NAJWYŻSZA IZBA KONTROLI

Delegatura w Bydgoszczy

LBY.410.016.03.2022

Pan
Michał Zaleski
Prezydent Miasta Torunia
Urząd Miasta Torunia
ul. Wały gen. Wł. Sikorskiego 8
87-100 Toruń

WYSTĄPIENIE POKONTROLNE

zmienione zgodnie z treścią uchwały nr KPK-KPO.443.201.2022 z 10 stycznia 2023 r.

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Bydgoszczy
ul. Wały Jagiellońskie 12, 85-950 Bydgoszcz
T +48 52 567 58 00, F +48 52 567 58 60
lby@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Urząd Miasta Torunia, ul. Wały gen. Wł. Sikorskiego 8, 87-100 Toruń[1],

Kierownik jednostki kontrolowanej

Michał Zaleski, Prezydent Miasta Torunia[2], od 18 listopada 2002 r.

Zakres przedmiotowy kontroli

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym.
2. Optymalizacja wykorzystania oprogramowania oraz wydatków związanych z jego nabyciem i użytkowaniem.

Okres objęty kontrolą

Lata 2019-2022 do dnia zakończenia kontroli[3], 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[4]

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy

Kontrolerzy

1. Elżbieta Warda-Fereniec, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/116/2022 z 1 lipca 2022 r.
2. Karol Sobieszczyk, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LBY/131/2022 z 31 sierpnia 2022 r.

(akta kontroli str. 1-3)

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli negatywnie ocenia proces postępowania z posiadanym przez Urząd oprogramowaniem.

W Urzędzie nie posiadano pełnej i rzetelnej wiedzy na temat wykorzystywanego oprogramowania, ponieważ prowadzona ewidencja nie zbierała danych w trybie rzeczywistym i ciągłym na zasobach, a ponadto nie monitorowano w niej terminów ważności licencji. Nie prowadzono czasowych (w zaplanowanych odstępach) przeglądów oprogramowania i licencji mających na celu potwierdzenie aktualności oraz kompletności ich spisu. Ponadto nie zatrudniono audytora wewnętrznego i nie prowadzono w latach 2020-2022 audytów wewnętrznych, pomimo takiego obowiązku określonego w ustawie o finansach publicznych[6].

NIK zauważa, że w Urzędzie nie dokonywano systematycznej analizy funkcjonalności i efektywności posiadanego oprogramowania. W toku kontroli stwierdzono przypadki instalacji oprogramowania EOL (end of life)[7], a także korzystnie ze starych wersji

[1] Dalej: „Urząd" lub „UMT".
[2] Dalej: „Prezydent".
[3] Tj. 26 października 2022 r.
[4] Dz. U. z 2022 r. poz. 623, dalej: „ustawa o NIK".
[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[6] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r., poz. 1634), dalej: „ustawa o finansach publicznych"..
[7] Czyli takie oprogramowanie, które zostało oficjalnie wycofane ze względu na luki w bezpieczeństwie.

oprogramowania, w tym krytycznych oraz aplikacji niezwiązanych z realizacją obowiązków służbowych.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym

Opis stanu faktycznego

1.1. Zgodnie z regulaminem organizacyjnym Urzędu, będącym załącznikiem do zarządzenia Prezydenta[9], zadaniami realizowanymi od 1 listopada 2017 r. przez Biuro Projektów Informatycznych[10], była: informatyzacja Urzędu, wykonywanie prac programistycznych, prowadzenie działań w zakresie strategii rozwoju usług informatycznych. Nadzór nad BPI przypisany został Sekretarzowi Miasta, do którego zadań należało nadzorowanie działalności i koordynacja prac Biura.

W wewnętrznej strukturze organizacyjnej oraz szczegółowym zakresie działania BPI, stanowiącej załącznik nr 1 do zarządzenia Prezydenta nr 329 z 6 listopada 2017 r. i nr 356 z 5 grudnia 2017 r. określono, że do zadań Biura należało w szczególności: prowadzenie działań związanych z rozwojem systemów dziedzinowych, prowadzenie analiz związanych z oceną potrzeb dot. zakupów oraz systemów niezbędnych do prawidłowego funkcjonowania tych systemów , koordynowanie zakupów , prowadzenie wdrożeń związanych z uruchomieniem nowych systemów, modułów, funkcjonalności, projektowanie i tworzenie własnych aplikacji na potrzeby Urzędu.

Z dniem 1 października 2020 r. zarządzeniem Prezydenta nr 206 ustalono nową strukturę organizacji i szczegółowy zakres działania BPI zgodnie z którą zadania Biura miały być realizowane poprzez przydzielone 10,5 etatu, z tego: w Referacie Sieci Światłowodowej i Systemów Telekomunikacyjnych[11] – 3,5 etatu, w zespole ds. wsparcia – dwa etaty, czterech pracowników na stanowiskach urzędniczych i dyrektor. Do zadań Biura należało m.in:

- administrowanie i utrzymanie sieci IP, nadzór nad siecią IP/MPLS w tym łączy pomiędzy lokalizacjami Urzędu, udział we wdrażaniu nowych systemów teleinformatycznych, pozyskiwanie funduszy z Unii Europejskiej na realizację projektów informatycznych (Referat);

- zakup sprzętu, oprogramowania biurowego oraz zapewnienie sprawności technicznej urządzeń, administrowanie, nadzorowanie eksploatacji, zapewnienie serwisu i asysty technicznej wdrożonych systemów informatycznych, w tym kompleksowo systemu OTAGO.

(akta kontroli str. 13-85)

W Urzędzie nie było sformalizowanej procedury dotyczącej zarządzania oprogramowaniem komputerowym. Według opinii, powołanego przez NIK, biegłego brak ustanowionych zasad zarządzania licencjami, które obejmowałyby wszystkie kwestie i wymagane czynności niezbędne do zarządzania i nadzoru nad całym cyklem życia oprogramowania, nieobjęcie kontroli w czasie rzeczywistym nad instalowaniem i wykorzystywaniem oprogramowania na wszystkich urządzeniach, w tym smartfonów/tabletów oraz brak zidentyfikowanych innych skutecznych mechanizmów

[8] 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.

[9] Zarządzenie nr 378 z dnia 30 października 2013 r. zmienione 11 zarządzeniami Prezydenta: nr 254 z dnia 18 września 2017 r., nr 319 z dnia 31 października 2017 r., nr 202 z dnia 28 września 2020 r., nr 205 z 15 czerwca 2018 r., nr 51 z 6 marca 2017 r., nr 329 z 6 listopada 2017 r., nr 356 z 5 grudnia 2017 r., nr: 202 i 206 z 28 września 2020 r., nr 86 z 14 kwietnia 2021 r. i nr 89 z 21 marca 2022 r.

[10] Dalej: „BPI" lub „Biuro".

[11] Dalej: „RSŚST" lub „Referat".

kontrolnych w tym zakresie (np. okresowe przeglądy), nie zapewniał skutecznego nadzoru nad instalowanym i wykorzystywanym oprogramowaniem.

