NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.017.03.2022

Pan
Roman Ciepiela
Prezydent Miasta Tarnowa
Urząd Miasta Tarnowa
ul. Mickiewicza 2
33-100 Tarnów

WYSTĄPIENIE POKONTROLNE

zmienione zgodnie z treścią uchwały Komisji Rozstrzygającej z 13 stycznia 2023 r.

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta Tarnowa, ul. Mickiewicza 2, 33-100 Tarnów (*Urząd*).
Kierownik jednostki kontrolowanej	Roman Ciepiela, Prezydent Miasta Tarnowa od 2 grudnia 2014 r.
Zakres przedmiotowy kontroli	1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym. 2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem.
Okres objęty kontrolą	Lata 2019-2022 do dnia zakończenia kontroli, z wykorzystaniem dowodów wytworzonych przed i po tym okresie, jeżeli miały one istotny wpływ dla ustaleń i ocen kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Krakowie
Kontroler	Mariusz Pindral, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/115/2022 z 26 lipca 2022 r. i nr LKR/148.2022 z 19 października 2022 r. (akta kontroli str. 1-4, 927)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

NIK negatywnie ocenia zarządzanie oprogramowaniem komputerowym w Urzędzie Miasta Tarnowa w latach 2019-2022[3].

Uzasadnienie oceny ogólnej

Urząd nie zapewnił wystarczających mechanizmów kontrolnych do sprawowania skutecznego nadzoru nad zarządzaniem licencjami na oprogramowanie. Brak było szczegółowych zasad zarządzania licencjami i monitorowania sposobu użytkowania posiadanego oprogramowania. Miało to istotny wpływ na efektywność użytkowania i poziom wykorzystania jego funkcjonalności.

W Urzędzie nie obejmowano kontrolą w czasie rzeczywistym czynności instalowania i wykorzystywania oprogramowania na smartfony i tablety oraz nie wprowadzono innych skutecznych mechanizmów kontrolnych w tym zakresie (np. okresowych przeglądów). NIK zauważa, że przyczyną części stwierdzonych nieprawidłowości mogła być niewystarczająca obsada kadrowa w Wydziale Informatyzacji Urzędu.

W ramach stosowanego narzędzia L.S. nie zapewniono kompletności danych dotyczących wszystkich posiadanych i wykorzystywanych licencji. Utrzymywano w nim archiwalne wpisy, nie gromadzono danych w trybie ciągłym i rzeczywistym z urządzeń przenośnych (smartfonów i tabletów) oraz części komputerów (20%). Nie identyfikowano programów typu portable, pomimo istniejącej funkcjonalności L.S. Świadczyło to o nieefektywnym wykorzystaniu narzędzia do monitorowania licencji. Tymczasem kontrola wykazała przypadki zainstalowania większej liczby programów, niż wynikająca z posiadanych licencji. Ze względu na niekompletność danych w L.S. Wydział Informatyzacji nie był w stanie wykonywać automatycznego i kompletnego porównania weryfikującego legalność posiadanego przez Urząd oprogramowania. Jednocześnie zaznaczyć należy, że nie przeprowadzano w inny sposób okresowych i kompleksowych audytów w wyżej opisanym zakresie.

NIK negatywnie ocenia sposób nabywania oprogramowania SaaS. Urząd nie wykazał, iż w procesie pozyskiwania oprogramowania w modelu SaaS dokonywana była rzetelna ocena i weryfikacja spełnienia określonych wymagań (w przypadku potencjalnych zakupów odnoszących się do przetwarzania danych osobowych), m.in. wiarygodności dostawcy, w tym pod kątem zapewnienia wsparcia technicznego i bezpieczeństwa, spełnienia wymagań bezpieczeństwa, dostępności umowy SLA, spełnienia wymagań związanych z zarządzaniem danymi, polityki kopii zapasowej, spełnienia wymagań kontroli dostępu, czy wymagań RODO i innych przepisów prawa. Zaznaczyć należy, że w Urzędzie nie określono szczegółowych zasad nabywania i wykorzystywania oprogramowania w modelu SaaS.

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

[3] Kontrola NIK obejmowała oprogramowanie użytkowane w Urzędzie Miasta Tarnowa, przy czym w ramach oprogramowania dziedzinowego jedynie system KSAT 2000 I.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[4] kontrolowanej działalności

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym

Opis stanu faktycznego

1.1. Zasady i procedury zarządzania oprogramowaniem komputerowym były określone w:

1) Regulaminie organizacyjnym[5], w którym Wydziałowi Informatyki przypisano m.in. zadania wdrażania, użytkowania i bieżącego nadzorowania wykorzystywanego oprogramowania komputerowego;

2) Regulaminie udzielania zamówień publicznych[6], w którym uregulowano m.in. kwestie zakupu oprogramowania;

3) Procedurze System Zarządzania Bezpieczeństwem Informacji według normy PN-ISO/IEC 27001:2013;

4) Procedurze ISO: Zarządzanie systemami IT w Urzędzie Miasta Tarnowa, w której uregulowano sprawy zarządzania oprogramowaniem:

- bezpieczeństwa,
- środowiskowym,
- aplikacje dziedzinowe (m.in. systemy finansowo-księgowe, kadrowo-płacowe, podatków, ewidencji ludności, CEPIK, Centralny Rejestr Umów, elektroniczny obieg dokumentów, itp.).

Oprogramowanie dziedzinowe uwzględnione było w omawianej procedurze ISO pod kątem obowiązków i realizowanych czynności przy wykorzystaniu tego oprogramowania (ujęcie funkcjonalne);

5) Procedurze ISO: Nadzór i aktualizacja oprogramowania oraz systemów komputerowych – dotycząca wszystkich wykorzystywanych programów i systemów informatycznych;

6) Procedurze ISO: Planowanie procesu zakupów oraz tworzenie zapisów w dokumentacji pozwalającej wybrać wykonawcę zdolnego do należytego wykonania zamówienia o wartości rynkowej równej lub wyższej od kwoty określonej w art. 2 ust. 1 pkt. 1 ustawy Prawo zamówień publicznych[7] – wykorzystywanej również do planowania i przeprowadzania zakupów oprogramowania;

7) Procedurze ISO: Zasady funkcjonowania platformy komunikacyjnej w ramach intranetu – regulującej sprawy dostępu, administrowania i publikowania informacji na platformie komunikacyjnej;

8) Procedurze ISO: Instrukcja określająca system haseł i uprawnień administratorów systemów komputerowych oraz zasady archiwizacji systemów komputerowych i baz danych – regulującej sprawy przydziału haseł, częstotliwości ich zmian, rejestrowania i wyrejestrowywania użytkowników, metodę i częstotliwość tworzenia kopii awaryjnych, sprawdzania obecności wirusów i sposób postępowania w tym zakresie, przechowywania nośników informacji, dokonywania przeglądów i konserwacji oprogramowania i zbioru danych, jak również zabezpieczenia zbiorów danych;

---

[4] 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.

[5] Zarządzenie Prezydenta Miasta nr 63/2002 z 25.11.2002 r. w sprawie nadania regulaminu organizacyjnego Urzędu Miasta Tarnowa z późn. zm.

[6] Zarządzenie Prezydenta Miasta Tarnowa nr 463/2017 z 17.10.2017 r. z późn. zm. oraz nr 9/2021 z 15.01.2021 r.

[7] Dz.U. z 2022 r., poz. 1710, dalej: pzp z 2019 r.

9) Instrukcjach pracy zdalnej oraz uruchamiania systemów dziedzinowych;

10) Instrukcji kontroli i serwisu stanowisk IT;

11) Instrukcji zakupu i instalacji pakietów oprogramowania typu Office;

12) Instrukcji czynności rejestracyjnych sesji Rady Miasta;

13) Instrukcji czynności zabezpieczających laptopy do pracy poza siecią Urzędu w ramach czynności kontroli zewnętrznej;

14) Instrukcji udostępniania stanowiska komputerowego do pracy zdalnej.

Ww. zarządzenia i procedury nie uległy zmianie od 2019 r. w zakresie dotyczącym zarządzania oprogramowaniem.

(akta kontroli str. 5-156, 280-291)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: zasady dotyczące nabywania oprogramowania uregulowane są w procedurach ogólnourzędowych. Urząd nie posiada jednej procedury dotyczącej wdrażania i użytkowania oprogramowania, ponieważ ze względów praktycznych byłoby to bardzo trudne do realizacji i nieefektywne z uwagi na różnorodność oprogramowania. Zasady dostawy, wdrożenia, licencjonowania jak również serwisu autorskiego uregulowane są na etapie prowadzonego postępowania o udzielenie zamówienia publicznego w specyfikacji istotnych warunków zamówienia, jak również w zawieranych późniejszych umowach (również dotyczących utrzymania oprogramowania). Kwestie związane z użytkowaniem oprogramowania są realizowane metodą szkoleń stanowiskowych i każde zakupione oprogramowanie dziedzinowe posiada dokumentację dla użytkownika i administratora. Tylko w zakresie pracy zdalnej stworzono w Urzędzie dodatkowe instrukcje obsługi oprogramowania, gdyż wymagało to logowania do VPN do sieci Urzędu. Urząd posiada natomiast odrębną procedurę dotyczącą nadzoru i aktualizacji oprogramowania oraz systemów komputerowych. Ponadto Urząd posiada umowy z dostawcami oprogramowania dziedzinowego dotyczące utrzymania aktualizacji produktu, obsługi sytuacji kryzysowych i utrzymania linii wsparcia. Role i odpowiedzialności przypisane są w zakresach obowiązków oraz wynikają z regulaminu organizacyjnego Urzędu.

(akta kontroli str. 920-923)

Zadania związane z obszarem zarządzania licencjami przypisane zostały Wydziałowi Informatyzacji, który zgodnie z Regulaminem Organizacyjnym odpowiadał za prowadzenie ewidencji oprogramowania użytkowego, z określeniem zakresu jego zastosowania i udzielonymi licencjami, jak również kontrolę legalności stosowanego oprogramowania. Zasady zarządzania oprogramowaniem zdefiniowano w załączniku nr 8 Polityki ochrony danych osobowych - „Instrukcja zarządzania systemem informatycznym". W dokumencie nie rozróżniano oprogramowania, na te, które są zainstalowane na komputerach czy też innych urządzeniach np. smartfonach i tabletach.

