W drodze ankiety telefonicznej przeprowadzonej z pracownikami zaangażowanymi w realizację RPO WP, na których stanowiskach zainstalowane są te oprogramowania (w tym licencje bezterminowe), stwierdzono, że są one na bieżąco wykorzystywane. W przypadku systemu LSI RPO WP 2014-2020, którego odpłatna obsługa wygasła 15.01.2021 r., zgodnie ze złożoną w postępowaniu o udzielenie zamówienia publicznego ofertą, utrzymywany jest przez dostawcę. Koniec usługi hostingu wynikający z umowy, przypada na dzień 15.01.2023 r. Obecnie system jest wykorzystywany w ramach perspektywy 2014-2020 m.in. do naborów, składania wniosków aplikacyjnych oraz do aktualizacji realizowanych zadań. Aplikacja jest nielicencjonowana, właścicielem kodów źródłowych jest zamawiający.

(akta kontroli, t. I str. 459-468)

3. W okresie objętym kontrolą Urząd poniósł następujące wydatki związane z nabyciem i korzystaniem z oprogramowania komputerowego:

a) w roku 2019 – 2 378 502,66 zł, w tym: oprogramowanie chmurowe – 86 807,02 zł, nabycie pozostałego oprogramowania (w tym licencje) bez subskrypcji – 1 580 201,28 zł, aktualizacja oprogramowania 192 337 zł, przedłużenie umów licencyjnych – 0,00 zł, subskrypcja licencji 59 392,56 zł, instruktaże oraz szkolenia związane z nabytymi licencjami – 2 500 zł, opłaty za wsparcie i asysty techniczne – 457 264,8 zł,

b) w roku 2020 – 4 167 017,46 zł, w tym oprogramowanie chmurowe – 132 105,16 zł, nabycie pozostałego oprogramowania (w tym licencje) bez subskrypcji – 2 136 052 zł, aktualizacja oprogramowania – 2 337 zł, przedłużenie umów licencyjnych – 25 295 zł, subskrypcja licencji 136 476,59 zł, instruktaże oraz szkolenia związane z nabytymi licencjami – 0,00 zł, opłaty za wsparcie i asysty techniczne – 1 734 751,71 zł,

c) w roku 2021 – 9 856 247,21 zł, w tym oprogramowanie chmurowe – 60 708,60 zł, nabycie pozostałego oprogramowania (w tym licencje) bez subskrypcji – 8 042 962,38 zł, aktualizacja oprogramowania 2 952 zł, przedłużenie umów licencyjnych – 0,00 zł, subskrypcja licencji 78 373,64 zł, instruktaże oraz szkolenia związane z nabytymi licencjami – 36 776,48 zł, opłaty za wsparcie i asysty techniczne – 1 634 474,11 zł,

d) w roku 2022 (I półrocze) – 2 692 645,15 zł., w tym oprogramowanie chmurowe – 11 136,80 zł, nabycie pozostałego oprogramowania (w tym licencje) bez subskrypcji – 1 422 000,90 zł, aktualizacja oprogramowania 1 180 zł, przedłużenie umów licencyjnych – 0,00 zł, subskrypcja licencji 12 868,75 zł, instruktaże oraz szkolenia związane z nabytymi licencjami – 0,00 zł, opłaty za wsparcie i asysty techniczne – 1 245 458,70 zł.

(akta kontroli, t. I str. 331, 469-474)

4-5. W Urzędzie nie określono pisemnych zasad nabywania i wykorzystywania oprogramowania w modelu SaaS. Brak było również dowodów potwierdzających, że w procesie pozyskiwania oprogramowania w modelu SaaS dokonywana jest ocena lub weryfikacja np.:
- wiarygodności dostawcy, w tym pod kątem zapewnienia wsparcia technicznego i bezpieczeństwa,
- spełnienia wymagań bezpieczeństwa,
- dostępności umowy SLA i spełnienia oczekiwań Urzędu,
- spełnienia wymagań związanych z zarządzaniem danymi (śledzenie zmian na poziomie rekordów bazy danych, zapewnienia możliwości eksportu danych w popularnych formatach, zasady rozdzielania danych (multi-tenancy),
- 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).
Urząd nie monitoruje w sposób ciągły, kto wykorzystuje lub rozpoczął wykorzystywanie rozwiązania w modelu SaaS.

Odnosząc się do powyższego Zastępca Dyrektora podał m.in., że:
- *weryfikacja była realizowana, ale jej wynik nie był dokumentowany. W Departamencie nie było przygotowanej check listy do tego zadania. Według Departamentu dokumentowanie takiej weryfikacji nie jest konieczne*,
- *wzór umowy w sprawie zakupu oprogramowania był weryfikowany pod względem dostępności SLA, a także korzystności dla Urzędu, co nie było udokumentowane. Niemniej warunki tego zakupu określone przez wydawnictwo Wolters Kluwer były korzystne (kupujący nie miał możliwości ich negocjowania, to tzw. umowa przystąpienia)*.

Wyjaśniając, czy Urząd dokonał weryfikacji projektu umowy i regulaminu m.in. sprawdzając czy określono maksymalny czas trwania okna serwisowego, czy zapewniono wcześniejsze powiadomienie w przypadku prac serwisowych, czy zapewniono procedurę obsługi zgłoszeń i błędów dotyczących aplikacji, czy określono maksymalny czas na obsłużenie zgłoszenia / rozwiązania problemu Zastępca Dyrektora podał m.in. *w naszym rozumieniu rzeczy, funkcjonalność aplikacji LEX nie wymaga definiowania warunków umownych, o których mowa w pytaniu*.

(akta kontroli t. I str. 174-191, 449-452 oraz t. II str. 19-48)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

W Urzędzie nie było zasad dotyczących nabywania i wykorzystywania oprogramowania w modelu SaaS. Departament nie dokumentował czynności dokonywanych w tym zakresie.
Zakupione licencje objęte kontrolą zostały nabyte zgodnie z zapotrzebowaniem i zainstalowane.
Wydatki związane z nabywaniem i utrzymaniem oprogramowania były dokonywane prawidłowo.

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli na podstawie art. 53 ust. 1 pkt. 5 ustawy o NIK, przedstawia następujące wnioski:
1. Utworzenie wykazu oprogramowania zawierającego kompletne i aktualne informacje o posiadanych i wykorzystywanych licencjach, stosowanego na wszystkich zasobach sprzętowych.
2. Podjęcie działań w celu objęcia nadzorem używanego oprogramowania na wszystkich posiadanych zasobach sprzętowych.
3. Podjęcie działań w celu prowadzenia systematycznych przeglądów używanego oprogramowania pod kątem zgodności z posiadanymi licencjami.
4. W stwierdzonym przypadku braku licencji - zapewnienie używania przez Urząd oprogramowania na podstawie licencji.

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 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.

Rzeszów, 9 listopada 2022 r.

Najwyższa Izba Kontroli
Delegatura w Rzeszowie

Kontroler
Wilhelm Dmytrów
Główny specjalista kontroli państwowej

/-/

Dyrektor
Wiesław Motyka

/-/