(akta kontroli str. 568-585)

Prezydent wyjaśnił, że w Urzędzie nie ma takiej procedury, jednakże w zakresie zakupu licencji przestrzegane są zasady dotyczące udzielania zamówień publicznych uregulowane w zarządzeniu Prezydenta Nr 247 z 22 września 2021 r., a zasady wdrażania i użytkowania oprogramowania opisane są w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

(akta kontroli str. 133-142)

1.2. W latach 2019-2021 w Urzędzie zostały przeprowadzone trzy audyty wewnętrzne. Dwa przeprowadzono na podstawie rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[12] z raportami stanu na dzień 18 grudnia 2020 r. i 17 grudnia 2021 r. Rekomendacje poaudytowe obejmowały:

- wprowadzenie informatycznego systemu do nadawania i przechowywania uprawnień do systemów informatycznych w oparciu o kartę obiegową;

- przygotowanie koncepcji utworzenia serwerowni głównej i zapasowej dla kluczowych zasobów;

- wdrożenie systemu rejestrowania wykonywanych czynności administracyjnych.

Prezydent podał, że rekomendacje te są w trakcie realizacji.

Audytor wewnętrzny Urzędu przeprowadził w 2019 r. zadanie zapewniające ujęte w planie audytu na ten rok pn. „*Ocena bezpieczeństwa teleinformatycznego w Urzędzie Miasta Torunia (wybrane aspekty)*. W sprawozdaniu z tego zadnia sformułował dwie rekomendacje dotyczące:

- podejmowania działań zapewniających, żeby osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia i uczestniczyły w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji; bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań tych osób;

- ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, tak aby w rocznym planie sprawdzeń na rok 2020 Inspektor Ochrony Danych Osobowych[13] zaplanował audyt zgodności przetwarzanych informacji pod kątem ochrony danych osobowych w Urzędzie z wykorzystaniem przenośnego sprzętu komputerowego oraz zalecił formalne dostosowanie wewnętrznie obowiązujących instrukcji, zgodnie z obowiązującym nazewnictwem i zmieniającym się wewnętrznie środowiskiem organizacyjnym.

Audytor opracował *Plan audytu wewnętrznego na rok 2020*, w którym zaplanował wykonanie *Audytu bezpieczeństwa informacji*, jednakże audyt ten nie został wykonany, gdyż audytor zakończył pracę w Urzędzie 31 stycznia 2020 r., a na jego miejsce nie zatrudniono następcy. Szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 87-103, 133-143, 525-539, 655)

W badanym okresie, w BPI zatrudnionych było od 10 do 11 pracowników[14]. W okresie tym przeprowadzono cztery procedury naboru na stanowiska związane z obsługą informatyczną Urzędu, w tym trzy nabory zewnętrzne i jeden wewnętrzny. Fluktuacja

[12] Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. Dz. U. 2017 r. poz. 2247.
[13] Dalej: „IOD".
[14] W etatach od 9,5 do 10.

kadr w komórce tej wynikała ze zwolnienia pracowników jak i z przejścia na emeryturę. Wszyscy pracownicy posiadali zakresy obowiązków. Zadania dotyczące zarządzania licencjami przypisano trzem pracownikom, natomiast za efektywność wykorzystania licencji odpowiadało dwóch pracowników.

W badanym okresie (2019-2022 do 27 września) pracownicy BPI odbyli 28 szkoleń, kursów z zakresu informatycznego, w tym jedno szkolenie dotyczące zakresu spraw związanych z licencjami[15].

(akta kontroli str. 133-141, 656-657)

W Urzędzie prowadzono spis licencji i oprogramowania w oparciu o plik Excela i z pomocą dedykowanego programu typu *inventory tool*, a zestawienie subskrypcji i asyst technicznych prowadził pracownik BPI odpowiedzialny za zakupy. BPI prowadziło ewidencję instalowanego oprogramowania dla wszystkich komórek organizacyjnych. Program ewidencjonował sprzęt komputerowy będący w posiadaniu Urzędu wraz z zainstalowanym na nim oprogramowaniem. Umożliwiał identyfikację użytkownika danego sprzętu komputerowego, korzystającego z danej licencji oraz wskazywał miejsce instalacji oprogramowania.

Prowadzona przez Urząd ewidencja oprogramowania/licencji w tym systemie nie była jednak kompletna, tj. nie zawierała wszystkich danych o użytkowanym oprogramowaniu i licencjach lub zawierała programy niebędące już w posiadaniu Urzędu. Ponadto pomimo, że system ten posiadał wiele funkcjonalności, nie wykorzystywano jego możliwości, tj. nie zbierano danych w trybie rzeczywistym i ciągłym na zasobach, nie monitorowano stanu użycia i legalności licencji, nie wykonywano cyklicznych przeglądów licencji w celu określenia poziomu ich wykorzystania (w tym daty ważności - szczególnie w przypadkach czasowych subskrypcji) co opisano w sekcji *Stwierdzone nieprawidłowości*.

Inventory tool zostało nabyte przez Urząd w 2013 r. za cenę 64,0 tys. zł. W latach 2019-2021 zawarto z wykonawcą tego oprogramowania trzy umowy na przedłużenie i wsparcie techniczne dla licencji na łączną kwotę 47,4 tys. zł, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 326-334, 339-378, 568-585, 659-667, 675-710)

W Urzędzie nie zapewniono rozwiązań technicznych umożliwiających skuteczne i rzeczywiste zarządzanie posiadanymi zasobami, takimi jak urządzenia mobilne typu smartfon czy tablet, co szczegółowo przedstawiono w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 339-378, 568-585, 667)

Badanie dziesięciu zmian pracowników na stanowiskach pracy wykazało, że we wszystkich przypadkach licencje przypisane były do komputerów przez nich użytkowanych. Z tego w czterech przypadkach nie nastąpiły zmiany dotyczące użytkowania licencji przez danego pracownika, ponieważ zmieniał on komórkę organizacyjną Urzędu przechodząc do niej wraz z dotychczas użytkowanym komputerem. W czerech kolejnych przypadkach nie odnotowano zmian dotyczących licencji, ponieważ komputery, na których były zainstalowane przydzielono innym pracownikom. Natomiast w dwóch przypadkach zwolniono licencje[16] wycofane z użycia typu OEM[17], w okresie od półtora roku do dwóch lat, od dnia w którym ci pracownicy przestali użytkować komputery, na których były one zainstalowane.

(akta kontroli str. 540-557, 668-669)

[15] Szkolenie on-line "Licencje na oprogramowanie" przeprowadzone w 2022 r.
[16] W obu przypadkach dotyczyło to oprogramowania MS Office 2007 Basic.
[17] Licencje były przypisane do danego urządzenia.

Dyrektor BPI wyjaśnił, że ww. licencje przeznaczone były do likwidacji. W związku z tym, że proces wycofywania z eksploatacji komputerów odbywa się w większych partiach, są one gromadzone w magazynie sprzętu przeznaczonego do likwidacji i likwidowane zbiorczo.