(akta kontroli str. 5-156, 280-291, 818-851)

W Urzędzie stworzono system dualnej odpowiedzialności i przypisanych ról, w którym od strony merytorycznej wszelkie wymagane przez RODO zgody i polecenia wydawał Administrator Danych Osobowych i Lokalni Administratorzy Danych Osobowych - LADO (najczęściej dyrektorzy odpowiednich wydziałów). Drugi pion stanowiła obsługa techniczna odpowiedzialna za czynności informatyczne, które nadzorował Administrator Systemów Informatycznych przy bezpośrednim udziale Lokalnego Administratora Systemu Informatycznego - LASI. Każdy System Informatyczny posiadał formalnie przypisanego Lokalnego Administratora Systemu

Informatycznego. Wykaz LADO i LASI prowadził Inspektor Ochrony Danych Osobowych.

(akta kontroli str. 47-48, 171-214)

Dowody zakupu oraz ewidencja zakupionego oprogramowania prowadzono w module środków trwałych systemu finansowo-księgowego KSAT 2000 I. Urząd prowadził dystrybucję i redystrybucję zakupionego oprogramowania dziedzinowego (liczba licencji określona była w SIWZ) za pomocą modułu majątek (ewidencja wartości niematerialnych i prawnych) systemu KSAT8. W przypadku oprogramowania Windows sprzęt oznaczony był etykietą producenta z kodem aktywacyjnym dla posiadanej licencji lub oznaczeniem wskazującym na posiadanie tego numeru w BIOS. W przypadku oprogramowania MS Office od wersji 2013 na komputerach przyklejana była etykieta z kodem kreskowym, do której przyporządkowany był klucz aktywacyjny. Oprogramowanie dziedzinowe inwentaryzowane było na podstawie dokumentów zakupu i kodów kreskowych naklejonych na folie kontrolne we właściwych pomieszczeniach serwerowych. Sprawy związane z oprogramowaniem do zarządzania bezpieczeństwem informacji i siecią Urzędu uregulowane były w procedurze System Zarządzania Bezpieczeństwem Informacji według norm PN-ISO/IEC 27001:2013. Monitorowanie stanu użycia, ważności i legalności licencji odbywało się w trybie bieżącym na okoliczność realizowanych czynności serwisowych i interwencji stanowiskowych, przy prowadzonej inwentaryzacji oraz okresowo prowadzonej akcji wymiany/aktualizacji komponentów na stacjach roboczych.

(akta kontroli str. 49-156, 215-223)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: monitorowanie faktycznego wykorzystania i przydatności danego oprogramowania dziedzinowego jest obowiązkiem kierownika danej komórki organizacyjnej. Jest to jedyna osoba, która jest w stanie określić potrzeby licencyjne dla danego stanowiska pracy (dotyczy oprogramowania dziedzinowego). Przy okazji inwentaryzacji weryfikuje się czy zainstalowane oprogramowanie na danym stanowisku pracy jest faktycznie wykorzystywane i potrzebne.

(akta kontroli str. 920-923)

Urząd posiadał procedury ISO dotyczące realizacji zakupów, w tym oprogramowania powyżej i poniżej kwotowego progu ustawy Prawo zamówień publicznych (P-IX-06 i P-IX-07), jak również procedurę nadzoru i aktualizacji oprogramowania oraz systemów komputerowych (P-X-02). Zapisy procedury P-X-02 dotyczyły dużych systemów dziedzinowych nabywanych w trybie ustawy Prawo zamówień publicznych, jak np. systemy FK, Ewidencja Ludności, itp.

(akta kontroli str. 479-500)

W Urzędzie za zakup oprogramowania odpowiedzialny był wyłącznie Wydział Informatyzacji. Zasady zakupu oprogramowania dużych systemów dziedzinowych oraz innych przeprowadzanych w trybie ustawy Prawo zamówień publicznych były uregulowane w procedurach, w tym również w Regulaminie zamówień publicznych.

(akta kontroli str. 611-617)

Obowiązujące w Urzędzie procedury nie odnosiły się w sposób szczegółowy do zarządzania oprogramowaniem innym niż dziedzinowe oraz oprogramowaniem Windows i MS Office.

(akta kontroli str. 5-156, 280-291)

[8] W module tym ewidencjonowane jest przypisanie miejsca użytkowania, osoba użytkująca i identyfikatory pomocnicze.

1.2. W Wydziale Informatyzacji zatrudnionych było dwanaście osób. Wszyscy posiadali pisemne zakresy obowiązków, wraz ze wskazaniem osób zastępujących w razie nieobecności. Pracownicy Wydziału Informatyzacji posiadali odpowiednie wykształcenie oraz szkolenia[9]. W okresie objętym kontrolą pracownicy nie uczestniczyli w szkoleniach dotyczących zasad licencjonowania i zarządzania oprogramowaniem.

(akta kontroli str. 356-358)

W sprawie liczby etatów w Wydziale Informatyzacji, Dyrektor tego Wydziału wyjaśnił, że: Zwracałem się wielokrotnie do władz Miasta o zwiększenie zatrudnienia, gdyż wg sporządzanych przeze mnie analiz stanu zatrudnienia zakres przydzielonych zadań i przejmowanych zadań z jednostek organizacyjnych Gminy mocno przekracza możliwości składu osobowego Wydziału Informatyzacji.

(akta kontroli str. 920-923)

1.3. Urząd prowadził rejestry (ewidencja wartości niematerialnych i prawnych, L.S., ewidencja Excel) użytkowanego oprogramowania. Dane zawarte w rejestrach miały służyć identyfikacji użytkownika oraz miejsce użytkowania.

(akta kontroli str. 224-251, 278-279)

27 marca 2018 r. Urząd zakupił L.S. za 165 tys. zł, a następnie opłacał wsparcie do tego oprogramowania dla 800 zasobów typu komputer, pięciu administratorów helpdesk i 10 agentów helpdesk. W latach 2019-2022 roczny koszt wsparcia wyniósł, odpowiednio: 18,3 tys. zł, 18,3 tys. zł, 21,3 tys. zł oraz 18,3 tys. zł. Dyrektor Wydziału Informatyzacji wyjaśnił, że: *monitorowanie oprogramowania odbywa się (w ograniczonym zakresie – gdyż baza L.S. nie jest kompletna) za pomocą agentów zainstalowanych na stacjach roboczych (obejmuje około 80% użytkowanych stacji roboczych). Z monitorowania wyłączone są stacje sieci wyizolowanych.*

(akta kontroli str. 251-268, 920-923)

Na podstawie zbadanej próby dziesięciu osób, które zmieniły stanowisko pracy ustalono, że po odejściu pracowników z danego miejsca pracy, licencjonowane oprogramowanie było zwalniane, a następnie udostępniane innemu pracownikowi w ciągu kilku dni. Dyrektor Wydziału Informatyzacji wyjaśnił, że: *w przypadku gdy pracownik zwalnia się i komputer, który użytkował na swoim stanowisku nie jest już potrzebny to wraca do Wydziału Informatyzacji (jest serwisowany i przydzielany kolejnemu pracownikowi) i wówczas licencje biurowe i system operacyjny pozostają na danej stacji roboczej. W przypadku gdy pracownik miał licencję MS Office i komputer uległ uszkodzeniu, wówczas w zależności od wersji i praw licencyjnych, licencja jest przenoszona na inny sprawny komputer (MS Office równy lub wyższy niż 2013 r.). Starsze wersje OEM ulegają dezaktywacji. W przypadku gdy pracownik korzystał z oprogramowania open source i uzasadnia potrzebę instalacji MS Office wtedy następuje przegląd wolnych licencji a w razie ich braku zakup. Wydział prowadzi arkusz pomocniczy licencji Office. Powyższe kwestie uregulowane są w instrukcjach postępowania i realizacji czynności technicznych, serwisu i instalacji wprowadzonych regulacją WIN.1331.3.2019.*

(akta kontroli str. 231-243, 269-277, 280-292, 920-923, 928)

Na próbie 11 losowo wybranych licencji ustalono, że dostępne były dowody ich zakupu oraz dokumenty określające zasady licencjonowania (poza C. i oprogramowaniem open source). Licencje przechowywane były w wydzielonym pomieszczeniu budynku Urzędu, zlokalizowanym w strefie ograniczonego dostępu.

[9] M.in.: z zakresu bezpieczeństwa i obsługi oprogramowania wykorzystywanego w Urzędzie, administrowania systemami dziedzinowymi oraz metody zarządzania PRINCE2.

Licencje przechowywano w zamkniętej szafie, w segregatorach. Część licencji przechowywana była w wersji elektronicznej.

Dyrektor Wydziału Informatyzacji wyjaśnił, że: w sprawie nieuprawnionej instalacji oprogramowania C. przeprowadzono postępowanie wyjaśniające WIN.042.5.4.2022, w wyniku którego ustalono, że program został zainstalowany przy okazji przenoszenia danych z urządzenia pendrive i został zablokowany przez program antywirusowy ale L.S. System odnotował go w swoim rejestrze. Przeprowadzono kompleksowe czyszczenie rejestru Windows na danym stanowisku pracy.

(akta kontroli str. 293-319, 624-687)

Urząd nie posiadał oprogramowania, którego autorami byliby obecni lub byli pracownicy Urzędu.