(akta kontroli str. 757-760)

Badanie trzynastu wybranych licencji wykazało, że wszystkie posiadły dokumenty zakupu[18] wystawione na Urząd lub Gminę Miasto Toruń. Kontrola przechowywania i zabezpieczenia tych licencji wykazała, że nośniki/pliki instalacyjne dla nich (wersje pudełkowe umożliwiające instalację oprogramowania na różnych urządzeniach, wersje plastikowe – karty z kluczem) przechowywane były w zabezpieczonym w system dostępu pomieszczeniu, do którego wstęp posiadali wyłączne upoważnieni pracownicy BPI. Licencje elektroniczne przechowywane były na portalach producentów oprogramowania. Natomiast dla licencji bez kluczy w Urzędzie posiadano certyfikaty legalnego nabycia oprogramowania.

(akta kontroli str. 670-674)

W Urzędzie w badanym okresie korzystano z jednego oprogramowania pod nazwą AutoSMS, stworzonego przez jednego z pracowników Urzędu. Oprogramowanie to wykonane zostało przez Dyrektora BPI w ramach stosunku pracy, dlatego nie poniesiono z tego tytułu żadnych dodatkowych kosztów. Oprogramowanie uruchomione w 2021 r. zainstalowane było na komputerach Wydziału Obsługi Mieszkańców[19] oraz serwerze Web[20]. Oprogramowanie służyło do dokonywało rezerwacji miejsc dla mieszkańców w WOM, w sprawach związanych z rejestracją pojazdów. Kody/klucze źródłowe do tego oprogramowania przechowywane były na zasobie sieciowym – dysku sieciowym BPI.

(akta kontroli str. 133-143, 560-564, 715)

Prowadzony w Urzędzie spis/wykaz oprogramowania/licencji pozwalał na identyfikację liczby wykorzystywanych/wolnych licencji.

Z raportu BPI z 29 września 2022 r. wynikało, że posiadano 1599 licencji w tym 178 (11,1%) z nich nie były wykorzystywane. Dotyczyło to: 166 licencji MS Windows[21], sześciu licencji vSphere 6 Essentials, trzech licencji vSAN 6, dwóch licencji MS Office 21 Standard i jednej MS Project Professional 2010.

Dyrektor BPI wyjaśnił, że posiadanie 166 wolnych licencji MS Windows wynikało z sukcesywnej wymiany sprzętu komputerowego na nowy. Zwolnione licencje, które zakupione zostały w latach 2015-2016, służyły do użytkowania starszego sprzętu a obecnie nie mogą być wykorzystywane ze względu na brak wsparcia ze strony Microsoftu.

Z analizy ww. zestawienia wolnych licencji i zestawienia zakupionych licencji w latach 2019-2022 (do dnia 2 sierpnia 2022 r.) wynikało, że nie kupowano licencji, które już posiadano i z nich nie korzystano (wykazywano je jako wolne).

(akta kontroli str. 675-710, 714)

1.3. Dyrektor BPI wyjaśnił, że zasady akceptowalnego użycia służbowych zasobów IT określone zostały w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych[22] i nie uwzględniono w nich potrzeby tworzenia nowego dokumentu w tym zakresie, poza tymi zawartymi w tej Polityce.

---

[18] Faktury i umowy.
[19] Dalej: „WOM".
[20] Moduł obsługujący zgłoszenia telefoniczne.
[21] W tym: 114 MS Windows 10 Professional MPSA, 52 MS Windows 10 Professional SELECT.
[22] Dalej: „Polityka bezpieczeństwa".

Polityka ta wprowadzona zarządzeniem Prezydenta Nr 252 z 5 listopada 2020 r. zawierała m.in. trzy załączniki: (1) Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie, (2) Instrukcję bezpiecznego przetwarzania danych w Urzędzie, (3) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie.

W Instrukcji bezpiecznego przetwarzania danych w Urzędzie zawarto zapisy o tym, że zabrania się: (1) próbom omijania wewnętrznych i zewnętrznych barier bezpieczeństwa informacji, w szczególności odpinania urządzeń od domeny, deinstalowania programów antywirusowych, instalowania systemów operacyjnych bez zgody Służb IT; (2) kupowania oprogramowania oraz wdrażania innych usług związanych z systemami informatycznymi bez wiedzy i zgody Służb IT; (3) przechowywania prywatnych plików na dyskach sieciowych (np. serwerze plików); (4) podłączania zewnętrznych/prywatnych urządzeń IT (komputerów, notebooków, telefonów komórkowych, tabletów, dysków przenośnych, pendrive'ów itd.) bez stosownej zgody służb IT.

Natomiast w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie zawarto zapisy o tym, że w celu zabezpieczenia systemu informatycznego przed niepożądanym działaniem niebezpiecznego oprogramowania pracownikom zabrania się: (1) instalowania i uruchamiania bez zgody Służb IT jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Urzędzie; (2) podłączania bez ich zgody IT urządzeń (np. komputerów, urządzeń bezprzewodowych itd.) do systemu informatycznego; (3) połączenia z siecią publiczną z pominięciem systemu zabezpieczeń uruchomionego w Urzędzie; (4) samodzielnego przeprowadzania jakichkolwiek zmian oprogramowania i jego konfiguracji, które miałyby wpływ na bezpieczeństwo systemu informatycznego.

Dyrektor BPI wyjaśnił, że w celu zapewnienia przestrzegania powyższych zasad użytkownicy nie posiadają uprawnień do systemów operacyjnych pozwalających na samodzielne instalowanie oprogramowania.

Z Polityki Bezpieczeństwa wynikało także, że Administrator Systemów Informatycznych odpowiadał za: (1) Instalację i konfigurację oprogramowania na poszczególnych urządzeniach służących przetwarzaniu danych; (2) dokonywanie nie rzadziej niż raz do roku weryfikacji w zakresie zgodności z przepisami prawa oraz przyjętymi regulacjami zainstalowanego oprogramowania na stacjach roboczych poszczególnych użytkowników (i sporządzenie raportu).

Ponadto w Polityce Bezpieczeństwa zawarto zasady, iż: (1) każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami dotyczącymi ochrony danych osobowych; (2) korzystania z wyposażenia informatycznego oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków służbowych lub czynności zleconych przez Urząd; (3) wykorzystywania jedynie legalnego oprogramowania dostarczonego przez Urząd; (4) należytej dbałości o wyposażenie informatyczne i oprogramowanie.

Dyrektor BPI wyjaśnił, że każda z osób po przejściu szkolenia potwierdza jego fakt podpisem, zobowiązując się jednocześnie do oświadczenia o zachowaniu poufności wraz z potwierdzeniem odbycia szkolenia z ochrony danych osobowych.

(akta kontroli str. 264-304, 339-349)

W Urzędzie natomiast nie było sformalizowanej procedury dotyczącej zarządzania oprogramowaniem komputerowym. Ustanowione w Urzędzie zasady nie uwzględniały wszystkich etapów życia oprogramowania, w tym zasad monitorowania i nadzoru nad stanem użycia i legalności, w tym na urządzeniach typu smartfon/tablet,

konieczności weryfikacji pod kątem bezpieczeństwa nabywanych licencji, w tym również w modelu SaaS[23] oraz dopuszczania do instalacji programów darmowych, przechowywania i zabezpieczania kluczy instalacyjnych, ewidencjonowania posiadanych i używanych licencji, wycofywania/odinstalowywania licencjonowanego oprogramowania, odniesienia do zmian licencyjnych, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 264-304, 339-349, 568-654)

W badanym okresie w Urzędzie nie prowadzono czasowych (w zaplanowanych odstępach), przeglądów oprogramowania i licencji mających na celu potwierdzenie, że posiada on aktualny, kompletny ich spis oraz że posiada licencje na każde zainstalowane oprogramowanie, co było niezgodne z zapisami Polityki Bezpieczeństwa. Skutkiem tego było nieprawidłowe postępowanie z oprogramowaniem, co przedstawiono w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 339-349)

Dyrektor BPI wyjaśnił, że w 2018 r. wdrożono w Urzędzie usługę katalogową Microsoft Active Directory, która pozwala na centralne zarządzanie uprawnieniami, zdalną instalację oprogramowania. W ramach wewnętrznej polityki bezpieczeństwa przetwarzania danych użytkownicy nie posiadają uprawnień umożliwiających samodzielną instalację oprogramowania. Instalacji oprogramowania dokonują pracownicy BPI oraz firmy współpracujące w ramach umów o wsparcie techniczne. Weryfikacja zainstalowanego oprogramowania realizowana jest przy użyciu oprogramowania *inventory tool*, które pozwala na uzyskanie informacji o zainstalowanym oprogramowaniu. Sprawdzanie legalności oprogramowania jest również przeprowadzane przez pracowników BPI w przypadku prac mających na celu reinstalację lub upgrade systemu operacyjnego przed przyłączeniem do domeny

(akta kontroli str. 339-349)

W badanym okresie BPI nie posiadało zidentyfikowanych i wykrytych nieprawidłowości dotyczących oprogramowania a Urząd nie poniósł kar w związku z nielegalnym lub nieprawnie użytkowanym oprogramowaniem.

(akta kontroli str. 736-739)

W latach 2019-2022:

- przekazano 165 szt. sprzętu wraz z oprogramowaniem. We wszystkich przypadkach dotyczyło to oprogramowania – systemu operacyjnego Windows (pakietów biurowych) oraz przekazał jedno oprogramowanie Boardmaker&speaking, The Grid 2, Ivona Reader, uczestnikom projektu „Internet – świ@t w Twoim domu" na podstawie umów darowizny bądź sprzedaży, zgodnie z zarządzeniem Prezydenta nr 93 z dnia 28 kwietnia 2021 r.

- zlikwidowano 208 szt. sprzętu, w tym 101 szt. komputerów, które posiadały oprogramowanie. Oprogramowanie to zostało usunięte za pomocą urządzenia Degausser - służącego do trwałego i skutecznego niszczenia danych z nośników magnetycznych.

Kontrola 10 wybranych programów wykazała, że zastosowane mechanizmu usuwania danych ze sprzętu były realizowane w sposób skuteczny. Ze względu na likwidację

[23] SaaS - Oprogramowanie jako usługa (Software as a Service) to model udostępniania oprogramowania w chmurze, w którym dostawca chmury rozwija i utrzymuje aplikacje chmurowe, zapewnia ich automatyczne aktualizacje i udostępnia oprogramowanie swoim klientom za pośrednictwem Internetu na zasadzie „pay-as-you-go", czyli w zależności od wykorzystania zasobów.

sprzętu dyski po zdemontowaniu z komputerów zostały usunięte, rozmagnesowane a następnie przekazane do likwidacji.

(akta kontroli str. 740)

1.4. Badanie 10 wybranych licencji wykazało, że wszystkie były bezterminowe (wieczyste). Liczba możliwych instalacji zawierała się od jednej do 141. Natomiast łączna liczba możliwych dostępów do ich zainstalowania wynosiła 277, z tego faktycznie wykorzystanych było 275. Wszystkie badane licencje wykorzystane były zgodnie z umowami i warunkami tych licencji.

(akta kontroli str. 742-743)

Stwierdzone nieprawidłowości

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

1. Niezatrudnienie audytora wewnętrznego.

W Urzędzie od 1 lutego 2020 r. do czasu zakończenia kontroli (ponad dwa i pół roku) nie był zatrudniony audytor wewnętrzny, co było niezgodne z art. 274 ust. 3 ustawy o finansach publicznych.[24]

Prezydent wyjaśnił m.in., że w okresie epidemii i stanu zagrożenia epidemicznego covid-19, z uwagi na obostrzenia sanitarne, wynikające w szczególności ze zmian przepisów prawa w zakresie ograniczenia wykonywania zadań przez urzędy administracji publicznej do wykonywania wyłączeń niezbędnych do zapewnienia pomocy obywatelom, zalecenia pracy zdalnej oraz zaleceń ograniczenia bezpośrednich spotkań służbowych, w których uczestniczy wiele osób, nabory do Urzędu były przeprowadzane w ograniczonym zakresie. Ponieważ procedura naboru pracowników wiąże się z bezpośrednim, osobistym kontaktem członków komisji z kandydatami z zewnątrz – od początku 2020 r. do końca kwietnia 2021 r., tj. w szczytowym czasie pandemii nie prowadzono żadnego naboru zewnętrznego.

(akta kontroli str. 87-103, 133-143, 525-539, 655, 658)

NIK zauważa, że poprzez brak zatrudnienia audytora wewnętrznego pozbawiono Prezydenta wsparcia w realizacji celów i zadań przez systematyczną, niezależną i obiektywną ocenę kontroli zarządczej oraz czynności doradcze. W szczególności w roku 2020 nie zrealizowano planu audytu, zgodnie z którym miał zostać przeprowadzony m.in. audyt bezpieczeństwa informacji.

2. Nierzetelne prowadzenie ewidencji/wykazu oprogramowania i licencji.

Ewidencja ta:

a) nie zawierała kompletnych danych o użytkowanych oprogramowaniach i licencjach. W zestawieniu/ewidencji oprogramowania/licencji na dzień 30 sierpnia 2022 r. nie wykazano dwóch programów (w tym jednego używanego przez IOD). Ponadto przekazane zestawienie nie było spójne z zestawieniem zakupów. Np. jedno oprogramowanie w wykazie licencji Urzędu zostało oznaczone jako „licencja czasowa 24.03.2020-24.03.2021", natomiast w zestawieniu zakupów licencji i oprogramowania oznaczone jako „licencja wieczysta".

(akta kontroli str. 132-142, 364-378, 560-564, 568-585, 667, 675-713)

[24] W latach 2020-2022 ujmowano w planie finansowym dochody budżetu miasta w wysokości odpowiednio: 1 399,6 mln zł, 1 352,2 mln zł i 1 332,8 mln zł, czyli kwoty, które obligowały do prowadzenia audytu wewnętrznego. Na stronie internetowej Urzędu do dnia 8 września 2022 r. widniała informacja, że: *Z audytorem wewnętrznym można kontaktować się tylko za pomocą środków komunikacji elektronicznej, telefonów i poczty, bezpośrednia obsługa interesantów tylko po wcześniejszym umówieniu się na konkretny termin*. Dopiero 21 września 2022 r. ukazała się na stronie internetowej Urzędu informacja: *Wakat na stanowisku*. W Urzędzie rozpoczęto nabory na stanowiska urzędnicze po przerwie trwającej od 13 listopada 2019 r. do 4 maja 2021 r., jednak nie ogłoszono naboru na stanowisko audytora wewnętrznego. Dopiero we wrześniu 2022 r. ukazało się ogłoszenie o takim naborze..

b) nie zbierała danych w trybie rzeczywistym i ciągłym na zasobach, tj. nie monitorowała stanu użycia i legalności licencji poprzez wykonywanie cyklicznych przeglądów licencji (określenie cyklu, monitorowanie poziomu wykorzystania i daty ważności - szczególnie w przypadkach czasowych subskrypcji, wymagany sposób i elementy raportowania).