(akta kontroli str. 321)

1.4. W latach 2019-2022 Urząd zakupił 82 licencje za 17,4 tys. zł. Na dzień 24 października 2022 r. posiadał jedną wolną licencję Office 2013. Licencję zakupiono 19 sierpnia 2022 r. Dyrektor Wydziału Informatyzacji wyjaśnił, że: *19 sierpnia zakupiono 5 licencji office 2013, cztery wykorzystano a jedno stanowisko pracy jest w trakcie utworzenia.*

(akta kontroli str. 320, 920-923, 934)

Urząd nie zbywał odpłatnie sprzętu IT, przekazywał natomiast nieodpłatnie taki sprzęt tylko jednostkom organizacyjnym Gminy Miasta Tarnów. Przekazanie odbywało się na podstawie protokołów i umów. Sprzęt przekazywano z nośnikami danych, które uprzednio podlegały formatowaniu i wielokrotnemu nadpisywaniu. Brak było w tym zakresie procedur formalnych i protokołów z wykonanych czynności. Pracownicy Wydziału Informatyzacji przedstawili dokumenty potwierdzające formatowanie i wielokrotne nadpisywanie nośników danych, przeprowadzane na sprzęcie IT, który był przekazywany w trakcie kontroli NIK.

(akta kontroli str. 476-478, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: pomimo braku formalnych procedur w zakresie usuwania danych i licencji z nośników danych w sprzęcie IT przekazywanym jednostkom organizacyjnym Gminy Miasta Tarnów (należy podkreślić że często ze sprzętu IT usuwane są nośniki danych i podlegają utylizacji /tu funkcjonują formalne procedury i sporządzane są protokoły/ ze względu na ich zużycie i postęp technologiczny) istnieje minimalne ryzyko utraty poufności i nieuprawnionego użycia licencji, ponieważ sprzęt IT nie jest przekazywany bezpośrednio ze stanowisk pracy, ale trafia do Wydziału Informatyzacji, który również zajmuje się wspieraniem IT jednostek organizacyjnych i to pracownicy Wydziału Informatyzacji konfigurują na nowo przekazywany sprzęt jednostkom organizacyjnym, łącznie z jego instalacją na nowym miejscu eksploatacji (głównie pracownie komputerowe w szkołach). Nie bez znaczenia jest fakt, że jednostki które otrzymują taki sprzęt są również jednostkami organizacyjnymi Gminy Miasta Tarnowa i podlegają takim samym restrykcjom i procedurom w zakresie ochrony danych. Wymagane procedury zostaną wprowadzone.

(akta kontroli str. 618-623)

W latach 2019-2022 Urząd przekazał jednostkom organizacyjnym Gminy Miejskiej Tarnów łącznie 59 sztuk sprzętu IT, w tym 52 komputery i 5 laptopów wraz z licencjami Windows. Nie stosowano innych form zbywania lub nieodpłatnego przekazywania sprzętu IT.

(akta kontroli str. 693-816)

Urząd posiadał procedury likwidacji sprzętu IT[10]. Z czynności likwidacji sprzętu IT sporządzano protokoły.

(akta kontroli str.447-465, 611-617)

W Urzędzie nie było dokumentów potwierdzających, że w latach 2019-2022 czynności usuwania danych i programów z nośników danych były faktycznie wykonywane, przed nieodpłatnym przekazaniem sprzętu IT (z wyjątkiem przypadków przekazania dokonanych w trakcie kontroli). W czasie kontroli przedstawiono dokumenty, potwierdzające formatowanie i wielokrotne nadpisywanie nośników danych na sprzęcie IT, który w czasie trwania kontroli przeznaczony był do nieodpłatnego przekazania. Urząd posiadał dokumenty potwierdzające utylizację nośników danych oraz zawartego na nim oprogramowania ze sprzętu IT likwidowanego w latach 2019-2022.

(akta kontroli str. 461-475, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: W latach 2019 - 2022 nie miał miejsca incydent utraty poufności danych, ponieważ praktyka była taka, że nośniki danych, przed nieodpłatnym przekazaniem były formatowane i wielokrotnie nadpisywane (niskopoziomowe nadpisywanie, aby z wolnych obszarów pamięci uniemożliwić jakiekolwiek odzyskanie danych). Brak jest jedynie pisemnych procedur potwierdzających powyższą praktykę, co niezwłocznie zostanie uzupełnione. Natomiast nośniki danych ze sprzętu IT likwidowanego są utylizowane, co jest opisane w procedurach (Regulamin gospodarowania mieniem ruchomym, wniosek o likwidację sprzętu IT, itp.) i na tą okoliczność powstaje stosowana dokumentacja potwierdzająca (protokoły z likwidacji, karta przekazania odpadów). Dokumentacja z likwidacji nośników danych sporządzana jest w formie zdjęć oraz zawiera numery seryjne dysków oraz potwierdzenie wykonania utylizacji. Podsumowując, jeżeli sprzęt IT wychodzi poza Gminę (nie trafia do jej jednostek organizacyjnych) to nośniki danych są zawsze utylizowane, a jedynie w przypadku nieodpłatnego przekazania jednostkom organizacyjnym Gminy nośniki danych są czyszczone (poprzez formatowanie niskiego poziomu i wielokrotne nadpisywanie), choć w tym ostatnim przypadku brak jest formalnych procedur.

(akta kontroli str. 618-623)

W Urzędzie miały miejsce przeniesienia licencji Office 2013 pomiędzy stanowiskami pracy, zgodnie z posiadaną procedurą. Zostały one odnotowane w rejestrze wartości niematerialnych i prawnych. Powyższych danych nie odnotowano w L.S.

(akta kontroli str. 587-593, 611-617)

Każda osoba w ramach szkolenia RODO, potwierdzała znajomość zasad korzystania z zasobów IT oraz w przypadku wykonywania pracy zdalnej podpisywała dodatkowe dokumenty. Zasady korzystania z zasobów IT zawarte były również w zakresach czynności. Dla pracowników prowadzone były szkolenia uzupełniające z zasad bezpieczeństwa podczas korzystania z infrastruktury IT Urzędu.

(akta kontroli str. 322-329)

Planowe przeglądy i inwentaryzacje oprogramowania odbywały się na podstawie przepisów ustawy z dnia 29 września 1994 r. o rachunkowości[11]. Przeglądy przeprowadzała komisja inwentaryzacyjna. Dodatkowo przeglądy były realizowane na

[10] Wzór wniosku na likwidację wraz z wykazem sprzętu do likwidacji, zawierającym m.in. ocenę techniczną i uzasadnienie likwidacji każdorazowo wydawane było zarządzenie w sprawie powołania Komisji w sprawie oceny przydatności składników majątku, Zarządzenie nr 405/2018 Prezydenta Miasta Tarnowa z 9 października 2018 r. ws. wprowadzenia Regulaminu gospodarowania mieniem ruchomym w Urzędzie Miasta Tarnowa.

[11] Dz. U z 2021 r., poz. 217, dalej: *ustawa o rachunkowości.*

okoliczność czynności serwisowych, zgodnie z instrukcją kontroli i serwisu stanowisk IT w Urzędzie I-WIN-01-2019. Przeprowadzali je wyznaczeni pracownicy Wydziału Informatyzacji (posiadający odpowiednie wpisy w zakresie czynności). Przeglądy oprogramowania przeprowadzał również Inspektor Ochrony Danych Osobowych przy okazji przeprowadzanych audytów. Odpowiednie zapisy znajdowały się w raportach z audytu, w pozycjach audyt zasobów teleinformatycznych i audyt zasobów sprzętowych IT.

(akta kontroli str. 330-339)

Urząd posiadał oprogramowanie L.S. dające możliwości analizy zainstalowanego oprogramowania. Ponadto check point wydawał automatyczne komunikaty Administratorowi Systemów Informatycznych o instalacji produktów niebezpiecznych, mających wpływ na niekontrolowany ruch w sieci wewnętrznej.

(akta kontroli str. 330-336)

W lata 2019-2022 Urząd nie wycofał z ewidencji wartości niematerialnych i prawnych żadnych licencji. W toku kontroli została powołana komisja ds. oceny przydatności składników majątku.

(akta kontroli str. 687-688)

Wyjaśniając zasady użytkowania licencji Dyrektor Wydziału Informatyzacji podał, że: Licencje i zasady użytkowania oprogramowania dziedzinowego (np. FK/ Ewidencje itp) regulują zapisy umów (zakupu, utrzymaniowo-serwisowych). Szczególnymi przypadkami są licencje OEM (integralnie związane ze sprzętem), nie ewidencjonowane w zewnętrznych rejestrach, które nie można aktywować w przypadku awarii płyty głównej lub z uwagi na ograniczenia serwera aktywacyjnego w USA. Urząd kupuje roczne prawo dostępu do systemów (do użytkowania niektórych systemów/oprogramowań np. L., N.E., cenniki S. itp.), ale nie są to typowe licencje. Część licencji ściśle związana ze sprzętem OEM np. MS Office 2007, MS Office 2010 (gdzie prawo Microsoft zabrania przenoszenia oprogramowania), w przypadku trwałej awarii komputera, jest usuwane z ewidencji a koperty z nośnikami są wyodrębniane ze składu i licencje są dezaktywowane.

(akta kontroli str. 920-923)

W zbadanym zakresie nie stwierdzono w Urzędzie przypadków nielegalnego użytkowania oprogramowania i poniesienia kar z tego tytułu.

(akta kontroli str. 341)

W Urzędzie nie wdrożono mechanizmów kontrolnych (dotyczących wszystkich licencji) zapewniających, że proces dystrybucji uwzględniał warunki umowy licencyjnej. Prowadzony w Urzędzie rejestr statyczny (w Excel) umożliwiał jednak kontrolę nad dystrybucją oprogramowania Office i Windows. W toku niniejszej kontroli nie stwierdzono przypadku nieuprawnionej dystrybucji oprogramowania Windows i Office.

(akta kontroli str. 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: do kontroli dystrybucji wszystkich licencji zostanie wykorzystany L.S. Rejestry w Wydziale Informatyzacji pozwalają jednak na kontrolę dystrybucji oprogramowania Windows i Office co jest szczególnie przestrzegane.

(akta kontroli str. 618-623)

Powołany przez NIK biegły[12] zidentyfikował przypadki:

a) braku aktualizacji serwerowych systemów operacyjnych, wśród których funkcjonują również serwery pracujące pod kontrolą systemów bez wsparcia ;

b) braku aktualizacji aplikacji na poszczególnych serwerach;

c) nieaktualnych wersji aplikacji shareware na serwerach;

d) braku aktualizacji programów na hostach użytkowników (np. różne wersje przeglądarek), oprogramowania do łączenia się i zarządzania innymi komputerami mimo zakupu licencji na aplikację T., która odpowiada za ten proces;

e) instalacji różnych wersji tych samych programów na hostach użytkowników, co jednoznacznie pozwala stwierdzić, że zarządzanie poprawkami (nawet tych na poziomie krytycznym pod kątem bezpieczeństwa) jest na nieakceptowalnym poziomie;

f) oprogramowania na hostach użytkowników, określanego jako EOS (end of support), które nie posiada już wsparcia producenta;

g) oprogramowania na hostach użytkowników umożliwiającego synchronizację plików z chmurami publicznymi;

h) oprogramowania do łamania zabezpieczeń, generowania nielegalnych kodów czy wyszukiwania kodów;

i) oprogramowania dystrybuowanego jako SaaS, które służy do prowadzenia i synchronizacji np. notatek i plików;

j) oprogramowania na licencjach prywatnych, zainstalowanego na sprzęcie służbowym (np. B. na służbowym smartfonie).

(akta kontroli 818-834, 853-859)

Dyrektor Wydziału Informatyzacji wyjaśnił, że:

a) Odnośnie braku aktualizacji systemów operacyjnych. W odniesieniu do braku aktualizacji serwerowych systemów operacyjnych informuję, iż funkcjonuje na nich oprogramowanie dziedzinowe które na nowszych/zaktualizowanych dystrybucjach nie będzie działać. Autorzy oprogramowania dziedzinowego nie wspierają go w zakresie zgodności z najnowszymi dystrybucjami, a nowsze wersje oprogramowania dziedzinowego już się nie pojawiają choć UM w dalszym ciągu je eksploatuje. Wskazane serwery nie służą użytkownikom do przetwarzania danych osobowych (...). Planowana jest w najbliższym czasie migracja tych serwerów dla których jest to możliwe do najnowszych wersji (...).

b) Odnośnie braku aktualizacji aplikacji na poszczególnych serwerach (...) Informuję, iż przeglądarka (...) na serwerze (...) i dalsze aktualizacje tej przeglądarki na tym systemie operacyjnym nie są możliwe, tym samym jest to najbardziej aktualna wersja przeglądarki w wersji (...) dla tego systemu operacyjnego.

c) Odnośnie aplikacji shareware na serwerach (...). Istotnie aplikacja typu shareware (...) była zainstalowana na serwerze (...), po zwróceniu uwagi przez biegłego została niezwłocznie odinstalowana.

d) Odnośnie braku aktualizacji programów na stacjach, (...). Wykonywanie aktualizacji na stacjach końcowych nie jest zarządzane centralnie/domenowo i wykonywane w jednakowym czasie, zatem mogą istnieć różnice w wersjach przeglądarek na stacjach końcowych. Urząd nie narzuca użytkownikowi wyboru konkretnej przeglądarki internetowej a przeglądarki które są wykorzystywane/preferowane przez danego użytkownika same przypominają o aktualizacjach. Ponadto niektóre systemy wymagają konkretnej przeglądarki w wersjach starszych niż aktualna (...).

[12] Powołany na podstawie postanowienie Dyrektora Delegatury NIK w Krakowie o powołaniu biegłego z dnia 1 września 2022 r.

Odnośnie oprogramowania typu V. – jest to program o nieco węższym spektrum zastosowań niż wspomniany zakupiony T. i występuje on w różnych wersjach na stacjach jako składnik L.S.

e) Odnośnie różnych wersji tych samych programów świadczące o zarządzaniu poprawkami na nieakceptowalnym poziomie (...) oraz EOS (end of suport) (...). Wymienione oprogramowanie (...) nie jest użytkowane w Urzędzie Miasta Tarnowa (błąd w wyjaśnieniach). Urząd posiada jedynie 3 licencje A., którego elementem składowym nie jest wymienione oprogramowanie. Do trwałego usuwania danych z dysków wykorzystywane są narzędzia Microsoft służące do tego celu (...). Oficjalnie wycofany T. w wersji uruchomieniowej został wykryty tylko na jednym komputerze należącym do pracownika WIN w zasobach dotyczących wdrożenia systemu Tarnowskiej Karty Miejskiej. Oprogramowanie nie jest aktualnie użytkowane na danym stanowisku i stanowi jedynie archiwum z czasów wdrożenia.

f) Odnośnie oprogramowania typu iCloud. Oprogramowanie wykorzystywane było jedynie do konfiguracji telefonu i weryfikacji poprawności poświadczeń użytkownika telefonu. Oprogramowanie było legalne dostarczone przez producenta.

g) Odnośnie oprogramowania do łamania zabezpieczeń. Aplikacja C. została przypadkowo uruchomiona z pendriva, z którego pracownik przenosił dane. Aplikacja została zablokowana przez program antywirusowy. Oprogramowanie K. było używane przez pracownika Wydziału Informatyzacji w przypadku gdy naklejka licencyjna była nieczytelna lub zamazana.

h) Odnośnie oprogramowania SaaS (...). W wyniku przeprowadzonego postępowania wyjaśniającego ustalono, że oprogramowanie to nie zostało wykorzystane do synchronizacji danych z chmurą.

i) Odnośnie oprogramowania typu bitdefender na smartfonie. Jest to oprogramowanie antywirusowe zainstalowane i kupione przez użytkownika prywatnie. Nie stanowiło to złamania zasad licencji i bezpieczeństwa.

(akta kontroli 925-926)

W Urzędzie nie wprowadzono procedur dotyczących działań naprawczych w przypadku wystąpienia niezgodności zw. z zarządzaniem oprogramowaniem, w szczególności nie wskazano osób odpowiedzialnych za działania naprawcze w odniesieniu do konkretnych incydentów, nie wskazano krytycznego czasu reakcji oraz identyfikacji przyczyn w celu uniknięcia ponownego ich wystąpienia. Urząd posiadał procedurę zgłoszenia naruszenia zabezpieczeń danych osobowych w systemie przetwarzania danych osobowych, która również uwzględniała działania naprawcze i zapobiegawcze w przypadku użycia nieautoryzowanego oprogramowania. W toku niniejszej kontroli przedstawiono dowody potwierdzające realizację ww. procedury w przypadku wykorzystania nieautoryzowanego oprogramowania E. i icloud.

(akta kontroli str. 594-610, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: na okoliczność pojawiających się zagrożeń i obowiązków prawnych w ramach działań zapobiegawczych i naprawczych, w tym również dotyczących użycia nieautoryzowanego oprogramowania, prowadzone są akcje informacyjne i cykliczne szkolenia. Jeżeli użycie nieautoryzowanego oprogramowania związane jest z przetwarzaniem danych osobowych to podlega procedurze RODO WIN.042.5.4.2022. Niemniej jednak zostanie w Urzędzie wprowadzona procedura dotycząca działań naprawczych odnosząca się bezpośrednio do zarządzania oprogramowaniem.

(akta kontroli str. 618-623)

1.5. Pracownicy Wydziału Informatyzacji nie odbyli szkoleń dotyczących weryfikacji zgodności użytkowania oprogramowania z warunkami licencji. Powołany w trakcie kontroli NIK biegły nie zidentyfikował licencji specyficznych, których wykorzystanie wymagałoby przeszkolenia.

(akta kontroli str. 818-834)

Prowadzona przez pracowników Wydziału Informatyzacji weryfikacja oprogramowania z warunkami licencji odbywała się poprzez zapoznanie się z warunkami zamieszczonymi na stronie internetowej.

(akta kontroli str. 818-834)

Dyrektor Wydziału Informatyzacji wyjaśnił, że do weryfikacji licencji nabywanego oprogramowania zostanie zaangażowany Dział Prawny Urzędu.

(akta kontroli str. 920-923)

Na próbie dziesięciu wylosowanych licencji ustalono, że:

a) Licencja V. nabyta w 2022 r. - jedna możliwa do zainstalowania na serwerze z dostępem do wszystkich jednostek oświatowych (nieograniczona stanowiskowo) i jedna licencja faktycznie zainstalowana. Licencja zakupiona na czas nieokreślony, corocznie wykupywane było wsparcie i aktualizacja produktu.

b) Licencja E., nabyta w 2022 r. - jedna możliwa do zainstalowania na serwerze z dostępem dla pracowników Wydziału Geodezji i Architektury (nieograniczone stanowiskowo) oraz jedna licencja faktycznie zainstalowana. Licencja zakupiona na czas nieokreślony, corocznie wykupywane było wsparcie i aktualizacja produktu.

c) Licencja T. nabyta w 2022 r. - jedna możliwa do zainstalowania na serwerze z dostępem dla pracowników Wydziału Geodezji i Architektury (nieograniczone stanowiskowo) oraz jedna licencja faktycznie zainstalowana. Licencja zakupiona na czas nieokreślony, corocznie wykupywane było wsparcie i aktualizacja produktu.

d) Licencja P. - zainstalowana na serwerze pocztowym w celu ochrony skrzynek pocztowych utrzymywanych dla Urzędu i wyznaczonych jednostek organizacyjnych Gminy Miejskiej Tarnów. Licencja umożliwia ochronę max. 1001 skrzynek pocztowych, a faktycznie chronionych było 756. Dyrektor Wydziału Informatyzacji wyjaśnił, że: ze względu na politykę cenową dostawcy PROFFPOINT bardziej opłacalny był zakup ponad 1000 punktów chronionych.

e) Licencja A. na oprogramowanie narzędziowe służące do operacji na dyskach twardych przez serwis Wydziału Informatyzacji. Liczba możliwych do zainstalowania licencji zakupionych w 2021 r. wyniosła dwie (oraz jedna zakupiona w 2017 r.). Trzy licencje są faktycznie użytkowane. Nieograniczony czas obowiązywania licencji.

f) Licencja R. wykorzystywana w Wydziale Spraw Obywatelskich, na czas nieokreślony. Jedna licencja instalowana na serwerze na nieograniczoną liczbę użytkowników. Jedna licencja faktycznie użytkowana.

g) Licencja N. wykorzystywana do ochrony antywirusowej. Liczba licencji 500, liczba faktycznie wykorzystanych 500. Data ważności licencji do 13 września 2022 r.

h) Licencja Office 2013 r. (faktura dokumentująca zakup pięciu licencji, które są faktycznie użytkowane). Nieograniczony czas obowiązywania licencji.

i) Licencja C. wykorzystywana do zarządzania i ochrony sieci Urzędu. Zakupiono dwie licencje na dwa urządzenia chroniące dwa segmenty sieci (podstawową i zapasową). Faktycznie zainstalowane na dwóch urządzeniach brzegowych typu UTM. Licencja obowiązywała na czas nieokreślony. Wsparcie i aktualizację wykupiono do 16 września 2022 r. Na dzień 8 września 2022 r. rozstrzygnięto postępowanie na przedłużenie wsparcia i aktualizacji.

j) Licencja L. wykorzystywane pomocniczo jako oprogramowanie biurowe. Faktycznie użytkowanych 100 licencji. Liczba możliwych do zainstalowania produktów oraz ważność licencji – nieograniczona.