W Urzędzie zakupiono narzędzie *inventory tool* w 2013 r. za kwotę 64,0 tys. zł i wydano, w latach 2019-2021, na przedłużenie umowy i wsparcie techniczne 47,4 tys. zł. Pomimo, że istniały możliwości programowe, nie były one wykorzystywane. Tym samym posiadając profesjonalne narzędzie prowadzono ewidencję w pliku Excel.

(akta kontroli str. 132-142, 364-378, 560-564, 568-585, 667, 675-713)

Dyrektor BPI wyjaśnił, iż dwóch oprogramowań nie wykazano w wykazie licencji omyłkowo pomimo, że je posiadano. Jednocześnie podał, iż zakupiona licencja na użytkowanie oprogramowania do zdalnego dostępu była licencją czasową zakupioną na rok użytkowania od dnia zakupu. Zapis w zestawieniu licencji był zapisem prawidłowym a w zestawieniu zakupów był błędny.

Zastępca Prezydenta wyjaśnił, że ewidencja posiadanego oprogramowania prowadzona była w oparciu o plik Excela, który na bieżąco był aktualizowany przez pracowników BPI w przypadku pozyskania lub wygaszenia oprogramowania. Podstawowym źródłem informacji w tym zakresie stanowił ten plik. Audyty oprogramowania w tym zakresie były uruchamiane ręcznie i porównywane z bazą licencji prowadzoną w pliku Excel. Nie wszystkie posiadane przez UMT licencje były skatalogowane w systemie *inventory tool*. W związku z powyższym proces wykorzystania licencji realizowany był w oparciu o plik Excel oraz o ten program poprzez prowadzenie analiz porównawczych.

(akta kontroli str. 675-713, 744-749)

3. Brak w Urzędzie technicznych rozwiązań służących do monitoringu zainstalowanego oprogramowania na urządzeniach typu smartfon, tablet.

W Urzędzie nie prowadzono monitoringu zainstalowanego oprogramowania na urządzeniach typu smartfon czy tablet, w związku z czym nie prowadzono nadzoru i nie posiadano wiedzy o zainstalowanym na tych urządzeniach oprogramowaniu, w tym nieautoryzowanym.

Zgodnie z Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych[25], w części II A15 standardem kontroli zarządczej dla sektora finansów publicznych - Mechanizmy kontroli dotyczące systemów informatycznych – w Urzędzie, jako jednostce sektora finansów publicznych, powinno się określić mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych.

(akta kontroli str. 568-585, 744-749)

Zastępca Prezydenta wyjaśnił, że Urząd nie posiada oprogramowania oraz nie korzysta z usług operatora w zakresie umożliwiającym śledzenie aparatów telefonicznych wraz z pozyskiwaniem informacji o zainstalowanym oprogramowaniu. Zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, użytkownik danego sprzętu nie może dokonywać samodzielnego przeprowadzania jakichkolwiek zamian oprogramowania i jego konfiguracji mającego wpływ na bezpieczeństwo systemu.

[25] Dz. Urz. Min. Fin. Nr 15 poz. 84.

Telefony komórkowe przekazywane są ze standardową konfiguracją operatora świadczącego usługę.

(akta kontroli str. 744-749)

NIK zauważa, że brak szczegółowych regulacji dotyczących monitorowania urządzeń mobilnych (dotyczących np. częstotliwości weryfikacji legalności oprogramowania instalowanego na tych urządzeniach), skutkował brakiem nadzoru nad oprogramowaniem zainstalowanym na tego typu urządzeniach.

4. Nieuwzględnienie w ustanowionej w Urzędzie procedurze w szczególności zasad dotyczących:
- monitorowania i nadzoru nad stanem użycia i legalności oprogramowania oraz nadzoru nad realizacją procedury związanej z zarządzaniem licencjami, w tym na urządzeniach typu smartfony/tablety;

- zakresu konieczności weryfikacji pod kątem wymagań bezpieczeństwa w ramach nabywania licencji, w tym oprogramowania w modelu SaaS oraz zasad dopuszczania programów do instalacji, np. darmowych;

- przechowywania i zabezpieczania dostępu do nośników instalacyjnych, w tym kluczy licencyjnych i innych dokumentów licencyjnych, w tym utrzymywanych w środowiskach chmurowych;

- zasad ewidencjonowania wszystkich posiadanych licencji, w tym oprogramowania w modelu SaaS, w taki sposób, aby spis zapewniał dostępność aktualnych informacji na temat liczby posiadanych oraz wykorzystywanych licencji dla osób odpowiedzialnych za instalację;

- wycofywania/odinstalowywania (z uwzględnieniem wszystkich rodzajów urządzeń końcowych) licencjonowanego oprogramowania, którego termin ważności licencji się kończy i konieczności użycia właściwego dla danego oprogramowania narzędzia deinstalacji;

- odniesienia do zmian licencyjnych pojawiających się na rynku oprogramowania, np. monitorowania środowiska JAVA.

Dyrektor PBI wyjaśnił, że zasady prawidłowego użytkowania oprogramowania w Urzędzie zawarte są w dokumentach opisujących sposób przetwarzania danych osobowych oraz stosowane do tego środki techniczne i organizacyjne.

(akta kontroli str. 264-304, 339-349,568-654)

NIK zauważa, że brak ustanowionych mechanizmów kontrolnych we wskazanym zakresie powoduje, że w Urzędzie nie było możliwości skutecznego i efektywnego zarządzania licencjami na oprogramowanie.

5. Brak w badanym okresie[26] okresowych kontroli (co najmniej raz do roku) i sporządzania raportów oraz brak egzekwowania tego obowiązku, pomimo zapisów w Polityce Bezpieczeństwa obligujących do tego pracowników Urzędu.

W Urzędzie nie prowadzono czasowych (w zaplanowanych odstępach) przeglądów oprogramowania i licencji mających na celu potwierdzenie, że posiadano ich aktualny, kompletny spis oraz że posiadano licencje na każde zainstalowane oprogramowanie.

Zgodnie ze szczegółowym zakresem zadań i odpowiedzialności pkt 7 h) Polityki Bezpieczeństwa administrator systemów informatycznych zobowiązany był do dokonywania nie rzadziej niż raz do roku weryfikacji w zakresie zgodności z przepisami prawa oraz przyjętymi regulacjami zainstalowanego oprogramowania na stacjach roboczych poszczególnych użytkowników (i sporządzenie raportu).

[26] W latach 2019-2022 (do 30 sierpnia).

Dyrektor BPI wyjaśnił, że raporty takie nie były wykonywane. Przeglądy licencji prowadzone były wyrywkowo, a nie w zaplanowanych odstępach czasu. Prowadzona ewidencja oprogramowania zawiera wykaz urządzeń, na których zostało zainstalowane oprogramowanie. Licencje na środowiska wirtualne Vmware przechowywane były na koncie podmiotu, w serwisie prowadzonym przez producenta oprogramowania oraz w zasobach własnych Urzędu. Weryfikacja stanu licencji realizowana była na bieżąco w przypadku konieczności zainstalowania oprogramowania na nowym stanowisku/serwerze. W przypadku licencji których subskrypcja opiera się o rozwiązania Web lub chmurowe rozliczalność licencji realizowana była w oparciu o portale producentów, gdzie na bieżąco prezentowane był stan wykorzystania posiadanych licencji.

(akta kontroli str. 264-280, 339-349, 568-585)

Zastępca Prezydenta wyjaśnił ponadto, że przegląd licencji i zainstalowanego oprogramowania realizowany jest wraz z inwentaryzacją sprzętu, który aktualizowany jest na bieżąco podczas dokonywania zmian, reinstalacji, aktualizacji sprzętu, na którym zostało zainstalowane oprogramowanie. Ewidencja prowadzona jest w postaci elektronicznej w tabelach zawierających nr inwentarzowy sprzętu oraz wykaz oprogramowania.

(akta kontroli str. 744-749)

NIK zwraca uwagę, że niezależnie od prowadzonych ww. działań mających na celu potwierdzenie, że Urząd posiada aktualny, kompletny ich spis, oraz że posiada licencje na każde zainstalowane oprogramowanie, administrator systemów informatycznych zobowiązany był do dokonywania nie rzadziej niż raz do roku weryfikacji w zakresie zgodności z przepisami prawa oraz przyjętymi regulacjami zainstalowanego oprogramowania na stacjach roboczych poszczególnych użytkowników i tym samym, do sporządzenia raportów, których nie wykonywano.

6. Nieprawidłowe postępowanie z zainstalowanym oprogramowaniem:

a) w trakcie kontroli ujawniono, na wybranych losowo urządzeniach, przypadki instalacji oprogramowania EOL (end of life), czyli takie, które zostało oficjalnie wycofane ze względu na luki w bezpieczeństwie.

Dyrektor BPI wyjaśnił, że oprogramowanie to nie było oznaczone przez oprogramowanie *inventory tool* jako EOL. Było to darmowe oprogramowanie i służyło do szyfrowania oraz tworzenia szyfrowanych plików.

(akta kontroli str. 568-654, 757-760)

NIK zauważa, że za zarządzanie oprogramowaniem i licencjami odpowiada konkretna osoba, a nie oprogramowanie *inventory tool*, które jest jedynie narzędziem wspomagającym ten proces. Ww. oprogramowanie EOL zostało oficjalnie wycofane przez producenta a osoba odpowiedzialna za zarządzanie licencjami oraz administratorzy poszczególnych systemów powinni posiadać tę wiedzę.

b) korzystanie ze starych wersji aplikacji, w tym nawet krytycznych, wymagających aktualizacji.

Dyrektor PBI wyjaśnił, że starsza wersja tego oprogramowania była niezbędna do uruchomienia starszego oprogramowania, której nie gwarantują nowsze wersje tego oprogramowania (JAVA).

(akta kontroli str. 757-760)

Według opinii biegłego, w odniesieniu do starych wersji aplikacji, istotne było też to, że w Urzędzie używano w dużym zakresie oprogramowania bez wsparcia i aktualizacji zabezpieczeń np. Ms Office w wersjach już od wielu lat niewspieranych

oraz system operacyjny Windows XP (7 hostów) i Windows 7 (241 hostów). Informacja o planowanej dacie zakończenia wsparcia była dostępna już kilka lat wcześniej. Proces wymiany sprzętu odbywał się w Urzędzie sukcesywnie, jednak nie był realizowany w oparciu o harmonogram, który byłby zaakceptowany przez kierownictwo Urzędu.

(akta kontroli str. 568-585)

NIK zauważa, że w odniesieniu do starych wersji aplikacji, istotne było też to, że w Urzędzie używano w dużym zakresie oprogramowania bez wsparcia i aktualizacji zabezpieczeń np. Ms Office w wersjach już od wielu lat niewspieranych oraz system operacyjny Windows XP (7 hostów) i Windows 7 (241 hostów). Informacja o planowanej dacie zakończenia wsparcia była dostępna już kilka lat wcześniej. Proces wymiany sprzętu odbywał się w Urzędzie sukcesywnie, jednak nie był realizowany w oparciu o harmonogram, który byłby zaakceptowany przez kierownictwo Urzędu. Reasumując, takie „stare" oprogramowanie naraża cały Urząd na potencjalny wyciek danych.

c) aplikacje niezwiązane z pracą. Na poddanych badaniu komputerach zainstalowane było oprogramowanie do odtwarzania plików audio oraz nagrywania płyt CD, w bardzo starej wersji.

Dyrektor PBI wyjaśnił, że niezwiązany z pracą dodatek w zależności od dystrybucji systemu Windows 10 instalowany może być w sposób automatyczny wraz z systemem operacyjnym, dodatek ten może również instalować się podczas aktualizacji systemu. Inny program (stara wersja) służył natomiast do odtwarzania plików audio oraz dawał możliwość nagrywania płyt CD.

(akta kontroli str. 757-760)

Zdaniem NIK, w Urzędzie powinien zostać wzmożony nadzór, tak aby unikać instalacji aplikacji niezwiązanych z wykonywaniem obowiązków służbowych. Odnosząc się natomiast do wyjaśnień, stosowanie przez pracowników Urzędu oprogramowania przestarzałego, bez wsparcia technicznego, rodzi ryzyka w obszarze cyberbezpieczeństwa.

OCENA CZĄSTKOWA

NIK negatywnie ocenia działania podejmowane w Urzędzie w ww. zakresie. Nie posiadano pełnej i rzetelnej wiedzy na temat stanu wykorzystywanego oprogramowania, ponieważ prowadzona ewidencja była nierzetelna i nie zbierała danych w trybie rzeczywistym i ciągłym na zasobach. Nie prowadzono czasowych (w zaplanowanych odstępach) przeglądów oprogramowania i licencji mających na celu potwierdzenie, że posiadano aktualny, kompletny ich spis, oraz licencje na każde zainstalowane oprogramowanie. Nie prowadzono monitoringu zainstalowanego oprogramowania na urządzeniach, w tym również na urządzeniach typu smartfon/tablet, w związku z czym nie prowadzono nadzoru i nie posiadano wiedzy o zainstalowanym na tych urządzeniach oprogramowaniu, w tym nieautoryzowanym. Ponadto zidentyfikowano przypadki instalacji oprogramowania EOL, korzystanie ze starych wersji oprogramowań, w tym krytycznych oraz aplikacji niezwiązanych z realizacją obowiązków służbowych.
Ponadto nie zatrudniono audytora wewnętrznego i nie prowadzono w latach 2020-2022 audytów wewnętrznych, pomimo obowiązku wynikającego z ustawy o finansach publicznych.