(akta kontroli str. 315, 342-355)

Stwierdzone nieprawidłowości

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

1. Urząd nie posiadał pisemnych procedur dotyczących innego niż dziedzinowe oprogramowania obejmujących:
   - role i odpowiedzialności (dotyczące aktualizacji i bieżącego monitorowania ważności licencji),
   - nabywanie i wycofywanie licencji,
   - dystrybucję i redystrybucję,
   - inwentaryzację i przeglądy,
   - bezpieczeństwo i nośniki instalacyjne,
   - monitorowanie (stanu użycia, ważności i legalności licencji),
   - działania naprawcze.

   Nie określono również zasad badania efektywności wykorzystania licencji. Ponadto w procedurach nie uregulowano, kto jest odpowiedzialny za weryfikację umów licencyjnych i utrzymanie zgodności z przepisami praw autorskich i praw pokrewnych na zasobach sprzętowych.

   W ocenie NIK nieokreślenie ww. zasad było działaniem nierzetelnym i skutkowało m.in. brakiem możliwości potwierdzenia prowadzenia regularnego przeglądu oprogramowania i adekwatności podejmowanych działań naprawczych, czy też dokonywania każdorazowej oceny zasadności nabycia danego oprogramowania.

   (akta kontroli str. 611-617)

   Dyrektor Wydziału Informatyzacji wyjaśnił, że: oprogramowanie w Urzędzie można podzielić na oprogramowanie dużych systemów dziedzinowych (np. Tarnowska Karta Miejska, System Odpadów w Gminie, systemy finansowe i systemy edukacyjne) oraz pozostałe oprogramowanie użytkowe wykorzystywane na stacjach końcowych. Zasady zarządzania licencjami dużych systemów dziedzinowych są uregulowane odpowiednimi procedurami, natomiast zasady zarządzania licencjami pozostałego oprogramowania nie zostały opracowane i wdrożone, co niezwłocznie zostanie wykonane (…). Do weryfikacji treści umów licencyjnych zostanie zaangażowany dział prawny.

   (akta kontroli str. 618-623)

2. Urząd nie zarządzał skutecznie zasobami sprzętowymi, takimi jak smartfony i tablety pod kątem instalacji i wykorzystywania oprogramowania (brak zarządzania oprogramowaniem znajdującym się na tych zasobach). Urząd nie posiadał narzędzi klasy Unified Endpoit Management, Mobile Device Managment czy Enterprise Mobility Managment, nie potwierdził także prowadzenia monitorowania oprogramowania instalowanego na urządzeniach mobilnych w inny sposób, np. manualny.

   Wydawaniem, przenoszeniem przydziału i wycofywaniem urządzeń mobilnych z użytkowania zajmował się Wydziału Organizacyjny. Oprogramowanie zainstalowane na urządzeniach mobilnych nie było monitorowane przez żadną komórkę organizacyjną Urzędu. Badanie próby pięciu smartfonów pod kątem zawartego oprogramowania wykazało instalację przez użytkowników prywatnych aplikacji, w tym gier nie mających związku z wykonywanymi czynnościami

służbowymi. Pracownicy Urzędu przy wykorzystywaniu smartfonów, poprzez przeglądarkę internetową i dedykowane aplikacje mieli dostęp do poczty służbowej, co przy braku specjalistycznego oprogramowania do zarządzania smartfonami tworzyło ryzyko nieautoryzowanego dostępu do danych i ich bezpieczeństwa. Urząd posiadał laptopy, jednak nie na wszystkich zainstalowany był agent L.S.

W ocenie NIK brak monitorowania oprogramowania na urządzeniach mobilnych stwarza ryzyko w zakresie bezpieczeństwa oraz naruszenia praw autorskich i świadczy o nierzetelnym zarządzaniu oprogramowaniem na tych urządzeniach.

(akta kontroli str. 611-617, 818-834)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: zostaną wprowadzone procedury zarządzania smartfonami i tabletami, (…) zostanie rozważony zakup oprogramowania do zarządzania urządzeniami klasy portable oraz zostaną określone zasady badania efektywności wykorzystania licencji, a także dokonywania oceny w zakresie bezpieczeństwa wykorzystywanych lub wdrażanych aplikacji darmowych lub aplikacji dystrybuowanych w modelu „portable".

Wydział Informatyzacji przejmie zadnia związane z nadzorem nad oprogramowaniem smartfonów i tabletów, wprowadzi standard oprogramowania na tych urządzeniach i będzie wymagał podpisania od ich użytkowników oświadczenia o zasadach użytkowania. Zakupione zostanie również oprogramowanie do zarządzanie oprogramowaniem urządzeń mobilnych. Na laptopach również zostanie wprowadzony standard oprogramowania oraz procedury wymuszające okresowe, systematyczne logowanie się laptopów do sieci umożliwiające identyfikację i inwentaryzację oprogramowania przez L.S.

(akta kontroli str. 618-623, 920-923)

3. Urząd nie posiadał jednolitego rejestru licencji i oprogramowania, a prowadzone ewidencje były rozproszone (moduł majątek systemu KSAT 2000 I, ewidencja w Excel, L.S.). Rejestry licencji i oprogramowania pozwalały na określenie lokalizacji i użytkownika, jednak ewidencje statyczne utrudniały prowadzenie efektywnego nadzoru nad oprogramowaniem oraz stwarzały problemy z ich aktualnością. Dodać należy, że w prowadzonych rejestrach statycznych nie było informacji na temat daty wygaśnięcia licencji, daty zakończenia subskrypcji czy końca cyklu życia oprogramowania (takie informacje znajdowały się natomiast w dokumentach źródłowych). NIK podkreśla, że wszyscy użytkownicy końcowi stacji roboczych mieli nieograniczone prawa administratora, co skutkowało m.in. możliwością zainstalowania oprogramowania bez weryfikacji pracowników Wydziału Informatyzacji i utrudniało prowadzenie rejestrów.

   Efektywny nadzór oraz aktualność rejestru licencji może zapewnić jedynie oprogramowanie typu inventory tool, np. L.S., do którego wprowadzono by wszystkie licencje. Tymczasem wg stanu na 21 września 2022 r. do L.S. wprowadzonych było zaledwie ok. 20% licencji. Podpięte do L.S. stacje robocze raportowały zdarzenia zw. z instalacją nowego oprogramowania, jednak ze względu na brak kompletnego spisu oprogramowania utrudniona była weryfikacja dopuszczalnych czynności instalacyjnych. NIK zwraca uwagę, że na zakup L.S. wydano 165 tys. zł, a łączny koszt wsparcia w latach 2019-2022 wyniósł 76,2 tys. zł.

   Pomimo, iż pracownicy Urzędu przed objęciem stanowiska pracy podpisywali oświadczenie zobowiązujące do nieinstalowania nieautoryzowanego oprogramowania i przyjmowali do wiadomości, że jedyną uprawnioną komórką do instalacji oprogramowania jest Wydział Informatyzacji, to zidentyfikowano przypadki zainstalowania na stacjach roboczych większej liczby programów niż liczba posiadanych licencji (m.in. T., W., A., E.).

W ocenie NIK powyższe działania były nierzetelne, ponieważ stwarzały ryzyko istotnego zagrożenia bezpieczeństwa informatycznego Urzędu oraz naruszenia praw autorskich.

(akta kontroli str. 251-268, 578-586, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: *niezwłocznie do L.S. zostaną wprowadzone wszystkie posiadane licencje i oprogramowanie będące w posiadaniu Urzędu w celu przeprowadzenia kompletnego audytu. Ponadto odpowiedni pracownik zostanie skierowany na szkolenie w zakresie wykorzystania L.S. do zarządzania oprogramowaniem.*

Wydział Informatyzacji skoncentruje się na prowadzeniu ewidencji z wykorzystaniem L.S., co pozwoli na bieżącą inwentaryzację i nadzór nad faktycznym wykorzystaniem licencji i oprogramowania. Wydział Informatyzacji podjął czynności mające na celu ograniczenie praw administratora dla użytkowników końcowych stacji roboczych. Zidentyfikowane w toku kontroli NIK przypadki zainstalowania większej liczby programów niż posiadanych licencji zostaną przeanalizowane przez Urząd i w uzasadnionych przypadkach odinstalowane. Większa liczba oprogramowania zainstalowanego niż posiadanych licencji wynika m.in. w przypadku T., W. z tego, że serwisanci dla wygody wykonania swoich czynności instalowali jednorazowo oprogramowanie a po zakończeniu swoich czynności nie odinstalowali niepotrzebnego już programu. Podobnie było z pozostałymi programami. Skutek był taki, że pomimo nie używania oprogramowania znajdowało się ona na stacji roboczej, co nominalnie przekraczało liczbę posiadanych licencji, choć faktycznie nie użytkowano większej jej liczby niż posiadane licencje. Urząd wprowadzi mechanizmy weryfikacji zainstalowanego oprogramowania po wykonaniu czynności serwisowych wraz z kontrolnym wydrukiem z rejestru Windows. Dodatkowo pełne wykorzystanie L.S. uniemożliwi wystąpienie wyżej opisanych niezgodności. W przypadku subskrypcji rocznych producenci oprogramowania informują o wygaśnięciu licencji. Niezwłocznie do L.S. zostaną wprowadzone wszystkie licencje i towarzyszące im dane w celu uzyskania pełnej kontroli nad aktualnością licencji i oprogramowania.