OBSZAR

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

Opis stanu faktycznego

2.1. W Urzędzie zapotrzebowanie na zakup oprogramowania specjalistycznego ustalane było przez BPI na podstawie zgłoszeń z wydziałów merytorycznych. Dyrektor

BPI wyjaśnił, że komórki dokonywały wewnętrznej oceny potrzeb w tym zakresie, a następnie BPI przeprowadzało weryfikację posiadanych i wykorzystanych licencji. W przypadku braku wolnych licencji dokonywało zakupu, o ile Biuro dysponowało odpowiednimi środkami finansowymi. Ponadto dodał, że komórki organizacyjne Urzędu najczęściej zgłaszały zapotrzebowanie na licencje Microsoft Office oraz programy użytkowe do przetwarzania tekstu czy obrazu. Zgłoszenia te weryfikowane były przez Biuro na zasadzie sprawdzenia w danym momencie wolnych posiadanych licencji możliwych do wykorzystania, zwłaszcza jeśli chodzi o licencje MS Office oraz programy biurowe, systemy operacyjne. BPI kupowało licencje oprogramowania Microsoft w programie licencjonowania grupowego (wolumenowego) MPSA (Microsoft Products and Services Agreement). W ramach tego programu, zakupione licencje nie były przydzielone bezpośrednio do kupowanego sprzętu, jak to miało miejsce w zakupach typu OEM. BPI miało więc możliwość przydzielania licencji na konkretne stanowisko tak długo, jak była ona wykorzystywana. Oznacza to, że w przypadku zwolnienia się stanowiska, część licencji ulega uwolnieniu i w miarę zgłaszanych potrzeb była przydzielana na inne stanowisko.

W badanych latach BPI dokonało zakupu 115 dodatkowych licencji MS Office, z których 45 było zaplanowane w budżecie i związane z uzupełnieniem stanowisk, dla których wykazano zapotrzebowanie oraz wymianę starych wersji oprogramowania. Natomiast zakup kolejnych 70 licencji był zaplanowany w roku 2021 r. i związany był z zakupem 50 sztuk zestawów komputerowych.

Zakup pozostałych licencji był sporadyczny, zgłaszany w trakcie roku i wynikał z nałożonych na działy zadań, których nie można było przewidzieć w roku poprzedzającym. Takie zakupy były realizowane na bieżąco z paragrafu wydatków bieżących.

W latach 2019-2022 w Urzędzie było zatrudnionych odpowiednio 474, 462, 415 i 425 pracowników. W badanym okresie zakupiono m.in. moduł Zamówienia publiczne w systemie LEX z dostępem w 2019 i w 2020 r. dla 500 użytkowników i w 2021 r. dla 300 użytkowników.

Zastępca Prezydenta wyjaśnił, że pakiet ten wchodził w skład programu *LEX Administracja* i w ramach dostępu Urząd otrzymywał licencje dostępowe do modułu z określonym maksymalnym ich limitem. W kolejnej rocznej umowie na okres 2022/2023 zamówiono w tym module 300 dostępów, przy użyciu w poprzednim okresie wynoszącym 270 użytkowników. Ponadto podał, że na potrzeby kolejnych zakupów będą dalej prowadzone sprawdzenia dotyczące liczby niezbędnych dostępów.

(akta kontroli str. 339-378, 827-840, 842-893)

2.2. W Urzędzie nie posiadano narzędzia pozwalającego na automatyczną weryfikację efektywności zainstalowanego oprogramowania w skali Urzędu, działającego np. poprzez wyświetlenie listy aplikacji na komputerach użytkowników wraz z informacją o ich użyciu, bądź nie.

Dyrektor BPI wyjaśnił, że BPI dokonywało weryfikacji efektywności zainstalowanego oprogramowania w ograniczonym zakresie w przypadku aplikacji użytkowanych na mniejszą skalę. Weryfikację taką umożliwiało oprogramowane typu *inventory tool*, które oferowało selektywne sprawdzenie użycia 10 najczęściej użytkowanych aplikacji przez konkretnego użytkownika[27]. W przypadku posiadania przez pracownika BPI informacji o zainstalowanym na konkretnym komputerze oprogramowaniu, Biuro miało możliwość, analizując ten widok, określenia, czy użytkownik wykorzystywał aplikację, czy nie. Jeśli aplikacja taka została wyświetlona

[27] Po wejściu do widoku Komputery -> (weryfikowany komputer) -> statystyki.

w widgecie „użycie oprogramowania” to znaczyło, że jest użytkowana, jeśli nie została wyświetlona oznaczało, że nie jest użytkowana.

(akta kontroli str. 565-566)

Kontrola wykazała, że w Urzędzie nie wprowadzono mechanizmu kontrolnego oraz nie przeprowadzano każdorazowej analizy/weryfikacji/oceny pod kątem zasadności wykorzystania oprogramowania i dokonywania zakupu usługi na jego utrzymanie, co szczegółowo przedstawiono w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 565-566)

W badanym okresie dokonano 18 zamówień związanych z oprogramowaniem OTAGO na łączną kwotę 3 262,5 tys. zł.Z tego trzy zamówienia na asystę techniczną: w 2019 r. o wartości 867,6 tys. zł, w 2020 r. o wartości 928,7 tys. zł i w 2021 r. o wartości 977,8 tys. zł udzielone zostały w trybie przetargu nieograniczonego. Pozostałe 15 zamówień, w tym trzy na asystę techniczną[28] i 12 na rozbudowę i rozszerzenie funkcjonalności użytkowanego systemu udzielone zostały każde o wartości poniżej 30 tys. euro w 2019 r. i 2020 r. oraz poniżej 130 tys. zł w 2021 r., tj. w trybie poza ustawą o zamówieniach publicznych, stosownie do art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych[29], a od 1 stycznia 2021 r. stosownie do art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych[30].

(akta kontroli str. 438)

Dyrektor BPI wyjaśnił, że zakupy kolejnych modułów lub funkcjonalności zintegrowanych systemów informatycznych dokonywane były w porozumieniu z wydziałami merytorycznymi. W pierwszej kolejności prowadzone były rozmowy z wydziałem merytorycznym w celu omówienia zasadności dokonania zakupu oraz kwestie dokonania zakupu u różnych dostawców. Przyczynami dokonywania zakupów w przypadku zintegrowanego systemu informatycznego były zazwyczaj zmieniające się przepisy prawa, nakładające na gminę nowe obowiązki lub zmiany dotychczasowych przepisów, a wymagające dokonania istotnych zmian w oprogramowaniu. Zakupy mogły wynikać również z poprawy funkcjonowania oprogramowania, a dzięki zakupowi bardziej zawansowanych mechanizmów ułatwiały pracę pracownikom.

(akta kontroli str. 339-349)

Badanie sześciu[31] wybranych oprogramowań SaaS wykazało, że BPI analizował wykorzystanie przydzielonego dostępu do usługi m.in. poprzez zgłoszenia zapotrzebowania na utworzenie konta (np. Lex-Administracja) lub poprzez udostępnienie konta (np. dla Wydziału Prawnego w celu publikacji postępowań przetargowych).