(akta kontroli str. 618-623)

4. W Urzędzie zainstalowano większą liczbę oprogramowania T. i W., niż liczba zakupionych licencji.

(akta kontroli str. 545-577, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: potwierdzenia zakupów licencji i praw do użytkowania stanowią faktury zakupu, stosowne sticker, dokumenty licencyjne, i inne dokumenty wydruki licencji elektronicznych stanowiące materiał licencyjne w zależności od rodzaju oprogramowania i producentów. Na okoliczność wykrytego oprogramowania niezgodnego z licencjami zostało przeprowadzone postępowanie wyjaśniające WIN.042.5.4.2022 w wyniku którego usunięto je.

(akta kontroli str. 618-623)

5. W ewidencjach Urzędu (KSAT 2000 I, ewidencja w Excel) ujęto oprogramowania Windows 2000 oraz Word 2003, które nie było wykorzystywane w związku z likwidacją komputerów i nie zostało wycofane z ewidencji pomimo, że nie spełniało definicji aktywów o których mowa w art. 3 ust. 1 pkt 12 ustawy o rachunkowości.

(akta kontroli 216-217, 317-319, 545-577, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: Urząd jest w trakcie realizacji procedury likwidacji nieużytkowanych wartości niematerialnych i prawnych, tak więc niewykorzystywane oprogramowanie zidentyfikowane w czasie kontroli NIK

(Windows 2000, Word 2003 itp.) zostanie usunięte z ewidencji i zlikwidowane. Następnie cały proces zostanie zakończony audytem L.S.

(akta kontroli 618-623)

6. Urząd nie posiadał procedur oraz dokumentacji potwierdzającej usunięcie danych z dysków[13], jak również dedykowanego oprogramowania do trwałego wymazywania danych z nośników i funkcji wystawiającej certyfikat, który potwierdza wymazanie danych na nośniku o danym numerze seryjnym.

   W ocenie NIK powyższe może świadczyć o nierzetelnym wykonywaniu obowiązków w zakresie zarządzania oprogramowaniem i dodatkowo może stwarzać ryzyka związane z bezpieczeństwem.

   (akta kontroli str. 611-617)

   Dyrektor Wydziału Informatyzacji wyjaśnił, że: działania w zakresie nieodpłatnego przekazywania sprzętu IT nie są zależne od indywidualnych decyzji pracowników, ponieważ wymagają akceptacji Prezydenta (który podejmuje decyzję), pracowników Wydziału Organizacyjnego (którzy przygotowują dokumenty przekazania oraz umowę) oraz pracowników IT, którzy wykonują czynności techniczne związane z przygotowaniem sprzętu do przekazania. Nie wykorzystywanie dedykowanego oprogramowania do trwałego wymazywania danych i oprogramowania z nośników nie oznacza, że sprzęt IT przekazywany jest z danymi i oprogramowaniem. Czynności polegające na wymazaniu danych i usunięciu programów są wykonywane poprzez formatowanie i kilkukrotne nadpisywanie zawartości dysku. Co prawda nie ma z tej czynności sporządzanego protokołu, ale w praktyce brak było incydentów związanych z pozostawieniem danych na przekazywanych nośnikach. Stosowne pisemne procedury zostaną wprowadzone. Należy podkreślić, że faktyczne czynności usuwania danych i oprogramowania są wykonywane, jednak brak jest w tym zakresie formalnych procedur.

   (akta kontroli str. 618-623)

7. Urząd nie prowadził zaplanowanych okresowych przeglądów oprogramowania i licencji, w tym środowisk wirtualnych, mających na celu potwierdzenie, że spis jest aktualny, kompletny oraz że posiada licencje na każde zainstalowane oprogramowanie.

   W trakcie kontroli zidentyfikowano przypadki zainstalowania na serwerze wirtualnym niewspieranego oprogramowania W., T.

   (akta kontroli str. 501-508, 611-617)

   W ocenie NIK brak okresowych i pełnych audytów oprogramowania stanowi nierzetelne działanie, które utrudnia efektywne i skuteczne zarządzanie oprogramowaniem (stwierdzono przypadki wykorzystywania oprogramowania niewspieranego oraz nieaktualnego).

   Dyrektor Wydziału Informatyzacji wyjaśnił, że: Wydział Informatyzacji zobowiązuje się przeprowadzania okresowych pełnych audytów posiadanego oprogramowania i licencji. W tym celu zostaną m.in. uzupełnione dane w L.S. Za przeglądy autoryzowanego oprogramowania na środowiskach wirtualnych odpowiedzialni są ASI, LASI. Wprowadzone zostaną formalne procedury, które wyeliminują przypadki stwierdzone w trakcie kontroli posiadania nieaktualnych wersji oprogramowania. W. wykorzystywany jest do (...), nie świadczy usług na zewnątrz więc stanowi ograniczone ryzyko dalszego użytkowania. Nie został wymieniony na aktualne oprogramowanie z powody braku pieniędzy. Wydział Informatyzacji zwróci się do

[13] Dotyczy sprzętu IT przekazywanego jednostkom organizacyjnym, a nie wycofywanego z użycia.

Prezydenta o uwzględnienie w planie budżetu na 2023 r. środków na aktualizację oprogramowania, w tym niezbędnego L.S. (...).

(akta kontroli str. 618-623)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia organizację, użytkowanie i nadzór nad oprogramowaniem komputerowym w Urzędzie.
W Urzędzie nie określono szczegółowych zasad zarządzania licencjami obejmujących wszystkie elementy i wymagane czynności niezbędne do zarządzania i nadzoru nad całym cyklem życia oprogramowania. Zasoby kadrowe, którym przypisano realizację elementów przedmiotowego zadania były niewystarczające. Nie zapewniono - w ramach posiadanego przez Urząd narzędzia do monitorowania oprogramowania - kompletności danych o wszystkich posiadanych i wykorzystywanych licencjach, co skutkowało brakiem możliwości efektywnego wykorzystania tego narzędzia. Nie zapewniono stałej i bieżącej informacji na temat wszystkich posiadanych i wykorzystywanych licencji, w szczególności użytkowanych na różnych typach urządzeń. Nie potwierdzono wykonywania audytów (przeglądów) całości zasobów pod kątem wykrycia nielegalnego oprogramowania. W toku kontroli NIK stwierdzono przypadki nieprawidłowego użytkowania licencji.

OBSZAR

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

Opis stanu faktycznego

2.1. W latach 2019-2022 Urząd zakupił[14], odpowiednio: 25 licencji za 3 269,2 tys. zł, 18 licencji za 914,3 tys. zł, 20 licencji za 1 015,4 tys. zł i 20 licencji za 1 113,8 tys. zł. Za zakup oprogramowania merytorycznie odpowiadał Wydział Informatyzacji, który przygotowywał wnioski dla Zespołu Zamówień Publicznych realizującego procedurę zakupu. Na etapie przygotowania budżetu, Wydział Informatyzacji przedkładał Wydziałowi Budżetu i Sprawozdawczości plany zakupu oprogramowania w ramach planu wydatków na rok następny. Procedura ta uregulowana była w zarządzeniu w sprawie przygotowania budżetu Miasta. Dyrektor Wydziału Informatyzacji wyjaśnił, że: *90% wydatków na zakup oprogramowania stanowi zakup aktualizacji i utrzymania już eksploatowanych dużych systemów dziedzinowych, więc mechanizm kontrolny zapewniający zasadność zakupu stosowany jest automatycznie. Tylko niewielka część to zakupy interwencyjne brakującego oprogramowania, które są realizowane po uprzednim złożeniu wniosku do Wydziału Informatyzacji (bądź są efektem realizacji procedur serwisowych) i weryfikacji czy Urząd posiada potrzebne oprogramowanie w wolnych zasobach. Nie dokonywano zmian w corocznych planach zakupów oprogramowania.*

(akta kontroli str. 17-46, 383-386, 391-394, 920-923, 929-933)

W toku kontroli nie stwierdzono przypadku zainstalowanego a niewykorzystywanego oprogramowania. Nieprzydatne oprogramowanie podlegało likwidacji, na podstawie § 9 Regulaminu gospodarowania mieniem ruchomym w Urzędzie Miasta Tarnowa[15].

(akta kontroli str. 387-390)

2.2. Urząd realizując projekt Centrum Usług Wspólnych, mający na celu optymalizację zarządzania dziedzinowymi systemami IT, przeprowadził analizy ekonomiczne, ryzyka, wariantowe i specyficzne. Analizy te dotyczyły m.in. potrzeb w zakresie zakupu oraz optymalnego i efektywnego wykorzystania oprogramowania, a przede wszystkim utworzenia wirtualnego środowiska przetwarzania danych samorządowych

[14] Podane kwoty dotyczą wydatków związanych z zakupem, przedłużeniem licencji i utrzymaniem oprogramowania.

[15] Zarządzenie nr 405/2018 Prezydenta Miasta Tarnowa z 9 października 2018 r.