(akta kontroli str. 751-754)

W badanym okresie zakończył się okres trwałości pięciu zrealizowanych projektów ze środków europejskich: Zielony Pomost, ZSIM – Zintegrowany System Informacyjny Miast, Nowoczesna sieć szerokopasmowa, Budowa monitoringu wizyjnego miasta i „Internet – świat w twoim domu”. Licencje (36 wieczyste) pozyskane w czterech pierwszych projektach nadal są użytkowane po okresie trwałości projektów. Natomiast w przypadku ostatniego projektu pozyskano 299 licencji, w tym 135 zostało

[28] Na dwa miesiące 2019 r. i jeden miesiąc 2020 r. z powodu unieważnienia postępowania przetargowego.
[29] Dz. U. z 2019 r. poz. 1843 ze zm.
[30] Dz. U. z 2022 r., poz. 1710 ze zm..
[31] W tym po jednym z 2019 i 2022 r. i po dwa z 2020 i 2021 r.

przekazanych beneficjentom, sześć zostało zlikwidowanych wraz z komputerami, 54 zostało w Urzędzie i 10 licencji specjalistycznych pozostaje niewykorzystanych.

(akta kontroli str. 750)

2.3. W latach 2019-2022 (do 30 czerwca) poniesiono wydatki na nabycie i korzystanie z oprogramowania w tym związanych m.in. z dostosowaniem lub aktualizacją programów komputerowych, przedłużeniem umów licencyjnych, subskrypcją licencji w łącznej kwocie 4 459,5 tys. zł w tym: 1,943,2 tys. zł w 2019 r., 1 870,5 tys. zł w 2020 r., 1 918,3 tys. zł w 2021 r. i 410,5 tys. zł w 2022 r.

Ponadto zakupiono urządzenia, które dostarczone były wraz z oprogramowaniem lub licencjami w łącznej kwocie 1 667,0 tys. zł w tym: 719,6 tys. zł w 2019 r., 463,8 tys. zł w 2020 r. i 483,6 tys. zł w 2021 r.

(akta kontroli str. 305-310)

2.4. Badanie sześciu[32] wybranych oprogramowań[33] SaaS wykazało, że oprogramowania te spełniały określone wymagania bezpieczeństwa, tj. od momentu rozpoczęcia użytkowania nie stwierdzono przypadków podatności na utratę dostępności, integralności i poufności informacji. Badane oprogramowania były testowane przed ich zakupem np. poprzez prezentację ofert i weryfikację otrzymanych listów referencyjnych. W procesie zakupu uwzględniano także weryfikację spełnienia wymagań RODO[34].

(akta kontroli str. 753-754)

2.5. Badanie sześciu[35] ww. wybranych oprogramowań SaaS wykazało, że w Urzędzie przed zakupem:

- każdorazowo dokonywano oceny procesu nabycia oprogramowania, uwzględniającej wiarygodność dostawcy pod kątem zapewnienia ciągłości usługi oraz zapewnienia wsparcia technicznego i bezpieczeństwa;

- weryfikowano dostępność umowy SLA, a także oceniano, że umowa ta była korzystna dla jednostki;

- weryfikowano projekty umów, zapewniając w ten sposób m.in. możliwość wcześniejszego powiadomienia o pracach serwisowych, zgłaszania błędów aplikacji.

Biegły wskazał potrzebę doprecyzowania na etapie nabywania oprogramowania SaaS o takie kwestie jak weryfikacja: zapewnienia szyfrowania data-in-transit w oparciu o bezpieczne protokoły i algorytmy, polityki kopii zapasowej, w tym częstotliwość wykonywania kopii i okresu retencji oraz przechowywania, spełnienia wymagań kontroli dostępu, spełnienia wymagań RODO (i innych wymagań wynikających z określonych przepisów prawa).

(akta kontroli str. 755-756)

Stwierdzone nieprawidłowości

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

W Urzędzie nie wprowadzono mechanizmu kontrolnego oraz nie przeprowadzano każdorazowej analizy/weryfikacji/oceny pod kątem zasadności wykorzystania oprogramowania i dokonywania zakupu usługi na jego utrzymanie.

(akta kontroli str. 390-400, 568-585, 735)

[32] Po dwa nabyte w 2019 i 2020 i po jednym z 2021 i 2022 r.

[33] Lex, dostęp do internetowej platformy informatycznej, system BIPLO, dostęp do systemu kalkulatorów.

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz. U. UE L z 2016 r., poz.119 Nr 1 ze zm.

[35] Po dwa nabyte w 2019 i 2020 i po jednym z 2021 i 2022 r.

Dyrektor BPI wyjaśnił, że nie wprowadzono mechanizmu kontrolnego i nie weryfikowano każdorazowo wykorzystania oprogramowania w kontekście zakupu usługi na jego utrzymanie oraz nie dokonywano systematycznej weryfikacji adekwatności przydzielonych użytkownikom narzędzi informatycznych pod kątem ich niezbędności do realizacji zadań. Jednakże podał, że analizy takie wykonywane były każdorazowo podczas konstruowania budżetu w zakresie przedłużenia licencji i oprogramowania. Analizy zasadności i celowości realizowane były przez działy merytoryczne, które zgłaszały zapotrzebowanie na zakup oprogramowania. Kolejnym etapem była weryfikacja posiadanych zasobów pod kątem możliwości wykorzystania licencji będących własnością Urzędu.

(akta kontroli str. 339-349, 744-749, 757-;760, 788-791)

NIK zauważa, że niezależnie od prowadzenia analiz podczas konstruowania budżetu w Urzędzie powinno zapewnić się wprowadzenie systemowego mechanizmu kontrolnego oraz przeprowadzanie każdorazowej analizy/weryfikacji/oceny pod kątem zasadności wykorzystania oprogramowania i dokonywania zakupu usługi na jego utrzymanie.

OCENA CZĄSTKOWA

W Urzędzie nie dokonywano systematycznej analizy funkcjonalności i efektywności posiadanego oprogramowania.

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 uwagi i wnioski:

Uwagi

NIK nie formułuje uwag.

Wnioski

1. Zapewnienie prowadzenia audytu wewnętrznego.
2. Wprowadzenie zasad zarządzania oprogramowaniem i licencjami.
3. Podjęcie działań w celu rzetelnego prowadzenia ewidencji oprogramowania i licencji jak również ujęcia w niej oprogramowania instalowanego na tabletach i smartfonach.
4. Zapewnienie skutecznego zarządzania i nadzoru nad oprogramowaniem wykorzystywanym na urządzeniach mobilnych (typu smartfon, tablet).
5. Prowadzenie czasowych przeglądów oprogramowania i licencji oraz dokumentowanie podejmowanych czynności, w tym działań naprawczych.
6. Wprowadzenie mechanizmu kontrolnego zapewniającego analizę/weryfikację /ocenę pod kątem zasadności wykorzystania oprogramowania i dokonywania zakupu usługi na jego utrzymanie.

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 Bydgoszczy. 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.

Bydgoszcz, 28 października 2022 r.

Najwyższa Izba Kontroli
Delegatura w Bydgoszczy
p.o. Dyrektor
(-) Tomasz Sobecki

Kontroler
(-) Elżbieta Warda-Fereniec
główny specjalista kontroli państwowej

zmian w wystąpieniu pokontrolnym dokonał:

p.o. Dyrektor
(-) Tomasz Sobecki