(chmura). Stanowiły one część dokumentacji wniosku projektowego w ramach działania 2.1.1. „Elektroniczna administracja" Regionalnego Programu Operacyjnego Województwa Małopolskiego. Dyrektor Wydziału Informatyzacji wyjaśnił, że: *na etapie składania wniosku RPO W, którego efektem była budowa środowiska chmury samorządowej, przeprowadzono analizy efektywności wykorzystania oprogramowania stosowanego w Gminie. Elementem podstawowym była inwentaryzacja przeprowadzona w fazie przygotowań aplikacyjnych. Podejście smart jako podstawa projektowania i realizacji CUW obecnie stanowi najbardziej efektywny model przetwarzania danych. Aplikacje, systemy są instalowane w jednym miejscu (CUW) co powoduje że jest jedno postępowanie na zakup oprogramowania wielostanowiskowego. Aktualizacje i zarządzanie są centralne, co ma szczególne znaczenie przy ograniczonej kadrze i potrzebach wynikających z wymagań technologicznych. Słuszność CUW potwierdza artykuł PAP (https://samorzad.pap.pl/kategoria/archiwum/cuw-jak-dzialaja-samorzadowe-centra-uslug-wspolnych-dwa-lata-funkcjonowania\). (…) Efektywność oprogramowania wpisana jest w podstawowe cechy utrzymywania środowiska wirtualnego, co powoduje efektywne wykorzystanie procesorów i pamięci. Bez wdrożenia rozwiązań CUW w Gminie Miasta Tarnowa nie byłoby wystarczających kadr informatycznych do realizacji zadań.*

(akta kontroli str. 359-382, 920-923)

Efektywność wykorzystania dziedzinowego oprogramowania zapewniał prowadzony model wirtualnej chmury dla Urzędu i wszystkich jego jednostek organizacyjnych, umożliwiający wirtualny przydział i kontrolę dostępu do danych i oprogramowania. Urząd z uwagi na utrzymywanie własnego środowiska chmury samorządowej i obowiązki wynikające z RODO nie korzystał z usług SaaS w zakresie przetwarzania danych z systemów dziedzinowych.

(akta kontroli str. 395)

LASI odpowiadali za dostępne dla użytkowników funkcjonalności danego systemu dziedzinowego i korzystając z modułu "użytkownicy" weryfikowali stan bieżący ustawień w tym rejestrze. Przełożony danego pracownika wnioskował do LASI o nadanie uprawnień i dostępu we wnioskowanym systemie. Dyrektor Wydziału Informatyzacji wyjaśnił, że: *weryfikacja adekwatności przydzielonych użytkownikowi narzędzi informatycznych związana jest z zakresem obowiązków pracownika i leży w gestii przełożonego tego pracownika, który korzystając z formularzy składa do Wydziału Informatyzacji stosowne wnioski. Wnioski składane są na okoliczność zatrudnienia, zwolnienia lub zmiany zakresu obowiązków. Co pewien okres czasu Lokalni Administratorzy Systemów Informatycznych porównują rejestr użytkowników systemu ze stanem informacyjnym o pracownikach dostępnym w intranet lub w dziale kadr.*

(akta kontroli str. 396-398, 920-923)

W okresie objętym kontrolą, tj. w latach 2019-2022 (wrzesień), nie upływał okres trwałości żadnego z projektów finansowanych ze środków UE, dotyczących systemów informatycznych do realizacji zadań publicznych.

(akta kontroli str. 399)

Wykorzystywany w Urzędzie system KSAT 2000 I został zakupiony jako aplikacyjne oprogramowanie. Umowy na utrzymanie systemu traktowały ten system jako jeden produkt od którego naliczano jedną opłatę za utrzymanie. System składał się z 20 modułów, tj.:

- Administrator systemów aplikacji,
- Analiza płynności finansowej,

- Centralna kartoteka kontrahentów,
- Centralny rejestr umów,
- Egzekucja,
- Ewidencja,
- Ewidencja kadrowa,
- Ewidencja koncesji alkoholowych,
- Fakturowanie,
- Księga główna,
- Majątek,
- Należności i zobowiązania,
- Organizacja pracy Urzędu,
- Planowanie i monitorowanie budżetu,
- Płace,
- Raportowanie Adhoc,
- Repozytorium systemu,
- Sprawozdawczość budżetowa,
- Podatki,
- System gospodarki nieruchomościami,
- Wieloletnia prognoza finansowa.

Dostawcą systemu KSAT 2000 I był Centralny Ośrodek Informatyki Górniczej wyłoniony w trybie przetargu nieograniczonego. W latach 2019-2022 koszty utrzymania systemu wynosiły, odpowiednio: 209 tys. zł, 250,1 tys. zł, 253,9 tys. zł, 265,7 tys. zł. Na podstawie wydruków zawartości poszczególnych modułów stwierdzono, że wszystkie były wykorzystywane. System nie był rozbudowywany.

(akta kontroli str. 691-692, 935-1216)

2.3. W latach 2019-2022 r., Urząd na nabycie i utrzymanie oprogramowania komputerowego wydatkował, odpowiednio: 3 269,2 tys. zł, 914,3 tys. zł, 1 015,4 tys. zł i 1 113,8 tys. zł. Wydatki poniesione na zakup oprogramowania zostały ujęte w rejestrze wartości niematerialnych i prawnych lub jednorazowo odpisane w koszty w księgach rachunkowych systemu KSAT.

(akta kontroli str. 442-446)

2.4. Urząd określił wymagania bezpieczeństwa środowiska teleinformatycznego w szczegółowym opisie przedmiotu zamówienia do projektu „Centrum Usług Wspólnych[16]". Urząd nie pozyskiwał licencji i oprogramowani dla rozwiązań chmurowych. W pozostałych przypadkach zapisy dotyczące bezpieczeństwa i ochrony danych osobowych były formułowane jako wymagania krytyczne w SIWZ i opisu przedmiotu zamówienia. Do wszystkich umów dołączono stosowne klauzule.

(akta kontroli str. 400-441)

Urząd określił wymagania bezpieczeństwa jakie musiały spełniać duże systemy dziedzinowe. Stosowne zapisy znajdowały się w umowach eksploatacyjnych lub dokumentach zakupu tych systemów. Urząd nie określił jednak wymagań bezpieczeństwa, jakie muszą spełniać aplikacje i pozostałe oprogramowanie (o mniejsze wartości).

(akta kontroli str. 519-544, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: Urząd określał wymagania bezpieczeństwa dla systemów dziedzinowych, jednak nie robił tego w stosunku do oprogramowania drobnego o mniejszej wartości, ponieważ przedmiotowe

[16] Postępowanie WIN.271.7.2017. pn. „Dostawa, instalacja i konfiguracja sprzętu komputerowego oraz oprogramowania na potrzeby realizacji projektów drugie podejście dotyczącym infrastruktury technicznej zamawianej przez Gminę Miasta Tarnowa".

oprogramowanie ma charakter ogólnodostępnych i powszechnych produktów, a więc należy uznać też że bezpiecznych. Jednak mając na uwadze ustalenia kontroli NIK, również w tym przypadku będą dokonywane szczegółowe analizy produktów, w tym zapisów licencyjnych.

(akta kontroli str. 618-623)

2.5. Urząd nie korzystał z SaaS w zakresie obsługi usług związanych z oprogramowaniem dziedzinowym. Posiadał natomiast oprogramowanie SaaS nie związane bezpośrednio z przetwarzaniem danych osobowych. Wykorzystywał je pomocniczo m.in. system wideokonferencji Z., L., T., E., S. Użytkowane w Urzędzie oprogramowanie SaaS nie wykorzystywało baz danych i eksportu danych. Oprogramowanie E. było wykorzystywane do nagrywania sesji Rady Miejskiej i publikowania w BIP. Urząd posiadał również umowę regulującą zasady przetwarzania danych w przypadku S. Brak było odrębnych zasad postępowania z oprogramowaniem SaaS, jak również brak było dokumentów potwierdzających weryfikację dostawcy SaaS.

(akta kontroli str. 395, 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: Urząd wykorzystuje oprogramowanie SaaS tylko dla celów pomocniczych i nie grozi to utratą ciągłości działania, poza oprogramowaniem e-sesja, gdzie podpisano umowę zawierającą zapisy typowe dla SLA. W urzędzie zostaną wprowadzone zasady weryfikacji dostawcy oprogramowania SaaS, jak również zasady postępowania z tym oprogramowaniem.

(akta kontroli str. 618-623)

W przypadku oprogramowania e-sesja wykorzystywane były indywidualne konta dostępowe, a uprawnienia nadawane były przez LASI. Oprogramowanie to wykorzystywało hasła i wymuszało ich okresową zmianę oraz po pewnym okresie bezczynności dokonywało auto rozłączenia. Podobne zasady obowiązywały w pozostałym wykorzystywanym oprogramowaniu SaaS.

(akta kontroli str. 611-617)

Dyrektor Wydziału Informatyzacji wyjaśnił, że: W przypadku oprogramowania SaaS mającego wpływ na ciągłość realizowanych zadań, tj. oprogramowania E., zakup i wdrożenie zostało przeprowadzone w drodze pełnej procedury przetargowej. SIWZ i OPZ zawierały stosowne zapisy odnoszące się do wymagań w zakresie bezpieczeństwa, ciągłości pracy oraz czasu reakcji w zw. z awarią. Pozostałe oprogramowanie SaaS z racji, że ma charakter pomocniczy nie ma formalnie określonych zasad zarządzania nim.

(akta kontroli str. 618-623)

W przypadku oprogramowania SaaS: L., S., E. Urząd posiadał umowy, w ramach których dokonano weryfikacji prawnej dostawców (m.in. w CEIDG i KRS). Zapisy umowy ws. zakupu e-sesja potwierdzały sprawdzenie wiarygodności dostawcy (§ 1 ust. 2 umowy), dostępność umowy SLA (§3 umowy), warunki bezpieczeństwa i przechowywania danych (§2 umowy), politykę tworzenia kopii zapasowych i dostępu do nich (załącznik nr 1 do umowy) oraz spełnienie wymagań RODO i kontroli dostępu (załącznik RODO do umowy). Zapisy umowy ws. zakupu L. potwierdzają sprawdzenie wiarygodności dostawcy (pkt I załącznika do umowy), wymagania bezpieczeństwa (pkt X załącznika do umowy), dostępność umowy SLA (pkt X załącznika do umowy), zasady dostępu do kopii zapasowej (pkt XII załącznika do umowy), zasady RODO oraz kontrolę dostępu (pkt XII załącznika do umowy). Zapisy umowy ws. zakupu smsApi potwierdzały sprawdzenie wiarygodności dostawcy (§1 umowy), zapewnienie

szyfrowania (§2 umowy), dostępność umowy SLA (§5 umowy), spełnienie wymagań RODO oraz kontroli dostępu (załącznik do umowy).

(akta kontroli str. 861-918)

Stwierdzone nieprawidłowości

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

1. Urząd nie posiadał tzw. "białej listy oprogramowania", tj. autoryzowanego bezpiecznego oprogramowania dostępnego do użytku. L.S. wysyłał komunikaty o nowo zainstalowanym oprogramowaniu, jednak z uwagi na niekompletność danych w tym systemie, powiadomienia te nie były efektywnie wykorzystywane (L.S. nie sprawdzał automatycznie autoryzacji oprogramowania). W toku kontroli zidentyfikowano przypadek zainstalowania jednej gry, która była płatnym, komercyjnym oprogramowaniem (data ostatniego uruchomienia 2015 r., komputer z zainstalowaną grą wycofany w styczniu 2022 r.).

   (akta kontroli str. 611-617, 817)

   Niewprowadzenie białej listy oprogramowania NIK ocenia jako działanie nierzetelne, poważnie utrudniające bieżącą kontrolę nad zainstalowanym oprogramowaniem i zarządzanie nim.

   Dyrektor Wydziału Informatyzacji wyjaśnił, że: Urząd wprowadzi standard autoryzowanego oprogramowania na stacjach roboczych, a po uzupełnieniu bazy danych L.S. rozpocznie prowadzenie cyklicznych audytów w tym zakresie.

   (akta kontroli str. 618-623)

2. W Urzędzie nie określono szczegółowych zasad nabywania i wykorzystywania oprogramowania w modelu SaaS. Nie potwierdzono także, że w procesie pozyskiwania tego oprogramowania dokonywana była każdorazowo ocena i weryfikacja spełniania wymagań organizacji, w tym w szczególności:
   - *wiarygodności dostawcy, również pod kątem zapewnienia przez dostawcę wsparcia technicznego (serwisu w wymaganym przez jednostkę czasie) i bezpieczeństwa;*
   - *dostępności SLA;*
   - *spełniania 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 zapasowych, w tym częstotliwości wykonywania kopii i okresu retencji oraz przechowywania,*
   - *spełniania wymagań kontroli dostępu itp.*

   Brak wystarczającej dbałości o potrzeby Urzędu w procesie nabywania oprogramowania w modelu SaaS NIK ocenia jako działanie nierzetelne. W efekcie braku ww. analiz na etapie nabywania oprogramowania nie dochowano należytej staranności w celu zapewnienia, że nabyte oprogramowanie będzie adekwatne do potrzeb jednostki, a także że będzie spełniało niezbędne w jednostce wymagania techniczne i w zakresie bezpieczeństwa.

   (akta kontroli str. 611-617, 818-834)

   Dyrektor Wydziału Informatyzacji wyjaśnił, że: w*eryfikując dostawcę i oceniając bezpieczeństwo zakupionego oprogramowania (poza systemami dziedzinowymi) korzystano z wiedzy ogólnodostępnej. Urząd zwraca uwagę aby systemy SaaS nie*

przetwarzały danych osobowych. Jednak w dostępnym zakresie dodatkowa weryfikacja będzie przeprowadzana. Utrata ciągłości działania oprogramowania SaaS nie jest niebezpieczne dla Urzędu, ponieważ oprogramowanie to nie jest wykorzystywane do świadczenia usług krytycznych i ma charakter jedynie pomocniczy. Stosowane zapisy SIWZ ujmują wymagania w zakresie RODO, obowiązków LASI którzy administrują każdym systemem przypisanym w ramach zakresu czynności. Wykorzystywane systemy dziedzinowe obowiązkowo gromadzą logi transakcyjne a systemy bezpieczeństwa dokumentują ruch na sieci, ruch między węzłami sieci VPN, i analizują oraz raportują sytuacje anormalne. Zostanie wprowadzony mechanizm kontrolny dla pozostałego oprogramowania SaaS (mającego charakter pomocniczy).

(akta kontroli str. 618-623)

3. W Urzędzie brak było zasad weryfikacji zasadności nabywania pozostałego oprogramowania i monitorowania ich licencji (poza dużymi systemami dziedzinowymi) wykorzystywanego przez pracowników Urzędu. Urząd nie posiadał też mechanizmów kontrolnych zapewniających pozyskanie optymalnej liczby licencji pozostałego oprogramowania (poza dużymi systemami dziedzinowymi).

   Zidentyfikowano pojedyncze przypadki oprogramowania (R., S., Z.), gdzie przed dokonaniem zakupu weryfikowano zasadność zakupu i liczbę wystarczających stanowisk. Nie zidentyfikowano natomiast takiej oceny zasadności i liczby licencji w stosunku do pozostałego oprogramowania np. W., T., A., E. itp. Dyrektor Wydziału Informatyzacji przedstawiał Prezydentowi Miasta Tarnowa raporty, które zawierały informacje o stopniu wykorzystania i zapotrzebowaniu na system operacyjny Windows oraz MS office. Raporty te nie miały jednak charakteru audytowego (tylko statystyczny) i nie obejmowały całego wykorzystywanego w Urzędzie oprogramowania.
   NIK ocenia jako nierzetelne nieustalenie procedur weryfikacji zasadności nabywania pozostałego oprogramowania (w tym określenia optymalnej liczby licencji) i ich monitorowania.

   (akta kontroli str. 501-508, 509-518, 611-617)

   Dyrektor Wydziału Informatyzacji wyjaśnił, że: Urząd posiada procedury i faktycznie analizuje zasadność nabycia i liczbę licencji jeśli chodzi o duże oprogramowanie dziedzinowe i inne kupowane w trybie ustawy Prawo zamówień publicznych, ale również weryfikuje zasadność i liczbę nabywania oprogramowania biurowego MS Office, jak również Windows (to komórki merytoryczne oceniają i wnioskują o zakup jeśli jest taka potrzeba - a Dyrektor Wydziału Informatyzacji sporządza na koniec roku statystykę z tego oprogramowania i załącza do raportu prezentowanego Prezydentowi Miasta Tarnowa). Brak jest faktycznie szczegółowych regulacji dotyczących zasadności nabywania pozostałego oprogramowania (o mniejszej wartości) i procedur monitorowania ich licencji. Takie procedury zostaną wprowadzone. Przygotowane projekty zakupu licencji systemów dziedzinowych oraz oprogramowania MS Office, na etapie ustalania SIWZ, funkcjonalności, w uzasadnionych przypadkach, są konsultowane z wydziałem merytorycznym np. Wydział Infrastruktury Miejskiej (...) , Wydział Edukacji (...) , Wydział Księgowości (...). Projektowane i składane wnioski zakupowe są kontrolowane i zatwierdzane przez Zespół Zamówień Publicznych. Równocześnie dokumenty zakupowe podlegają kontroli prawnej prowadzonej przez radców prawnych UM. Urząd nie kupuje licencji nadmiarowych. Uzupełniane są jedynie ilości licencji niezbędnych w ramach wymiany tych , które utraciły aktualność technologiczną.

   Dyrektor Wydziału Informatyzacji dodał, że: w Urzędzie zostaną wprowadzone procedury kontrolne zapewniające pozyskiwanie optymalnej liczby licencji.

   (akta kontroli str. 618-623)

OCENA CZĄSTKOWA

Sposób wykorzystania oprogramowania nie był optymalny w odniesieniu do wydatków poniesionych na jego nabycie, co NIK ocenia negatywnie.
W Urzędzie nie wprowadzono standardu autoryzowanego oprogramowania na stacjach roboczych (tzw. „białej listy oprogramowania"). Nie określono również szczegółowych zasad nabywania i wykorzystywania oprogramowania w modelu SaaS. Nie potwierdzono także, że w procesie pozyskiwania tego oprogramowania dokonywana była każdorazowo ocena i weryfikacja spełniania wymagań Urzędu, w tym potrzeby ich nabycia, co stwarzało ryzyko poniesienia zbędnych wydatków związanych z zakupem i utrzymaniem oprogramowania. Nie w pełni wykorzystywano możliwości L.S., który zakupiono w 2015 r. za 165 tys. zł, a na jego wsparcie w latach 2019-2022 wydatkowano 76,2 tys. zł.

IV. Uwagi i wnioski

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

Wnioski

1. Określenie i wprowadzenie szczegółowych zasad zarządzania oprogramowaniem (licencjami).
2. Wprowadzenie rozwiązań organizacyjnych i technicznych zapewniających kompletność danych o posiadanym oprogramowaniu, w tym podjęcie działań zapewniających optymalne wykorzystanie posiadanych narzędzi informatycznych.
3. Objęcie monitorowaniem całego oprogramowania, dokumentowanie podejmowanych czynności, w tym działań naprawczych.
4. Zweryfikowanie zasadności przyznania uprawnień administratora użytkownikom końcowych stacji roboczych.
5. Wprowadzenie procedur potwierdzania usunięcie danych z dysków sprzętu IT przekazywanego innym jednostkom organizacyjnym.
6. Wprowadzenie mechanizmów kontrolnych zapewniających bieżącą i okresową weryfikację kompletności i legalności instalowanego w Urzędzie oprogramowania.
7. Określenie i wdrożenie szczegółowych zasad nabywania i wykorzystywania oprogramowania w modelu SaaS.
8. Opracowanie procedur umożliwiających ocenę zasadności nabywanego oprogramowania, w tym określenia ich optymalnej liczby.
9. Rozważenie zwiększenia liczby zatrudnionych wykwalifikowanych pracowników w Wydziale Informatyzacji z uwagi na strategiczny charakter wykonywanych zadań.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Krakowie. Prawo zgłaszania zastrzeżeń, zgodnie

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.
W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Kraków, 28 października 2022 r.

Kontroler
/-/
Mariusz Pindral
główny specjalista kontroli państwowej

Dyrektor
Delegatury Najwyższej Izby Kontroli
w Krakowie
/-/
Jolanta Stawska

Zmian w wystąpieniu pokontrolnym dokonał: