NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ. 410.021.02.2022

Pan
Piotr Krzystek
Prezydent Miasta Szczecin

Urząd Miasta Szczecin
Plac Armii Krajowej 1
70-456 Szczecin

WYSTĄPIENIE POKONTROLNE

Zmienione zgodnie z treścią uchwały nr KPK-KPO.443.197.2022
Zespołu Orzekającego Komisji Rozstrzygającej Najwyższej Izby Kontroli
z 9 stycznia 2023 r.

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Urząd Miasta Szczecin, Plac Armii Krajowej 1, 70-456 Szczecin[1].

Kierownik jednostki kontrolowanej

Piotr Krzystek, Prezydent Miasta Szczecin[2] od 4 grudnia 2006 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[3].

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 Szczecinie.

Kontrolerzy

1. Radosław Kropiowski, doradca ekonomiczny, upoważnienie do kontroli nr LSZ/115/2022 z 7 lipca 2022 r.
2. Krzysztof Zawadzki, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LSZ/114/2022 z 7 lipca 2022 r.

(akta kontroli str. 1-5)

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

W Urzędzie przyjęto procedury zarzadzania oprogramowaniem komputerowym, w tym nabywania, wdrażania, użytkowania i nadzorowania, jednakże wdrożone zasady zarządzania licencjami nie zawierały szczegółowych uregulowań obejmujących wszystkie elementy i czynności niezbędne do zarządzania i nadzoru nad pełnym cyklem ich funkcjonowania, w tym nie określono szczegółowych zasad nabywania i wykorzystywania programów w modelu SaaS[6]. Zasoby kadrowe odpowiedzialne za zarzadzanie oprogramowaniem (Wydział Informatyki[7]) były nieadekwatne do skali zadań, wykonywanych przez Urząd wraz z jednostkami organizacyjnymi Gminy Miasto Szczecin[8].

[1] Dalej: Urząd lub UM.
[2] Dalej: Prezydent.
[3] Czynności kontrolne w Urzędzie zakończyły się 28 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] Oprogramowania jako usługi (Software as a Service, SaaS) - 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; dalej: *SaaS*.
[7] Dalej: Wydział.
[8] Dalej: Gmina.

Urząd w ograniczonym zakresie wykorzystywał posiadane narzędzia do monitorowania oprogramowania. Skutkiem braku podejmowania wszystkich działań monitorujących oprogramowanie było ujawnienie przypadków instalowania programów bez ważnej licencji. Urząd dysponował danymi o posiadanych zasobach informatycznych i stopniu ich wykorzystania (m.in. za pomocą systemu ICOR) oraz sprawował nadzór nad dokumentacją licencyjną i nośnikami oprogramowania.

Urząd podejmował działania w celu optymalizacji wykorzystania posiadanego oprogramowania. Nie stwierdzono wolnego/niewykorzystywanego oprogramowania. W procesie planowania zakupów uwzględniano rzeczywisty san posiadanych zasobów informatycznych. Przyjęte rozwiązania w zakresie planowania, finansowania i realizacji działań podejmowanych w ramach zarządzania oprogramowaniem uwzględniały faktyczne potrzeby Urzędu. W badanym postępowaniu o udzielenie zamówienia publicznego na świadczenie usług asysty technicznej oraz rozwoju Zintegrowanego Systemu Informatycznego wspomagającego zarządzanie finansami Miasta (ZSI-FK) została przeprowadzona analiza, o której mowa w art. 83 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych[9]. Jednak w ocenie NIK zastosowanie trybu zamówienia z wolnej ręki w postępowaniu tego zamówienia publicznego naruszało art. 214 ust. 1 pkt 1 lit. a i b Pzp, określający przesłanki zastosowania tego trybu, na które powołał się Urząd.

OBSZAR

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym.

Opis stanu faktycznego

1.1. Przyjęte procedury zarządzania oprogramowaniem komputerowym, w tym nabywania, wdrażania, użytkowania i nadzorowania.

Wydział był komórką organizacyjną odpowiedzialną w Urzędzie za organizację oraz nadzór nad sprzętem i oprogramowaniem komputerowym. Do jego zadań należała m.in. informatyzacja Urzędu oraz koordynacja informatyzacji jednostek organizacyjnych Gminy, a także związane z tym działania m.in. takie jak: budowa baz danych i systemu map komputerowych, budowa i administrowanie sieci. Wydział był odpowiedzialny za gospodarowanie, obsługę i zapewnienie sprawnego funkcjonowania sprzętu, oprogramowania i sieci komputerowych; bieżące ich administrowanie i dostosowywanie do potrzeb. W okresie objętym kontrolą dwukrotnie zmieniono regulamin wewnętrzny Wydziału. Określono w nim m.in. strukturę wewnętrzną wraz z obsadą etatową, zakres czynności pracowników, obieg dokumentacji, zasady zastępowania pracowników.

Procedury postępowania z oprogramowaniem określone były w Regulaminie korzystania z zasobów informatycznych Urzędu – Załącznik Nr 4 do Zarządzenia Nr 150/18 Prezydenta z 6 kwietnia 2018 r. w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu[10], który udostępniony był do wglądu pracownikom Urzędu w zakładce regulaminy oraz bezpieczeństwo komputera i sieci w Uminecie (wewnętrzny Intranet). Nadawanie uprawnień do oprogramowania opisane zostało w zarządzeniu Prezydenta Nr 327/19[11]. Opublikowano i udostępniono wszystkim pracownikom UM informację dot. „Standardu oprogramowania" - strona UMINET zakładka Bezpieczeństwo komputera i sieci.
W Wydziale wyodrębniono stanowisko głównego specjalisty ds. administrowania certyfikatami i licencjami.

[9] Dz.U. z 2022 r. poz. 1710, ze zm.; dalej: Pzp.
[10] Dalej: Polityka Bezpieczeństwa.
[11] Zmieniające zarządzenie w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin z 26 lipca 2019 r. Zarządzenie pod adresem: https://bip.um.szczecin.pl/chapter_131182.asp?soid=203B6037DB8942FBB7D052031B852D22

Zasady gromadzenia i przechowywania dowodów zakupu oraz zasady ewidencjonowania oprogramowania i utrzymania kompletności i aktualności ewidencji określała Polityka Rachunkowości Urzędu – Zarządzenie Prezydenta Nr 552/19 z 31 grudnia 2019 r., ze zm. Dodatkowo ewidencja dowodów zakupu i licencji prowadzona była przez Wydział w systemie ICOR. Certyfikaty i licencje w formie papierowej przechowywane były w magazynie Wydziału.

(akta kontroli str. 36-43, 1907-1921, 1927-1939, 1972-1977)

W sprawie zarządzania urządzeniami mobilnymi Dyrektor Wydziału wyjaśnił, że: *Urządzenia typu smartfon są wykorzystywane tylko do połączeń telefonicznych, nie łączą się z siecią Urzędu i nie są własnością Wydziału. Ewidencja tych urządzeń oraz ich przeglądy są w zakresie Miejskiej Jednostki Obsługi Gospodarczej (…) wykonany audyt w trakcie kontroli potwierdził brak instalacji oprogramowania innego niż systemowe dołączone do smartfona.*

(akta kontroli str. 1548-1551)

W procedurach Urzędu[12] nie doprecyzowano zasad i kryteriów weryfikacji oprogramowania (np. pod kątem bezpieczeństwa w procesie nabywania); zasad utrzymania kompletności i aktualności ewidencji; zasad dystrybucji i redystrybucji licencji oraz wycofywania licencji; zasad i częstotliwości okresowych przeglądów; zasad monitorowania stanu użycia i legalności; zasad zarządzania oprogramowaniem z uwzględnieniem wszystkich rodzajów urządzeń końcowych (np. tabletów lub smartfonów). Zostało to również potwierdzone przez powołanego przez NIK biegłego[13] w dziedzinie audytu systemów informatycznych[14] (szerzej opisano w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 56-60, 1978-1981)

1.2. Pracownicy wykonujący zadania w zakresie zarządzania licencjami / oprogramowaniem komputerowym.

W Wydziale za zarządzanie poszczególnymi licencjami odpowiedzialne były osoby, wykazane w systemie I.[15], tj. w bazie danych posiadanego przez Urząd oprogramowania. Na poszczególnych poziomach dostępności, mogło z niej korzystać 37 wyznaczonych pracowników Wydziału (odpowiedzialnych za wskazane programy). Do każdej aplikacji przydzielono jedną osobę odpowiedzialną za jej administrowanie. Zadania z zakresu zarządzania oprogramowaniem (od trzech do dziewięciu) wykonywało 24 pracowników[16] Wydziału.

(akta kontroli str. 1133, 1155-1161. 1414-1422)

Wszyscy pracownicy Urzędu uczestniczyli w szkoleniach przeprowadzonych przez Inspektora Danych Osobowych w zakresie ochrony danych osobowych, bezpieczeństwa komputera i sieci oraz procedur w ramach Polityki Bezpieczeństwa. Dodatkowo w ramach służby przygotowawczej nowo zatrudnieni pracownicy byli przeszkoleni z obsługi systemu zarządzania dokumentami i zadaniami pracowników eDOK.

(akta kontroli str. 337-338, 1500-1501)

Zastępca Dyrektora Wydziału wyjaśniła, że: *każdy nowozatrudniony pracownik przed dopuszczeniem do przetwarzania danych winien odbyć obowiązkowe*

[12] Tj. regulaminach organizacyjnych Urzędu, regulaminach określających szczegółowe zakresy zadań realizowanych przez jednostki organizacyjne Urzędu, oraz regulaminach wewnętrznych Wydziału i Polityce Bezpieczeństwa.

[13] Na podstawie art. 49 ust. 1 i 2 ustawy o NIK.

[14] Ekspert do spraw audytu systemów informatycznych oraz systemów zarządzania bezpieczeństwem informacji.

[15] I. to system bazodanowy.

[16] Dla danego zadania wykonywało je więcej niż jedna osoba.

szkolenie z zakresu ochrony danych i bezpieczeństwa informacji. Oświadczenie, które stanowi załącznik Nr 14 do zarządzenia składane jest w dniu wstępnego szkolenia, o którym mowa w zdaniu wyżej. Ponadto pracownicy przechodzą tzw. służbę przygotowawczą, w trakcie której uczestniczą w szkoleniu przeprowadzonym przez Inspektora Ochrony Danych pod nazwa. „Ochrona danych osobowych", w ramach którego zostają zapoznani z tematyką związaną z bezpieczeństwem informacji, zasadami użycia zasobów, cyberbezpieczeństwem itp. Służba przygotowawcza kończy się egzaminem. Szkolenia przeprowadzone przez IOD dają gwarancję, że żaden z pracowników nie zostanie pominięty i uzyska podstawową wiedzę dotyczącą zasad związanych z bezpieczeństwem informacji. Dodatkowo, w §1 ust. 1 załącznika nr 1 do Zarządzenia Prezydenta (…) 150/18 jest mowa, iż „kierownicy odpowiadają za przeszkolenie instruktażowe pracowników w zakresie bezpieczeństwa informacji na stanowiskach pracy. Tak więc dodatkowo uświadamiają pracowników o tym, jak bezpiecznie korzystać z komputera i zasobów. W tym miejscu do protokołu dołączam wzór Oświadczenia do Zarządzenia Prezydenta nr 150/18, Dwie karty służby przygotowawczej z podpisami pracowników oraz karta z egzaminu. Łącznie 4 karty. Inspektor Ochrony Danych Osobowych szkoli także z bezpiecznego komputerów i zasobów informatycznych. Chodzi o to by korzystali z urządzeń IT w zakresie akceptowalnym to znaczy bez jakiejkolwiek ingerencji w oprogramowanie zgodnym z zasadami z polityce bezpieczeństwa.

(akta kontroli str. 1500-1508, 1907-1926)

Pracownicy Wydziału przeprowadzali szkolenia pracowników Urzędu i jednostek organizacyjnych Gminy z obsługi funkcjonalnej udostępnionych systemów, w tym z zakresu obsługi: Systemu Informacji Przestrzennej Miasta Szczecin (2016 r. dla ok. 650 uczestników); systemu eDOK (2021 r. dla ok. 500 uczestników); szkolenie w zakresie publikacji wykazów nieruchomości w systemie LEG.
Administratorzy systemów uczestniczyli w szkoleniach dotyczących zarządzania aplikacjami M., a w ramach umów wdrożeniowych brali udział w szkoleniach/warsztatach instruktażowych administrowania systemami.

(akta kontroli str. 337-338)

W latach 2019-2022 przeprowadzono łącznie 56 szkoleń[17] za kwotę 55,1 tys. zł[18]. Uczestniczyło w nich w 2019 r. 245 pracowników Urzędu, w 2020 r. 191, w 2021 r. 1 353, a w 2022 r. 76. Przedmiotem szkoleń była obsługa oprogramowania oraz polityka bezpieczeństwa. (akta kontroli str. 353)

W sprawie przeprowadzonych szkoleń z zarządzania oprogramowaniem osób, które w Urzędzie odpowiadały za wykonywanie tych zadań, Dyrektor Wydziału wyjaśnił, że: *W 2020 r. odbyły się dwa szkolenia z zakresu: Licencjonowanie oprogramowania M. dla pięciu osób oraz Szkolenie z systemu do zdalnej instalacji oprogramowania dla 10 osób. To było właśnie związane z zarządzaniem oprogramowaniem i dotyczyło ściśle wykonywanych w związku z tym obowiązków.*

(akta kontroli str. 1978-1981)

Braki kadrowe w Wydziale odpowiedzialnym za zarządzanie oprogramowaniem na dzień rozpoczęcia kontroli[19] wynosiły cztery wakaty, w 2021 r. jeden, 2020 r. trzy, 2019 r. dwa. W wyniku przeprowadzonych przez Urząd w latach 2019-2022 naborów, przyjęto do pracy w 2020 r. jedną osobę, a w 2021 r. cztery. W latach 2019-2022 r. z Wydziału odeszły trzy osoby zarządzające oprogramowaniem.

(akta kontroli str. 1693)

[17] Z tego w 2019 r. 14, 2020 r. 15, 2021 r. 24 i 2022 r. trzy.
[18] Z tego w 2019 r. 25,1 tys. zł, 2020 r. 10,0 tys. zł, 2021 r. 20,0 tys. zł, 2022 r. 0,0 zł.
[19] 8 lipca 2022 r.

W dniach 28 września 2020 r. i 31 sierpnia 2021 r. odeszli pracownicy Referatu Wsparcia Użytkowników, którzy prowadzili nadzór nad użytkowaniem programów funkcjonujących w Urzędzie oraz przyjmowaniem zgłoszeń o działaniu i uwag odnośnie ewidencji sprzętu komputerowego i oprogramowania. Wyżej wymienione obowiązki przejął główny specjalista w Referacie Wsparcia Użytkowników. Natomiast 31 maja 2022 r. z Wydziału odszedł administrator zajmujący się kontrolą stanu wykorzystania zasobów informatycznych Urzędu, w tym kontrolą bieżącej pracy użytkowników oraz nadzorem nad aktualnością i legalnością oprogramowania komputerowego w Urzędzie.

(akta kontroli str. 1985)

Zastępca Dyrektora Wydziału oświadczyła, że: *przyczyną braku zainteresowania naborami były ograniczone możliwości finansowe w zakresie wysokości proponowanego wynagrodzenia; niemożność wykonywania pracy zdalnej i duży popyt rynku komercyjnego IT. W Urzędzie były nieobsadzone stanowiska związane z cyberbezpieczeństwem, analizą i projektowaniem w Referacie Projektów, administrowaniem siecią komputerową oraz oprogramowaniem. Skutkiem fluktuacji kadr była utrata kluczowych specjalistów, którzy zabrali swoje know-how, znajomość procesów, strukturę organizacji, rynku oraz wypracowane kontakty z firmami informatycznymi. Skutkiem fluktuacji jest też przerzucanie obowiązków na innych pracowników.*

(akta kontroli str. 339-340, 1693-1694, 1985)

W Analizie potrzeb i wymagań dla projektu ZSI-FK, opisanej w pkt. 2.2. niniejszego wystąpienia pokontrolnego wskazano, że obejmowała ona łącznie z Urzędem 39 jednostek Gminy. Według regulaminów organizacyjnych Urzędu, do zadań Wydziału należało m.in. opracowywanie, wdrażanie i nadzorowanie programów informatyzacji Urzędu i jednostek organizacyjnych Gminy; opracowywanie, wdrażanie i nadzorowanie projektów dotyczących poprawy jakości form obsługi mieszkańców i interesantów oraz zwiększenie efektywności pracy pracowników Urzędu i jednostek organizacyjnych Gminy. Wydział posiadał 40 etatów.

(akta kontroli str. 64-254, 339-340)

1.3. Informacje o posiadanych zasobach informatycznych i nadzór nad dokumentacją licencyjną i nośnikami oprogramowania.

Spis licencji i oprogramowania, w tym subskrypcji, wykorzystywanych w Urzędzie w ramach wszystkich systemów oraz dane dotyczące samych systemów przechowywane były w systemie I. Obejmował on m.in. dane ilościowe, takie jak: liczba programów (283), maksymalna liczba licencji, liczba osób korzystających z danego programu, wykorzystanie procentowe, datę wygaśnięcia licencji[20], koszty zakupu licencji całościowe oraz na osobę korzystającą. System wskazywał też liczbę posiadanych licencji i liczbę instalacji. Z danych w nim zawartych wynikało, że wszystkie programy zainstalowane w Urzędzie były wykorzystywane. Wydatki związane z utrzymaniem systemu I. w latach 2019-2022[21] wyniosły 577,4 tys. zł.
Do weryfikacji oprogramowania pod kątem zarządzania oprogramowaniem, monitorowania oprogramowania, inwentaryzacji i bezpieczeństwa IT przeznaczony był program typu Inventory tool eA.[22] zakupiony w 2009 r. za kwotę 65,3 tys. zł - doraźnie wykorzystywany do weryfikacji posiadanych zasobów (Urząd przedłożył

[20] W przypadku zbliżania się końca licencji system automatycznie o tym informował, co odnosiło się do całości posiadanego oprogramowania zarejestrowanego w systemie.
[21] Do 8 września 2022 r.
[22] https://www.e..eu/, funkcje eA. zarządzanie - https://www.eauditor.eu/zarzadzanie-it/#.

dwa raporty jego wykorzystania w okresie objętym kontrolą[23]). Wydatki na jego utrzymanie w latach 2019-2022[24] wyniosły 45,5 tys. zł brutto.

(akta kontroli str. 1132-1138, 1239-1246, 1531-1542, 1978-1984)

W Urzędzie do weryfikacji oprogramowania służyły także systemy M.[25], I., Zintegrowany System Informatyczny wspomagający zarządzania finansami Miasta[26] i program E. P.[27].

(akta kontroli str. 339)

Dyrektor wyjaśnił, że: *Głównymi narzędziami/aplikacjami do weryfikacji posiadanego oprogramowania i właściwych licencji jest: 1) eA. – system do inwentaryzacji komputerów i zainstalowanego oprogramowania, który pozwala monitorować zmiany w komputerach. On ma głównie za zadanie skanowanie komputerów. 2) M. – (wytworzony w ramach własnych zasobów, nie generujący wydatków) – umożliwia zarządzanie uprawnieniami i zgłoszeniami technicznymi dotyczącymi oprogramowania, weryfikację wniosków o uprawnienia do systemów. Pozwala na tworzenie raportu użytkowników wnioskujących o dostęp do danego oprogramowania, 3) I. – W.I. Licencje – (wytworzony w ramach własnych zasobów, nie generujący wydatków) – system w którym WINF prowadzi ewidencję każdego zainstalowanego w UMS oprogramowania, niezależnie od tego czy jest ono darmowe czy komercyjne, zawiera funkcjonalności pozwalające m.in. na: monitorowanie oprogramowania, licencji, np. ilość wolnych licencji, koszt na jednego użytkownika, itp. prowadzenie ewidencji oprogramowania, licencji, umów, faktur, kontrahentów w tym oprogramowania darmowego i niestanowiącego wartości niematerialnych i prawnych, wielokontekstowe wyszukiwanie oprogramowania, tworzenie raportów – np. w latach, oprogramowanie jednego producenta, typ oprogramowania itd. analizę załączników np. umowy, faktury, certyfikaty, powiadomienia o kończącym się terminie danego oprogramowania, licencji, 4) ZSI-FK - Moduł środki trwałe – służy do ewidencji środków trwałych, wartości niematerialnych i prawnych oraz pozostałych środków trwałych tj. wszystkie ruchy na środkach i wartościach które muszą być księgowane (przyjęcie na stan, przekazanie, likwidacja). Ponadto służy też do naliczania amortyzacji. Wszystkie operacje w tym module są przekazywane do księgi głównej i księgowane na kontach. Umożliwia wszechstronne zarządzanie wszystkimi typami środków trwałych przez cały cykl ich życia, z zachowaniem szczegółowych informacji dotyczących: daty nabycia, amortyzacji, nr seryjnego lokalizacji itd. Nie zawiera ewidencji oprogramowania darmowego. Ale też weryfikuje w związku z tym komputery w zakresie księgowym, np. takie jak przyjęcie na stan, amortyzacja. (…). 5) E. P. – system antywirusowy, którego dodatkową funkcją jest skanowanie w czasie rzeczywistym uruchomionego oprogramowania, tym samym jest używany jako uzupełnienie w wykrywaniu nielegalnego oprogramowania. Chodzi o to, że podczas skanowania pod kątem wirusów sprawdza on oprogramowanie, ale nie prowadzi ewidencji komputerów i zawartego na nich oprogramowania. E. wykrywa zagrożenia występujące na komputerach, ale nie zlicza poszczególnych licencji oprogramowania. To nie generuje dodatkowych kosztów. Poza pierwszym programem eA., pozostałe programy są programami wspomagającymi. Nie służą do weryfikowanie oprogramowania na komputerach roboczych.*

(akta kontroli str. 1978-1984)

[23] Do dnia rozpoczęcia kontroli.
[24] Do 26 października.
[25] M. było to system służący min. do zarządzanie uprawnieniami do oprogramowania.
[26] Dalej: ZSI-FK.
[27] E. P. to program antywirusowy

Dyrektor Wydziału wyjaśnił, że weryfikacja zasobów oprogramowania przy pomocy aplikacji eA. odbywała się doraźnie lub wedle potrzeb. Nie każde jego wykorzystanie było udokumentowane w formie raportów.

(akta kontroli str. 1135-1138, 1548)

Powołany przez NIK biegły stwierdził, że: w *systemie eA.: 1) Jednostka Kontrolowana nie prowadzi monitoringu stopnia wykorzystania licencji. Nie utrzymuje w systemie aktualnych danych o wszystkich posiadanych licencjach, aby monitorować ich stopień wykorzystania; 2) Jednostka Kontrolowana nie prowadzi udokumentowanych, regularnych przeglądów oprogramowania na zasobach zarejestrowanych w systemie eA.*

(akta kontroli str. 1957-1971)

Dodatkowo biegły stwierdził, że: *biorąc pod uwagę ustalenia związane z: brakiem zapewnienia kompletności danych na temat wszystkich posiadanych i wykorzystywanych licencji w ramach stosowanych narzędzi do monitorowania licencji, brakiem zbierania danych w trybie rzeczywistym i ciągłym na innych zasobach niż komputery Windows, brakiem weryfikacji programów typu freeware/portable oraz brakiem zidentyfikowanych skutecznych mechanizmów kontrolnych w tym zakresie ocena Biegłego w zakresie rzetelności, efektywności i funkcjonalności stosowanego narzędzia do monitorowania licencji jest negatywna.*

(akta kontroli str. 1957-1971)

Dyrektor Wydziału wyjaśnił, że: *Zarządzanie oprogramowaniem i licencjami w UMS jest prowadzone głównie przez autorski system I., który prowadzi statystyki wykorzystania licencji. Na 30 dni przed wygaśnięciem danej licencji, system informuje administratora o konieczności przedłużenia licencji celem zachowania ciągłości pracy UM. (…). We wskazanym wyżej systemie istnieje możliwość rejestrowania zapotrzebowania na wymagane w pracy licencje oprogramowania, co świadczy o tym, że Wydział Informatyki zarządza i nadzoruje oprogramowaniem i licencjami. Dzięki powyższym mechanizmom Winf nie dopuszcza do naruszania warunków licencji.* (…). *Przeglądy licencji, monitorowanie stanu użycia i legalności licencji prowadzone są zgodnie z zasadami ujętymi w paragrafie 16 wskazanego powyżej Zarządzania Prezydenta, za pomocą aplikacji I. WINF Licencje, w której to wdrożono m.in. mechanizm powiadamiania o zbliżającym się terminie wygaśnięcia licencji. Dodatkowo w przeglądach oraz monitorowaniu stanu użycia oprogramowania wykorzystywany jest system eA.. (…).* Weryfikacja zasobów oprogramowania przy pomocy aplikacji eAuditor odbywała się doraźnie, lub wedle potrzeb.

(akta kontroli str. k. 1137 k. 1425, 1303-1306, 1548-1551)

Brak wystarczającego stopnia wykorzystania oprogramowania e-A., w tym nieprowadzenie cyklicznie (minimalnie raz w roku) przeglądu licencji skutkującego m.in. wykryciem przez biegłego oprogramowania, na które jednostka nie posiadała ważnej licencji opisano w sekcji „Stwierdzone nieprawidłowości".

Na wybranej próbie dziesięciu komputerów w strukturze Urzędu, przeanalizowano zawarte na nich oprogramowanie (pięciu oprogramowaniem eA. oraz pięciu w systemie I.). Pięć wybranych losowo komputerów[28] zweryfikowano programem eA., pod kątem zainstalowanego na nich oprogramowania, z danymi zweryfikowanymi bezpośrednio przez pracownika Wydziału i ustalono że, dane te nie były zgodne. Program eA. nie generował danych na temat wszystkich

[28] Zweryfikowano komputery o następujących nazwach: j.10, k.10, m.10, s.10, w.10.

zainstalowanych programów. Potwierdzone rozbieżności dotyczyły pięciu programów[29] w każdym z badanych komputerów. Dokonujący weryfikacji pracownik oraz kierownik Referatu oprogramowania oświadczyli, że skontaktowali się z twórcą oprogramowania w celu naprawy funkcjonalności programu eA. W przypadku zweryfikowania zgodności użytkowanego oprogramowania w systemie I., na próbie pięciu[30] komputerów stwierdzono pełną zgodność w zakresie tego co wykazał system z weryfikacją tego co było użytkowane na poszczególnych komputerach.

(akta kontroli str. 833-881)

Dyrektor Wydziału wyjaśnił, że: (…) *oprogramowanie eA. rozpoznaje zainstalowane programy na stacjach roboczych w oparciu o szereg zmiennych, które muszą wystąpić, aby program zakwalifikował „zero-jedynkowo" występowanie bądź nie danej aplikacji na wskazanej stacji roboczej. Przede wszystkim system eA. bazuje na szeregu tzw. wzorców oprogramowania – wzorców publicznych, które zbudowane zostały przez producenta oprogramowania i na ich podstawie odbywa się weryfikacja czy na danej stacji jakieś zdefiniowane we wzorcach publicznych oprogramowanie występuje bądź nie. (…) rozpoznawanie i inwentaryzacja oprogramowania stanowi kolejną z wielu funkcjonalności tego systemu i na przykładzie kontroli widać, że nie jest to system doskonały. (…). Oprogramowanie eA. zapewnia wsparcie dla następujących systemów operacyjnych: MS W. oraz L.*

(akta kontroli str. 1303-1348)

W uzupełnieniu złożonych wyjaśnień Dyrektor Wydziału odnośnie przyczyn utrzymywania oprogramowania eA. stwierdził, że: *Oprogramowanie eA. pozwala zdalnie skanować zawartość komputera w zakresie sprzętu i oprogramowania. Pozwala wykryć nieautoryzowane oprogramowanie. Pozostałe programy bazują na tym co wprowadzi do nich operator na podstawie dokumentów źródłowych. Mimo swoich niedoskonałości eA. spełnia wymagania postawione przez WINF. Program wykrył nielegalne oprogramowanie. Program eA. nie ma zaprogramowanego badania warunków licencji. Ponadto chcę dodać, że eA. wykazał program I.V. jako freeware, czyli darmowy, z uwagi na takie wzorce publiczne. Jeśli chodzi o I. to aplikacje, które weryfikował to aplikacje, które wynikały z I.-a jako systemu. Program e-A. to program do skanowania zasobów Urzędu, które nie wykrywa programów chmurowych i tego co zostało zauważone, to na przykład przeglądarek.*

(akta kontroli str. 1978-1981)

Czterema głównymi producentami oprogramowania dla Urzędu (taka sama kolejność występowała w zakresie jego wykorzystania) byli M., E., C., T.

(akta kontroli str. 340)

W okresie objętym kontrolą pracownikami Urzędu przestały być 343 osoby. Na wybranej losowo próbie 40 byłych pracowników ustalono, że po zaprzestaniu świadczenia pracy, oprogramowanie było zwolnione i dostępne dla innego pracownika. Usunięcie / nadanie uprawnień do korzystania z oprogramowania wykonywane było w systemie I. i uwzględniane w spisie oprogramowania. W trakcie usuwania/nadawania tych uprawnień korzystano z systemu M.

(akta kontroli str. 883-942)

Dyrektor Wydziału wyjaśnił, że: *w Urzędzie funkcjonował system usuwania uprawnień dla poszczególnych użytkowników. Po okresie 6 miesięcy nie następował brak zwalniania licencji w przypadku aplikacji webowych ponieważ te przekazywane były innej osobie. Ponadto ilość dostępowa licencji była nieograniczona w przypadku aplikacji webowych. Oprogramowania systemowe było odinstalowywane po to, by*

[29] „G. Ch.", „M. F.", „Z.", „J.", „A. R.".
[30] Zweryfikowano komputery o następujących nazwach: AD., A., EP., KK., GM.

nie zostały po nim ślady pracy dotychczas pracującego na nim pracownika i oprogramowanie to także było od razu wykorzystywane. (…) niewykorzystywane oprogramowanie jest odinstalowane i czeka na przekazanie nowej osobie. (…). Aplikacje (…) nie są kasowane ze względu na to, że są webowe. Po prostu dostęp przekazywane są innej osobie, (…). Natomiast jeśli chodzi o oprogramowanie podstawowe to jest ono przeinstalowywane i przygotowywane pod potrzeby innego pracownika. Chodzi (…) o to, by nie zostawał ślad o innym pracowników, jakieś elementy jego pracy (…). Doprecyzowując. praktycznie całość aplikacji jest instalowana sieciowo. Sporadyczne wyjątki stanowią te instalacje którą są przechowywane na serwerze dostępne dla uprawnionego pracownika Wydziału Informatyki Urzędu. Instalacje oprogramowania zazwyczaj odbywają się w sposób automatyczny przez instalatora systemu.

(akta kontroli str. 1509-1513)

Na wybranej próbie dziesięciu licencji[31] stwierdzono, że w systemie I. przechowywane były umowy, licencje, dowody zakupu, certyfikaty autentyczności oraz warunki licencyjne. Dostęp do poszczególnych aplikacji posiadały uprawnione osoby[32], wykazane w systemie I. Przechowywane w nim były także pliki instalacyjne lub adresy WWW, pod którymi znajdowały się pliki instalacyjne.

(akta kontroli str. 1031-1131, 1531-1541)

Urząd posiadał 14 programów, których autorami było siedmiu pracowników Wydziału. Były one opracowane w ramach świadczenia stosunku pracy. Żaden z programów nie był wytworzony na podstawie umowy cywilnoprawnej.

(akta kontroli str. 341, 354-356)

Dyrektor Wydziału wyjaśnił, że: *Kod źródłowy aplikacji pisanych przez programistów UMS wygenerowany w systemie I. jest dostępny dla pracowników WINF. Tylko producent ma dostęp do kodu źródłowego jądra systemu w przypadku komercyjnego rozwiązania. Wynik generowanie I-a składa się z kodu producenta i z kodu programisty z Urzędu. Ten kod od programisty z Urzędu jest dostępny dla uprawnionych pracowników w Urzędzie. Idea systemu I. jest taka, że na podstawie wskazanych funkcjonalności on generuje kod.*

(akta kontroli str. 1978-1984)

Spis licencji w systemie I. pozwalał na identyfikację liczby wolnych licencji oraz wskazywał osoby odpowiedzialne za weryfikowanie danych dotyczących rzeczywistego wykorzystania licencji. W Urzędzie brak było nieużytkowanego oprogramowania, a tylko jeden program (WINZIP[33]) z 283 zaewidencjonowanych w systemie I., był wykorzystany w stopniu poniżej 30%. Był on przeznaczony do archiwizowania danych i zastąpiono go programem 7-Zip. Licencja na ten program była wieczysta i Urząd nie ponosił w związku z tym żadnych kosztów.

(akta kontroli str. 1531-1542)

W Urzędzie nie stwierdzono oprogramowania, które byłoby kupione i nie zostałoby zainstalowane.

(akta kontroli str. 1509-1513)

1.4. Zapewnienie przestrzegania zasad prawidłowego użytkowania oprogramowania oraz audyty legalności oprogramowania.

Dane dotyczące posiadanych przez Urząd licencji były przechowywane w ww. systemie I. Przeglądów w zakresie oprogramowania dokonywali pracownicy Wydziału, np. Główny Specjalista ds. administrowania systemami obsługi

[31] ZSI-FK, eA., T.V., A. A. P. 2017, KIR S. 2.0, N.++, A. 2020, M. B. T., E. P., M. P.
[32] Uprawnienie były nadawane dla konkretnej osoby na konkretne uprawnienie.
[33] WINZIP to oprogramowanie służące do archiwizacji danych.

interesantów i obiegu dokumentów – na bieżąco w zakresie analizy wykorzystania licencji oraz analizy zakupów; Inspektor ds. gospodarki sprzętem i oprogramowaniem oraz Kierownik Referatu Wsparcia Użytkowników w przypadku zakupu środków trwałych, zmiany użytkowników lub zmiany sprzętu; Dyrektor Wydziału i Zastępca Dyrektora ds. systemów w przypadku tworzenia planu zakupów oraz aktualizacji planu zakupów (dodatkowo Dyrektor przed przygotowaniem do utylizacji sprzętu i oprogramowania) oraz Administratorzy systemu którzy odpowiedzialni za oprogramowanie analizując potrzeby[34]. Środowiska wirtualne, deweloperskie, testowe i szkoleniowe nadzorowali administratorzy systemów. Przeglądy oprogramowania obejmowały stacje robocze bez urządzeń mobilnych (laptopy, tablety, smartfony).

(akta kontroli str. 341-342, 1531-1541)

Procedura postępowania w sytuacji stwierdzenia m.in. zainstalowania nielegalnego oprogramowania, określona została w załączniku nr 8 do Polityki Bezpieczeństwa „Klasyfikacja incydentów bezpieczeństwa teleinformatycznego w Urzędzie". W latach 2019-2022 (do dnia rozpoczęcia kontroli) Urząd nie wykazał wystąpienia takich przypadków.

(akta kontroli str. 342)

Powołany biegły stwierdził, że: „*Z przeprowadzonych testów na wybranej próbie komputerów zidentyfikowano 3 przypadki zainstalowanego oprogramowania I., dla którego nie potwierdzono posiadania przez Jednostkę Kontrolowaną licencji a na wybranych stacjach roboczych zidentyfikowano zainstalowaną wersję oprogramowania firmy O. J. w wersji wyższej niż 8u211 - której to licencjonowanie przez firmę O. zostało zmienione - w efekcie przestaje być darmową do użytku komercyjnego od 16 kwietnia 2019 roku*, co opisano w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 1957-1971)

Nie stwierdzono zainstalowania na komputerach Urzędu oprogramowana, którego licencje wygasły. W Urzędzie określona została procedura likwidacji aktywów trwałych (Zarządzenie Prezydenta Nr 174/19[35]). Na jej podstawie opracowana została przez Wydział „Procedura likwidacji sprzętu i oprogramowania". Wycofywanie z użycia sprzętu i oprogramowania z wygasłymi licencjami miało odbywać się po jego zakwalifikowaniu do likwidacji i akceptacji przez Dyrektora Wydziału. Miała być ona poprzedzona analizą przeprowadzoną z Kierownikiem Referatu Wsparcia Użytkowników oraz Inspektorem ds. gospodarki sprzętem i oprogramowaniem.

(akta kontroli str. 342, 1531-1541)

Dyrektor Wydziału wyjaśnił, że poza oprogramowaniem wykrytym przez biegłego nie było podobnych incydentów w okresie objętym kontrolą. Ich przyczyną mogło być nieświadome ściągnięcie aplikacji. Natomiast w przypadku nieprawidłowości związanych z użytkowaniem oprogramowania działania naprawcze podejmowane były na bieżąco.

(akta kontroli str. 1509-1513)

W uzupełnieniu złożonych wyjaśnień Dyrektor stwierdził, że: *Na podstawie pozostawionych plików mogę potwierdzić wykonane przeglądy na koniec 2019 i 2020 r. dotyczące zainstalowanego oprogramowania. Wynikało to z ograniczonej*

[34] Wykaz oprogramowania i osób nadzorujących znajduje się w systemie I.-WINF L.

[35] Zarządzenie Prezydenta Miasta Szczecin z 7 maja 2019 r. w sprawie powołania Stałej Komisji Likwidacyjnej ds. likwidacji rzeczowych składników majątku ruchomego Urzędu Miasta (zm. Zarządzenie Nr 108/21 Prezydenta z 1 marca 2021 r., Zarządzenie Nr 482/21 Prezydenta Miasta Szczecin z 6 października 2021 r. oraz Zarządzenie Nr 207/22 Prezydenta z 16 maja 2022 r.).

ilości pracowników posiadających wiedzę i uprawnienia do dokonywania ww. czynności. W Urzędzie na chwilę obecną są tylko dwie osoby, które mogłyby przeprowadzić takie przeglądy. Do maja 2022 roku były tylko dwie osoby, kiedy to odeszła trzecia osoba (przed majem 2022 roku były trzy osoby). Tu w rachubę wchodzi posiadanie odpowiednich uprawnień administratora systemu eA., ale też odpowiedniej wiedzy i umiejętności – wynikających z doświadczenia i przeszkolenia. Nadmiar obowiązków spowodowany jest brakiem kadry i problemami z naborem. eA., daje możliwość zweryfikowania, jakie pliki znajdują się na poszczególnych komputerach w Urzędzie Miasta. To więc musi też być osoba zaufana na wgląd w zawartość komputera. Pomimo braku procedury dotyczącej częstotliwości przeglądów, planowane jest procedura dotycząca z określoną częstotliwością wykonywanie przeglądów oprogramowania w Urzędzie, w polityce bezpieczeństwa.

(akta kontroli str. 1978-1981)

W okresie objętym kontrolą Urząd nie uiszczał kar związanych z nielegalnym lub nieprawnie użytkowanym oprogramowaniem.

(akta kontroli str. 343)

W Urzędzie określono zasady zbywania sprzętu IT[36]. W latach 2019-2022 (do 30 czerwca) przekazano 204 sztuk zainstalowanego oprogramowania m.in. na rzecz Zarządu Budynków i Lokali Komunalnych i Straży Miejskiej. W powyższym okresie Urząd zlikwidował również 954 sztuki oprogramowania.

(akta kontroli str.342, 360-390, 392)

Dyrektor wyjaśnił, że: *przed zbyciem lub przed przekazaniem dyski twarde były niszczone przy pomocy urządzenia E. Z czynności tej nie były sporządzane protokoły. Natomiast jeśli komputer użytkowany przez Urząd był przekazywany wraz z dyskiem, to dyski były dziesięciokrotnie nadpisywane.*

(akta kontroli str. 343, 1141-1142)

W uzupełnieniu złożonych wyjaśnień Dyrektor stwierdził, że: *Jeśli chodzi o bezpieczeństwo danych to komputery robocze w Urzędzie Miasta są to stacje robocze które łączą się z serwerem Urzędu, na którym znajdują się dokumenty i bazy danych. Na serwerach są zapisywane dane wrażliwe. Z uwagi na to, iż w Urzędzie używany jest E. demagnetyzer do całkowitego niszczenia dysków, czyszczenie dysków jest używane tylko w przypadku przekazywania sprzętu oświacie, do naszych jednostek, Zapisy istniejącej procedury uważałem za wystarczające, skoro dyski i tak ulegały zniszczeniu a potem likwidacji i z tego robiono protokoły likwidacyjne. Fizyczne niszczenie dysków odbywa się w siedzibie Wydziału Informatyki. W opracowanej procedurze likwidacji sprzętu planowane jest zamieszczenie dodatkowego zapisu dotyczącego dokumentowania zniszczenia dysków demagnetyzerem".* (akta kontroli str. 1980)

W Urzędzie w latach 2019-2022 przeprowadzone były przez podmioty zewnętrzne cztery audyty oprogramowania. Dotyczyły one m.in.: poprawności konfiguracji oraz działania środowisk centralnego zarządzania oprogramowaniem antywirusowym E. P. związanego z planowanym postępowaniem na wybór nowego oprogramowania antywirusowego; oceny zaawansowanej migracji Systemu Urzędu zbudowanego na platformie M. D. AX 2009 na platformę M. D. 365, celem oceny było dostarczenie analizy środowiska IT, wdrożonego oprogramowania, jego wykorzystania a także weryfikacja ewentualnych ograniczeń związanych z otoczeniem formalno-prawnym; Nadzoru Systemu Zarządzania Jakością w Wydziale w zakresie Zarządzanie zasobami – infrastruktura oraz środowiska funkcjonowania procesów, zakupy IT,

[36] Zarządzenie Prezydenta nr 174/19 z 7 maja 2019 r. w sprawie powołania Stałej Komisji Likwidacyjnej ds. likwidacji rzeczowych składników majątku ruchomego Urzędu Miasta (ze zm.).

Wsparcie użytkowników zasobów IT oraz zakupy sprzętu, oprogramowania i usług informatycznych, ocena dostawców; Zarządzanie środowiskiem pracy. W trzech audytach nie zostały stwierdzone nieprawidłowości. W wyniku audytu dotyczącego zweryfikowania poprawności konfiguracji oraz działania środowiska centralnego zarządzania E. P. sformułowanych zostało sześć rekomendacji w tym: „*w miarę możliwości ujednolicenie środowiska Windows do wspieranych wersji przez producenta M. – ułatwia to model zarządzania aktualizacji systemu operacyjnego", „zalecamy usunięcie niewykorzystanych zadań Klienta a następnie ich ponowną konfigurację w oparciu o aktualne polityki wykorzystywane w firmie wraz z wykorzystaniem unikatowych nazw zadań wraz z wykorzystaniem komentarzy. Zaleca się również wielokrotne wykorzystanie tych samych zadań."*

(akta kontroli str. 260-309, 310-314, 338-339)

Rekomendacje zostały wykonane.

(akta kontroli str. 1985)

W procedurach zarządzania licencjami nie określono procedur związanych z korzystaniem z usług zewnętrznych.

(akta kontroli str. 36-61, 1907-1934)

Stwierdzone nieprawidłowości

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

1. W procedurach Urzędu[37] nie doprecyzowano zasad i kryteriów weryfikacji oprogramowania (np. pod kątem bezpieczeństwa w procesie nabywania); zasad utrzymania kompletności i aktualności ewidencji; zasad dystrybucji i redystrybucji licencji oraz wycofywania licencji; zasad i częstotliwości okresowych przeglądów; zasad monitorowania stanu użycia i legalności; zasad zarządzania oprogramowaniem z uwzględnieniem wszystkich rodzajów urządzeń końcowych (np. tabletów i smartfonów). Nie ustanowiono również mechanizmu kontrolnego zapewniającego okresowe sprawdzanie wszystkich stacji roboczych, serwerów, urządzeń mobilnych i udostępnionych udziałów sieciowych użytkowników pod kątem obecności nieautoryzowanego oprogramowania, w tym weryfikacji oprogramowania freeware pod kątem możliwości użytkownika komercyjnego.

(akta kontroli str. 36-61, 1907-1944)

Powołany przez NIK biegły stwierdził m.in., że określone zasady postępowania nie obejmowały całego cyklu związanego z zarządzaniem licencjami. Nie określały szczegółowych zasad weryfikacji pod kątem bezpieczeństwa w procesie nabywania licencji oraz wycofywania licencji, ewidencjonowania (z uwzględnieniem wszystkich rodzajów urządzeń końcowych) i utrzymania kompletności i aktualności ewidencji, dystrybucji i redystrybucji licencji, częstotliwości okresowych przeglądów, monitorowania stanu użycia i legalności.

(akta kontroli str. 1957-1971)

Biegły zalecił ustanowienie i wdrożenie szczegółowych zasad zarządzania licencjami, które będą obejmowały co najmniej takie kwestie jak: zasady (listę kontrolną) nabywania, w tym weryfikacji pod kątem bezpieczeństwa oraz zasad wycofywania licencji; zasady gromadzenia i przechowywania dowodów zakupu; zasady ewidencjonowania (z uwzględnieniem wszystkich rodzajów urządzeń końcowych) i utrzymania kompletności i aktualności ewidencji; zasady dystrybucji i redystrybucji licencji; zasady i częstotliwość okresowych przeglądów; zasady monitorowania stanu użycia i legalności. *(akta kontroli str.1957-1971)*

[37] Tj. regulaminach organizacyjnych Urzędu, regulaminach określających szczegółowe zakresy zadań realizowanych przez jednostki organizacyjne Urzędu, regulaminach wewnętrznych Wydziału **i** Polityce Bezpieczeństwa.

Dyrektor Wydziału wyjaśnił, że: *Zasady zarządzania licencjami zostały określone w Polityce Bezpieczeństwa w szczególności w Załączniku Nr 4 (…). Dodatkowo dla zapewnienia nadzoru nad dystrybucją licencji i oprogramowania została Zarządzeniem Prezydenta Nr 327/19 z dnia wdrożona procedura nadawania uprawnień, będąca ważnym elementem procesu zarządzania oprogramowaniem. Nadawanie uprawnień odbywa się przy pomocy autorskiego rozwiązania w systemie M. i umożliwia tworzenie raportów dostępności do danego oprogramowania. W ramach procedur Systemu Zarządzania Jakością ISO 9001 opracowano procedurę Nr P-II-01 – Nadzór i aktualizacja oprogramowania oraz systemów komputerowych, która ma być wdrożona do nowej wersji Polityki Bezpieczeństwa. Wydział opracował i wdrożył również procedurę likwidacji sprzętu Informatycznego i oprogramowania zatwierdzoną w dniu 9 maja 2021 r. przez Dyrektora Wydziału. Zarządzanie oprogramowaniem i licencjami w UMS jest prowadzone głównie przez autorski system I., który prowadzi statystyki wykorzystania licencji. Na 30 dni przed wygaśnięciem danej licencji, system informuje administratora o konieczności przedłużenia licencji celem zachowania ciągłości pracy UM. W systemie I. jest prowadzona pełna ewidencja, statystyka wykorzystanych licencji oraz zamieszczone są skany dowodów zakupu w postaci umów, faktur, certyfikatów oraz numerów seryjnych licencji. We wskazanym wyżej systemie istnieje możliwość rejestrowania zapotrzebowania na wymagane w pracy licencje oprogramowania, co świadczy o tym, że Wydział Informatyki zarządza i nadzoruje oprogramowaniem i licencjami. Dzięki powyższym mechanizmom Winf nie dopuszcza do naruszania warunków licencji. W procesie nabywania (par. 16 ust. 4), oraz wycofywania oprogramowania (par. 9 ust. 4, pkt 5), a także dystrybucji i redystrybucji licencji uwzględniane są zasady bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu wprowadzone Zarządzeniem Nr 150/18 (…).*

Przeglądy licencji, monitorowanie stanu użycia i legalności licencji prowadzone są zgodnie z zasadami ujętymi w paragrafie 16 wskazanego powyżej Zarządzania Prezydenta, za pomocą aplikacji I. WINF Licencje, w której to wdrożono m.in. mechanizm powiadamiania o zbliżającym się terminie wygaśnięcia licencji. Dodatkowo w przeglądach oraz monitorowaniu stanu użycia oprogramowania wykorzystywany jest system eA.. Zasady i częstotliwość okresowych przeglądów zostały określone w par. 16 Polityki Bezpieczeństwa Informacji w ust. 14. Zasady monitorowania usług zostały określone w par. 16 Polityki Bezpieczeństwa Informacji w ust. 17 i ust. 20.

W ramach weryfikacji systemów pod kątem bezpieczeństwa w procesie nabywania licencji Wydział Informatyki wraz z inspektorem Ochrony Danych opracował ankietę bezpieczeństwa, która zostaje przekazana Wykonawcom przed zawarciem umowy głównej i umowy powierzenia przetwarzania danych. Każdy Wykonawca dostarczający system, w którym przetwarzane są dane osobowe jest weryfikowany pod kątem bezpieczeństwa przez administratorów Wydziału Informatyki, co jednocześnie odnajduje swoje odzwierciedlenie w specyfikacji i umowach. Działanie to nie jest objęte specjalną procedurą, lecz stanowi element dobrej praktyki. Zasady monitorowania stanu użycia i legalności nie są objęte dedykowaną procedurą.

Jednak mimo braku takiej procedury, administratorzy systemów dokonują monitoringu zgodnie z obowiązkami wynikającymi z zakresu czynności.

Zasady monitorowania mimo, że nie są ujęte bezpośrednio w procedurach są spójne z regulaminem korzystania z zasobów UM, a stan użycia i legalności można sprawdzić w dedykowanych systemach. Oprogramowanie jest nadzorowane a pracownicy Urzędu są informowani o zagrożeniach i konsekwencjach prawnych.

(akta kontroli str. 1548-1551, 1686-1688)

W przywołanych przez Dyrektora Wydziału uregulowaniach w § 9, 16, 17 i załączniku nr 4 do Polityki Bezpieczeństwa nie było postanowień, o których mowa

w wyjaśnieniach. W ocenie NIK brak określenia ww. zasad było działaniem nierzetelnym i skutkowało m.in. nieokreśleniem częstotliwości dokonywania przeglądów oprogramowania.

(akta kontroli str. 1907-1926)

2. W Urzędzie nie potwierdzono prowadzenia audytu, ani weryfikacji programów typu freeware / portalbe oraz nie wprowadzono skutecznych mechanizmów kontrolnych w tym zakresie.

(akta kontroli str. 1960)

Biegły stwierdził, że: *W toku prowadzonych czynności przeprowadzono weryfikację zainstalowanego oprogramowania pod kątem nielegalnych programów na podstawie komputerów wytypowanych z systemu eA. Z przeprowadzonych testów na wybranej próbie komputerów zidentyfikowano 3 przypadki zainstalowanego oprogramowania I., dla którego nie potwierdzono posiadania przez Jednostkę Kontrolowaną licencji. Licencja I. jest darmowa, ale tylko do użytku niekomercyjnego i wymaga zakupu licencji dla Urzędu. Ponadto, w wyniku analizy zebranych danych z przeprowadzonych testów na wybranych stacjach roboczych zidentyfikowano zainstalowaną wersję oprogramowania firmy O. J. w wersji wyższej niż 8u211 - której to licencjonowanie przez firmę O. zostało zmienione - w efekcie przestaje być darmową do użytku komercyjnego od 16 kwietnia 2019 roku (od wersji O. J. 8 SE o numerze 211 (8u211, 1.8.0_211-b12).*

(akta kontroli str. 1969)

Dyrektor Wydziału wyjaśnił, że (…) *Przeglądy licencji, monitorowanie stanu użycia i legalności licencji prowadzone są zgodnie z zasadami ujętymi w paragrafie 16 wskazanego powyżej Zarządzania Prezydenta, za pomocą aplikacji I. WINF Licencje, w której to wdrożono m.in. mechanizm powiadamiania o zbliżającym się terminie wygaśnięcia licencji. Dodatkowo w przeglądach oraz monitorowaniu stanu użycia oprogramowania wykorzystywany jest system eA..(…) Wydział Informatyki na bieżąco prowadzi przegląd instalowanego oprogramowania, które jest monitorowane przez systemy eA. i system E. Oba systemy pracują non stop, (…) stąd brak raportów potwierdzających wykonywanie audytów w zaplanowanych odstępach czasu. Działania te są prowadzone na bieżąco, a samo logowanie do systemu nie generuje raportu. Wynik działania programu ze szczególnym uwzględnieniem sytuacji alarmowych jest na bieżąco przeglądany przez pracowników Wydziału Informatyki (WINF), którzy podejmują odpowiednie działania. Nie ma potrzeby drukowania i zbierania dowodów z każdego skanowania komputerów bo wersja papierowa jest nieekonomiczna i nie daje możliwości obróbki elektronicznej pod kątem statystyk i raportów. Dowody przeglądów są zbierane tylko w sytuacji wykrycia incydentu związanego z instalacją niedozwolonego oprogramowania lub naruszenia zasad bezpieczeństwa sieci jako dowód w sprawie.*

(akta kontroli str. 1548-1551)

Dyrektor Wydziału wyjaśnił również, że: *na poziomie systemowym zablokowana została, możliwość instalowania przez pracowników oprogramowania prywatnego na sprzęcie Urzędu. Natomiast stwierdzone przypadki występowania oprogramowania do użytku niekomercyjnego, przez powołanego przez NIK biegłego, nie wymagały instalacji, dlatego zostało odnalezione na komputerze poddanym weryfikacji.* Odnośnie stwierdzonych przez biegłego nieprawidłowości Dyrektor Wydziału wyjaśnił że: „*Wydział Informatyki nie dysponował wiedzą o zmianie warunków licencjonowania na wykorzystywanie oprogramowania J. przez O. Zmiana warunków licencji została wprowadzona nieoczekiwanie, a informacja o tym prawdopodobnie była zamieszczana tylko w okienku informacyjnym wyświetlanym podczas instalacji lub upgread'u oprogramowania J., które wykonuje się w sposób automatyczny. Ponadto tak istotna informacja była zamieszczona*

w języku angielskim w sposób niejasny i mało wyeksponowany, co jest praktyką z perspektywy prawnych reguł wprowadzania zmian do umowy bardzo wątpliwą, a wręcz niedopuszczalną - niezależnie od prawa właściwego dla danej umowy licencyjnej. Oprogramowanie w chwili instalacji było darmowe. Podczas użytkowania i samoczynnej aktualizacji stało się komercyjne, jednak UM nigdy nie wykorzystywał tego oprogramowania do celów komercyjnych. J. wykonuje automatyczne aktualizacje w tle, nie pytając o zgodę i nie informując o zmianie warunków licencji. Użytkownik nie musiał wyrażać woli zmiany oprogramowania na nowszą wersję. System sam o tym decydował wymuszając decyzję na użytkowniku, który nie był i nie mógł być świadomy na co się godzi. Oprogramowanie J. nie jest wykorzystywane w aplikacjach tworzonych przez Wydział Informatyki na własne cele urzędu z czego wynika, że nie prowadzona była analiza sposobu licencjonowania tego oprogramowania w celu wykorzystania go wewnętrznie. J. jest wykorzystywana przez producentów różnego oprogramowania i przez wiele lat była darmowym oprogramowaniem narzędziowym niezbędnym do prawidłowego działania różnych aplikacji oraz funkcjonalności stron internetowych.(…). Z informacji uzyskanych od dostawcy systemu obiegu dokumentów (…) wynika, że niezbędne elementy J. wykryte przez aplikacje eA. są legalnie i nieodpłatne. (…) gdyby kontrolowany był świadom konsekwencji zmian licencyjnych, o których mowa wyżej, to i tak miałby podstawy do przyjęcia, iż korzystanie z oprogramowania J. w tym zakresie mieści się w granicach listy zaakceptowanych produktów O.[1]. Przeciwna argumentacja byłaby dość niecodzienna, gdyż musiałaby się wiązać z innego rodzaju komunikacją ze strony COI oraz wzbogaconą treścią konsultantów na infolinii. (…). Wydział Informatyki Urzędu nie miał podstaw do stwierdzenia, że licencje oprogramowania J. stały się płatne i nie miał takiej oficjalnej informacji od dostawcy oprogramowania lub jego producenta. Z informacji uzyskanych w Internecie wynika, że w 2019 roku firma O. wprowadziła ograniczenie w możliwości nieodpłatnego korzystania z oprogramowania J. Udostępniono możliwość nieodpłatnego korzystania z licencji wyłącznie do celów osobistych oraz na użytek deweloperski (np. do rozwijania, testowania lub demonstrowania aplikacji). Pracownicy Wydziału Informatyki wykorzystują oprogramowanie J. wyłącznie do użytku deweloperskiego, w szczególności do testowania i demonstrowania oprogramowania, co jest zgodne ze stanowiskiem firmy O. (…). Wzorcowa wersja instalacji oprogramowania J. została pobrana kilka lat temu ze stron producenta, a następnie przeniesiona na trwały nośnik aby przyspieszyć i ujednolicić proces instalacji. Pracownicy referatu technicznego nie korzystają z instalacji za pośrednictwem strony producenta, (…) Wydział Informatyki instalując starą wersję J. z własnych zasobów nie korzysta ze strony producenta, tym samym nie mógł posiąść wiedzy na temat zmiany sposobu licencjonowania. Oprogramowanie jak już wcześniej wskazano samo w sposób automatyczny aktualizowało się do nowszych wersji nie wyświetlając komunikatów przedstawionych przez biegłego (…) pracownicy Wydziału Informatyki nie stwierdzili żadnych komunikatów pokazujących się na ekranach monitorów podczas automatycznych aktualizacji. (…) oprogramowanie I.V, które nie wymaga instalacji a tym samym praw administratora, nie było wgrywane ani instalowane przez pracowników (…). Pracownik wgrał program na służbowym komputerze bez wiedzy i zgody przełożonego oraz pracowników Wydziału Informatyki. (…). Pracownik wykorzystywał oprogramowanie wyłącznie do celów prywatnych jako osoba fizyczna. Zatem oprogramowanie nigdy nie było wykorzystywane na potrzeby zadań realizowanych przez Urząd, tym samym nie było używane do celów komercyjnych.

(akta kontroli str. 1604-1605, 1686-1688)

[1] https://www.o…html

W ocenie NIK stosowane przez Urząd metody i procedury działania były niewystarczające, o czym świadczyło występowanie oprogramowania, na które Urząd nie posiadał ważnej licencji.

OCENA CZĄSTKOWA

Organizacja i skuteczność realizowania procesu postępowania z oprogramowaniem, a także sposób użytkowania programów komputerowych nie były w Urzędzie w pełni prawidłowe.

W Urzędzie nie określono szczegółowych zasad zarządzania licencjami, obejmujących wszystkie elementy i wymagane czynności niezbędne do skutecznej realizacji tego zadania. Urząd nie weryfikował systematycznie, mimo posiadanych narzędzi, wszystkich posiadanych zasobów pod kątem instalowania i korzystania przez pracowników z nielegalnego oprogramowania. Obsada kadrowa Wydziału, mimo podejmowanych działań w celu zatrudnienia nowych pracowników, była nieadekwatna do skali zadań Wydziału. Obejmowały one swym zakresem nie tylko Urząd, ale także pozostałe jednostki Gminy. O nieskuteczności podejmowanych działań świadczy stwierdzona w toku kontroli NIK obecność nieautoryzowanego oprogramowania na urządzeniach komputerowych. Urząd dysponował danymi o posiadanych zasobach informatycznych i stopniu ich wykorzystania (m.in. za pomocą systemu ICOR) oraz sprawował nadzór nad dokumentacją licencyjną i nośnikami oprogramowania.

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

Opis stanu faktycznego

2.1. Planowanie środków finansowych przeznaczonych na nabycie i utrzymanie licencji komputerowych (oprogramowania).

W Urzędzie planowanie potrzeb dotyczących oprogramowania było zestawiane z rzeczywistym stanem zasobów, jakim dysponowała jednostka. Proces nabywania licencji (podobnie jak pozostałych zamówień) określony został m.in. w zarządzeniach Prezydenta Nr 14/19, Nr 303/16, Nr 314/13, Nr 320/19, Nr 39/21, Nr 45/16[38]. Poszczególne Wydziały zgłaszały zapotrzebowanie na zakup oprogramowania. Weryfikacja i ocena zakupu licencji była dokonywana przez Wydział, po przesłaniu przez kierownika jednostki organizacyjnej Urzędu, zapotrzebowania oraz informacji, że oprogramowanie jest niezbędne do wykonywania obowiązków na danym stanowisku. Następnie Wydział weryfikował zasadność potrzeby i możliwość wykorzystania dostępnego w zasobach Urzędu oprogramowania, analizował stan wolnych licencji, analizował dostępność na rynku i możliwości finansowania w razie zakupu nowego oprogramowania.

(akta kontroli str. 343-346, 1638-1640)

Na podstawie przeanalizowanego postępowania o udzielenie zamówienia publicznego na świadczenie usług asysty technicznej oraz rozwoju ZSI-FK dla Gminy stwierdzono, iż proces dokonywania zakupu przebiegał zgodnie z przyjętymi zasadami, a przy określaniu przedmiotu zamówienia uwzględniono weryfikację aktywności użytkowników.

(akta kontroli str. 1638)

Urząd prowadził bazę danych na temat posiadanego sprzętu IT oraz oprogramowania. Decyzje dotyczące zakupów, były podejmowane także na podstawie zgłaszanych ustnie potrzeb na spotkaniach grup roboczych

[38] Zarządzenia dotyczyły m.in. zasad wykonywania w Urzędzie ustawy Prawo zamówień publicznych.

i przeprowadzonych analiz przez Wydział w zakresie: wydatków, wydajności systemów, wycofania z rynku produktów i brakiem wsparcia, zmiany statusu prawnego firm, poprawy bezpieczeństwa i funkcjonalności, konieczności wdrożenia nowych technologii oraz nowych zadań Gminy.

(akta kontroli str. 1638-1640)

W Urzędzie zakupiono (zaplanowane w trakcie roku) w: 2020 r. oprogramowanie A. i (T.-1 rok) dla Biura Architekta Miasta za kwotę 4,7 tys. zł oraz W. dla Biuro Dialogu Obywatelskiego za 71,4 tys. zł; 2021 r. System "S." dla Wydziału Kontroli i Audytu Wewnętrznego za kwotę 17,2 tys. zł oraz Internetowe kalkulatory podatkowe "P. D." za 103,6 tys. zł. Przyczyną zmian w planie wydatków, według oświadczenia Dyrektora Wydziału, była konieczność wykonywania zadań merytorycznych, dokonane zakupy dotyczyć miały usprawnienia pracy. W 2019 r. i 2022 r. nie wydatkowano środków na realizację zadań, które nie były pierwotnie zaplanowane.

(akta kontroli str. 1638-1644)

W latach objętych kontrolą producenci nie wystawiali faktur za nadmierne wykorzystanie licencji. Liczba licencji była ustalana na podstawie potrzeb Urzędu i możliwości finansowych. W Urzędzie w odniesieniu do programów „E. O. D." oraz „S. E. O. D." zainstalowano więcej licencji (1 500) niż pierwotnie zakładano (1 200). Dyrektor Wydziału oświadczył, że zwiększone nabycie wynikało z potrzeb jednostek Gminy, a licencje przekazane zostały nieodpłatnie przez Ministerstwo Cyfryzacji.

(akta kontroli str. 345, 826-832)

2.2. Analizy możliwości wdrożenia i efektywności wykorzystania posiadanych licencji (oprogramowania).

Urząd dokonywał analiz efektywności faktycznego wykorzystania oprogramowania za pomocą systemu I.

Najlepszym miernikiem efektywności, według oświadczenia zastępcy Dyrektora Wydziału, było wykorzystanie systemu wspomagającego obsługę komórek merytorycznych i mieszkańców. Analizy te wykonano w oparciu o dane dotyczące stopnia użytkowania systemów przeznaczonych do realizacji kluczowych procesów zarządzania.

(akta kontroli str. 347)

Dyrektor wyjaśnił, że: *Analiza stopnia użytkowania systemów: M. P. BI Pro, M. O., Z. P-1, System L. została przeprowadzona na podstawie ilości przydzielonych dostępów przez administratora w dedykowanym panelu administracyjnym danego systemu. W przypadku darmowego systemu C. W., zliczono ilość instalacji. System S. – w ramach umowy zakupiono 5 licencji, które przydzielono wskazanym pracownikom Wydziału Kontroli i Audytu Wewnętrznego. W/w dane mają również odzwierciedlenie w systemie I. umożliwiającym szybką weryfikację stopnia wykorzystania. W przypadku oprogramowania chmurowego nie mamy możliwości weryfikacji kto i ile pracuje na danym oprogramowaniu. Jeśli chodzi o kluczowe procesy zarządzania to Urząd nie posiada narzędzi do sprawdzenia (takie możliwości ma właściciel oprogramowania) jak często i jak długo i w jakim zakresie użytkownicy korzystają z tych programów. W przypadku oprogramowania aplikacji lokalnych, pewne dane można uzyskać na podstawie logowania. W przypadku systemu Z. I. i M. -a jest możliwość zweryfikowania częstotliwości logowania pracownika do systemu. Taką ewidencję prowadzi każdy system, do którego trzeba się logować. Standardowe aplikacje nie wykazują logowania do nich.*

(akta kontroli str. 1978-1981)

Urząd nie udokumentował działań w zakresie prowadzenia weryfikacji przerw w korzystaniu z komputerów. Wynikać to miało, według oświadczenia Dyrektora Wydziału, z braku rozwiązań systemowych oraz braku zasobów kadrowych, dużej liczby użytkowników (1 116) oraz oprogramowania (283), których to iloczyn generuje dużą ilość pracy.

(akta kontroli str. 956-980, 1531-1541, 1629, 1978-1981)

Poszczególne komórki Urzędu miały problemy z funkcjonowaniem oprogramowania, które zgłaszano i rejestrowano. Ich usunięcie potwierdzano w rejestrach zgłoszeń.

(akta kontroli str. 1629-1637)

Dyrektor Wydziału oświadczył, że: *zgłaszane problemy dotyczyły: zasadniczej funkcjonalności oprogramowania (np. problem w działaniu środowiska testowego, problem z operacjami, problem z drukowaniem, dodanie nowych raportów, korekta faktury, brak grupy uprawnień itp.). Problemy są niezwłocznie przekazywane wykonawcom zgodnie z procedurą ustaloną w treści umowy. Wykonawcy na bieżąco rozwiązują zgłaszane problemy. Wydział jest w posiadaniu rejestrów ww. zgłoszeń, które stanowią bazę wiedzy.*

(akta kontroli str. 1630)

Zamówienia dotyczące zakupów nowych modułów systemu ZSI-FK realizowane były w drodze zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego. Przeprowadzono postępowania w zakresie dwóch modułów o nazwie EGZEKUCJA (postępowanie BZP/39/10 z 2010 r.) oraz moduł OBSŁUGI GOSPODARKI ODPADAMI (postępowanie BZP/48/13 z 2013 r).

W 2021 r. przeprowadzono postępowanie o udzielenie zamówienia publicznego na świadczenie usług asysty technicznej oraz rozwoju ZSI-FK dla Gminy w 2021 r[39]. Na jego podstawie 1 lipca 2021 r. zawarto umowę na świadczenie przez 18 miesięcy usług asysty technicznej za kwotę wynagrodzenia wynoszącą maksymalnie 2 323 000,00 zł netto (2 857 290,00 zł brutto). Za jego realizację Urząd zapłacił w okresie od 1 lipca 2021 r. do 30 czerwca 2022 r. 1 415 550,00 zł netto (1 741 126,50 zł brutto). Postępowanie przeprowadzone zostało w trybie zamówienia z wolnej ręki, z naruszeniem przesłanek do jego zastosowania, określonych w przepisie art. 214 ust. 1 pkt 1 lit. a) i b) Pzp, co opisano w sekcji „Stwierdzone nieprawidłowości".

Urząd przeprowadził w lipcu 2021 r. na podstawie art. 83 Pzp analizę funkcjonalności poszczególnych modułów „Diagnoza stanu technicznego i merytorycznego oraz potrzeb w zakresie planowanych przedsięwzięć informatyzacji Gminy Miasto Szczecin", która została uzupełniona o opracowanie z 14 października 2021 r. „Analiza potrzeb i wymagań dla projektu ZSI-FK". Zostały one sporządzone dla potrzeb postępowania o udzielenie zamówienia publicznego na świadczenie usług asysty technicznej oraz rozwoju ZSI-FK dla Gminy[40]. W ramach analiz zbadano funkcjonalność modułów, analogiczne oferty jak i wykorzystanie modułów. Nie stwierdzono aby w ramach ZSI-FK funkcjonowały moduły nieużywane lub nieaktywne (ZSI-FK składał się z 27 obszarów funkcjonalnych, liczba użytkowników poszczególnych obszarów wynosiła od 11 do 1 065). Łączny koszt utrzymania tego systemu w latach 2019-2022 wyniósł 6 262,1 tys. zł, liczba logowań przekroczyła 61 mln.

(akta kontroli str. 1239-1244, 1657-1685, 1689-1892)

[39] Diagnozę wykonał C. D. i A. P. w lipcu 2021 r. Analizę potrzeb i wymagań dla projektu ZSI-FK także C. D. i A. P. w październiku 2021 r.

[40] Analiza obejmowała wraz z Urzędem 39 podmiotów

Na podstawie wybranej próby szczęściu programów C, M.P., M.O, Z., S., L. stwierdzono, że: Urząd zweryfikował jedynie faktyczne wykorzystanie oprogramowania ZOOM PRO-1 w zakresie użytkowania na podstawie raportów udostępnionych przez aplikację. W odniesieniu do pozostałych aplikacji nie były prowadzone analizy faktycznego korzystania z oprogramowania SaaS w zakresie logowań - wymienione aplikacje nie udostępniały narzędzi do monitorowania. W zakresie wykorzystania dostępów stwierdzono, iż wynosiły one od 87,4% (dla aplikacji L.) do 100% dla czterech aplikacji (w tym np. C.).

(akta kontroli str. 1619)

Urząd dokonywał weryfikacji kluczowych systemów takich jak ZSI-FK w 2019 r. oraz w 2021 r. W jej ramach przeprowadzona była inwentaryzacja zasobów Urzędu i jednostek organizacyjnych Gminy z czego sporządzono analizę „Diagnozy stanu technicznego i merytorycznego oraz potrzeb w zakresie planowanych przedsięwzięć informatyzacji Gminy Miasto Szczecin". W 2021 r. opracowano: „Wdrożenie Systemu Informacji Przestrzennej w Urzędzie Miasta Szczecin – analiza efektywności", oraz "Koncepcję rozwoju Systemu Informacji Przestrzennej Miasta Szczecin[41]". W 2021 r. w ramach systemu eDOK sporządzono analizę aktywnych użytkowników na podstawie Regulaminu Organizacyjnego każdego wydziału/biura. Koncepcja rozwoju systemu opracowana została w 2019 r. i 2021 r. aktualizowana była na bieżąco. W odniesieniu do pozostałych programów taka weryfikacja w latach 2019-2022 nie była prowadzona.

W odniesieniu do ZSI-FK zebrano dane w procesie inwentaryzacji stanu istniejącego, który wykonany był przy pomocy narzędzi elektronicznych udostępniających ankiety w siedmiu obszarach oraz na podstawie analizy stanu bieżącego, analizy procesów, zaplecza sprzętowego i możliwościach rozwoju istniejącego oprogramowania, kosztów (licencji na użytkowników), analizie ilości użytkowników. Efekty wynikające z badania ZSI-FK pozwalały ustalić szczegółowy zakres projektu (szczegółowy opis przedmiotu zamówienia), określić warunki i możliwości migracji danych, integracji systemu z innymi rozwiązaniami, pozyskać informacje o zasadach wykonywania testów oraz odbiorów, zidentyfikować ryzyka związane z realizacją przedsięwzięcia zdefiniować modele licencjonowania dla różnych kategorii użytkowników, zwymiarować infrastrukturę niezbędną do realizacji projektu, określić ramowy harmonogram realizacji projektu łącznie z etapami jego realizacji, oszacować koszty wdrożenia poszczególnych modułów i komponentów systemu. W przypadku SIPMS badanie prowadzone było przez jego administratora na bieżąco, analizującego potrzeby użytkowników, weryfikując użytkowników i szkoląc w zakresie obsługi systemu. Efektem było opracowanie koncepcji na pozyskanie środków i zwiększenie ilości użytkowników.

W programie eDOK przeanalizowano użytkowników i zweryfikowano strukturę organizacyjną pozwalającą efektywnie zarządzać systemem.

(akta kontroli str. 64-197, 1613-1618,)

Urząd był beneficjentem jednego projektu finansowanego ze środków Unii Europejskiej, którego trwałość zakończyła się w okresie objętym kontrolą. Program SIPMS wdrożony został w 2015 r. w ramach Europejskiego Funduszu Rozwoju Regionalnego. Termin zakończenia rzeczowego upływał 20 lipca 2015 r. a finansowego 28 lipca 2015 r. Projekt, według oświadczenia Dyrektora Wydziału, wpływał pozytywnie na rozwój aplikacji i systemów informatycznych dla sektora publicznego oraz wzrost usług publicznych świadczonych drogą elektroniczną. Budowa systemu polegała na gromadzeniu, aktualizacji i udostępnianiu danych

[41] Dalej: SIPMS.

przestrzennych przy użyciu nowoczesnych technologii informatycznych oraz reguł interoperacyjności zbiorów i usług związanych z zarządzaniem danymi przestrzennymi. W ramach projektu utworzony został portal udostępniania danych i usług przestrzennych w oparciu o wdrożoną infrastrukturę danych przestrzennych (sprzęt i oprogramowanie) służącą budowie i aktualizacji danych przestrzennych.
Do zadań projektu należało udostępnienie geoportalu Gminy, budowa i integracja baz SIPMS, założenie Geodezyjnej Sieci Uzbrojenia Terenu na obszarze Gminy.

Wykorzystanie systemu było następujące: założono konta dla 1 013 pracowników Urzędu, odnotowano 430 tys. odsłon, 225 tys. sesji i 102 tys. użytkowników. SIPMS był podstawowym systemem dla użytkowników wewnętrznych i zewnętrznych dostarczającym dane przestrzenne.

W 2020 r. Dyrektor Wydziału opracował „Analizę efektywności wdrożenia SIPMS w Urzędzie", a w 2021 r. powstała „Koncepcja rozwoju SIP". Ze względu na brak środków, podjęto próbę pozyskania środków unijnych na rozbudowę systemu. Roczne utrzymanie systemu wynosiło w latach 2019-2021 137,9 tys. zł rocznie.

(akta kontroli str. 1616-1618)

2.3. Poniesione wydatki na nabycie i utrzymanie oprogramowania komputerowego.

W latach 2019-2022 r. (do 30 czerwca) wydatki związane z obsługą informatyczną Urzędu wyniosły na: nabycie programów komputerowych 1 501,1 tys. zł; korzystanie z programów komputerowych 11 077,1 tys. zł w tym: dostosowanie i aktualizacja 468,4 tys. zł, przedłużanie umów licencyjnych 2 337,8 tys. zł, subskrypcja licencji 657,6 tys. zł, instruktaże i szkolenia związane z nabytymi licencjami 55,1 tys. zł, opłaty za wsparcie i asysty techniczne 7 613,3 tys. zł, wydatki na Wydział Oświaty 1 661,2 tys. zł. (akta kontroli str. 393)

2.4. Wprowadzone wymagania bezpieczeństwa dla systemów informatycznych dopuszczonych do przetwarzania informacji.

Na wybranej próbie sześciu programów (opisanych w pkt. 2.2. niniejszego wystąpienia pokontrolnego) ustalono, że w Urzędzie obowiązywały zasady weryfikacji planowanego do nabycie oprogramowania. Były one opisane w § 11 Polityki Bezpieczeństwa. Przeprowadzali ją pracownicy Wydziału, którzy określali warunki udziału w postępowaniach oraz przygotowywali specyfikacje. Weryfikacja planowanego do nabycia oprogramowania obejmowała: zgodność funkcjonalności oprogramowania z potrzebami Urzędu, kwestie związane z bezpieczeństwem, możliwość integracji, zasady licencjonowania, wsparcie, archiwizację danych. Dostawcy byli weryfikowani na podstawie referencji, opinii na temat jakości produktu oraz doświadczenia. W odniesieniu do planowania oprogramowania stosowano przepisy § 11 i § 16 pkt 4 Polityki Bezpieczeństwa, w którym wskazano, iż musiały być zdefiniowane cele wdrażanej usługi; użytkownicy usługi, rozumiani jako jednostki, które korzystały z danej usługi; wymagania w zakresie funkcjonalności, dostępności i wydajności usługi; wpływu na zmianę funkcjonowania Urzędu.
Ocena dostawcy była dokonywana na etapie planowania zakupów poprzez jego weryfikację (sprawdzenie certyfikaty, referencje, oceny użytkowników). Następnie radcy prawni Urzędu weryfikowali projekty umów pod kątem zgód Administratora Systemów Informatycznych, Inspektora Ochrony Danych Osobowych.
Zasady instalowania oprogramowania dostępnego w sieci publicznej w tym określonego przez jego wytwórcę lub właściciela praw autorskich, jako wolne, publicznie dostępne w tym darmowe zostało określone m.in. w § 37 ust. 5 załącznika nr 2 do Polityki Bezpieczeństwa. W sześciu badanych programach typu SaaS nie było opracowanych procedur bezpieczeństwa.

(akta kontroli str. 1625-1628)

Dyrektor Wydziału wyjaśnił, iż wymogi bezpieczeństwa uregulowane zostały zapisami w umowach lub dokumentacji z postępowania.

(akta kontroli str. 1626)

Za opracowanie procedury bezpieczeństwa informatycznego (cyberbezpieczeństwa) odpowiadał w latach 2019-2022 Inspektor Ochrony Danych Osobowych oraz Wydział. (akta kontroli str. 1627)

W przypadku oprogramowania SaaS proces weryfikacji spełniał wymagania RODO.

Biegły powołany przez NIK w opinii stwierdził m.in., że żadna umowa nie była zawierana bez asygnaty działu prawnego. Nawet w przypadku dużych umów całość była weryfikowana przez dział prawny, Inspektora Ochrony Danych Osobowych, który także weryfikował zapisy umowy.

(akta kontroli str. 1960, 1970)

2.5. Proces pozyskiwania usług SaaS.

Proces nabywania oprogramowania każdorazowo uwzględniał ocenę wiarygodności dostawcy pod kątem zapewnienia ciągłości usług[42]. W przypadku jednej z badanych aplikacji C., Urząd nie weryfikował dostawcy oprogramowania, według oświadczenia Dyrektora Wydziału, nie było takiej potrzeby ponieważ ta aplikacja była programem do telekonferencji. Pozostałe programy były oceniane jako wiarygodne pod kątem zapewnienia wsparcia technicznego i bezpieczeństwa. W każdym przypadku producenci zapewniali, co wynikało z postanowień umownych, wsparcie w zakresie bezpieczeństwa. Każda z sześciu aplikacji była poddana kwerendzie internetowej. Urząd ustalił, że w przypadku trzech aplikacji nie wystąpiły publiczne wycieki i incydenty, w pozostałych trzech stwierdzono ich wystąpienie[43].

(akta kontroli str. 1620-1624)

Dyrektor Wydziału wyjaśnił, że: *W okresie pandemii i ogromnego wzrostu zapotrzebowania na pracę zdalną, nasiliły się ataki na tego typu systemy. Na przykład w okresie zdalnej nauki, podczas prowadzenia lekcji bardzo często dochodziło do włamań do systemów MS. Jednak system ten po poprawkach jest dominującym systemem w oświacie. Incydenty występują wszędzie, a systemy są dość szybko naprawiane. Nawet w największych organizacjach jak M. występują luki w systemach operacyjnych Windows, które co miesiąc są aktualizowane. Każdy program ma jakieś luki, jednak korzystamy z komputera, systemu operacyjnego czy aplikacji. (…).* W Urzędzie nie były znane negatywne opinie pracowników firm dostarczających oprogramowanie na temat pracy u dostawców, wskazujących na niską jakość działania oprogramowania. W odniesieniu do wszystkich programów dostawcy posiadali referencje. Certyfikat bezpieczeństwa informacji okazany był w przypadku dwóch badanych programów M., w odniesieniu do jednego był do zapoznania się na stronie WWW, w pozostałych trzech przypadkach nie został przedstawiony.

(akta kontroli str. 1620-1624, 1981)

Proces nabywania oprogramowania SaaS w czterech przypadkach nie uwzględniał dostępności umowy SLA.

Według oświadczenia Dyrektora Wydziału nie była ona konieczna ze względu na to, iż nie były to aplikacje krytyczne dla pracy Urzędu. Przerwa w ich pracy nie powodowała problemów i przestojów. W dwóch przypadkach uwzględniono dostępność umowy SLA, jednak ze względu na cenę takiej umowy nie wykupiono.

[42] Weryfikowano aplikacje C., M. P., M. O., Z., S., L.
[43] Weryfikowano aplikacje C., M.O, Z.

W pięciu przypadkach, umowy były zadowalające dla Urzędu ze względu na takie czynniki jak obniżona cena; korzystne warunki wsparcia; obniżki w ramach dwuletniej umowy oraz licencje dla kilku jednostek. W przypadku programu C. ze względu na to, że program był darmowy, Urząd nie zawarł umowy.

Maksymalny czas otwarcia okna serwisowego był określony w przypadku czterech programów, warunku serwisowe określił producent. W aplikacji C. w warunkach użytkowania nie był określony maksymalny czas otwarcia okna serwisowego, zaś w przypadku programu Z., błędy były na bieżąco usuwane przez producenta, który określił warunki licencyjne i kary dotyczące umowy. W przypadku dwóch badanych aplikacji zapewniono procedurę zgłaszania błędów i zgłoszeń oraz określono maksymalny czas na zgłoszenie problemu, w pozostałych czterech przypadkach takiej procedury nie było, jednak błędy miały być usuwane automatycznie.

(akta kontroli str. 1620-1624)

W przyjętych procedurach nabywania oprogramowania SaaS nie zostały określone szczegółowe zadania i odpowiedzialność w zakresie oceny dostawcy i oprogramowania oraz zasad jego nabywania, co opisano w sekcji „Stwierdzone nieprawidłowości".

Stwierdzone nieprawidłowości

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

1. W odniesieniu do oprogramowania SaaS zasady zarządzania licencjami nie określały szczegółowych zadań i odpowiedzialności odnoszących się do nabywania i wykorzystywania oprogramowania w modelu SaaS w zakresie oceny lub weryfikacji odnoszących się do minimum takich kwestii jak: wiarygodność dostawcy, w tym pod kątem zapewniania wsparcia technicznego i bezpieczeństwa; spełnienia (wcześniej wyspecyfikowanych) wymagań bezpieczeństwa; dostępności umowy SLA i spełnienia oczekiwań Urzędu w tym zakresie; spełnienia wymagań związanych z zarządzaniem danymi (śledzenie zmian na poziomie rekordów bazy danych, zapewnienia możliwości eksportu danych w popularnych formatach, zasady rozdzielania danych (multi-tenancy); zapewnienia szyfrowania data-in-transit w oparciu o bezpieczne protokoły i algorytmy; polityki kopii zapasowej, w tym częstotliwości wykonywania kopii i okresu retencji oraz przechowywania; spełnienia wymagań kontroli dostępu; spełnienia wymagań RODO (i innych wymagań wynikających z określonych przepisów prawa).

(akta kontroli str. 1970-1971)

Powołany przez NIK biegły stwierdził, że: *„Biorąc pod uwagę wyjaśnienia związane procesem nabywania i wykorzystywania oprogramowania w modelu SaaS, oraz przedstawienie sposobu w jaki dokonywana jest ocena i weryfikacja spełnienia wymagań organizacji ocena Biegłego w zakresie nabywania i użytkowania SaaS jest pozytywna z zastrzeżeniami. Zastrzeżenia wynikają i odnoszą się do obserwacji związanej z brakiem mechanizmu kontrolnego zapewniającego, że w procesie pozyskiwania oprogramowania SaaS uwzględnia się określoną, adekwatną weryfikację i ocenę dostawcy i oprogramowania oraz ustanowione zasady nabywania oprogramowania nie określają szczegółowych zadań i odpowiedzialności w tym zakresie".*

(akta kontroli str. 1960)

Dyrektor Wydziału wyjaśnił, że: *Urząd korzysta z oprogramowania typu SasS w niewielkiej skali, starając się zapewnić własne oprogramowanie w tym zakresie. Nie mniej jednak wobec wszystkich dostawców stosowane są rygorystyczne wymagania dotyczące RODO. Ocena systemu bezpieczeństwa wykonawcy poprzez ankietę załączoną każdorazowo do umowy powierzenia przetwarzania danych*

pozwala przeprowadzić analizę i zweryfikować dostawcę pod kątem bezpieczeństwa IT". (akta kontroli str. 1551)

Wzór ankiety, o której mowa w powyższych wyjaśnieniach dotyczył tylko zabezpieczenia ochrony danych osobowych, zawierał pytania: 1) czy podmiot przetwarzający posiada certyfikat zgodny art. 42 RODO?; 2) Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO i jest on zgodny z przedmiotem postępowania?; 3) Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujących w jego organizacji system ochrony danych osobowych i uzyskał ocenę negatywną? W przypadku odpowiedzi „nie" na wszystkie ww. pytania należało odpowiedzieć na pozostałe 29 pytań.

(akta kontroli str. 1556)

NIK stwierdza, że istotna jest weryfikacja i ocena oprogramowania w toku rozpoznawania oferty rynkowej, a nie zawierania umowy. Urząd nie określił swoich wymagań dotyczących takiego oprogramowania. To, że Urząd korzystał z tego oprogramowania w niewielkiej skali nie ma znaczenia. Nawet przy jednym takim programie dane są przetwarzane poza infrastrukturą Urzędu, a w przypadku jakichkolwiek problemów administratorzy Urzędu nie mają wpływu na korzystanie z takiego oprogramowania.

2. Postępowanie o udzielenie zamówienia publicznego na świadczenie usług asysty technicznej oraz rozwoju Zintegrowanego Systemu Informatycznego wspomagającego zarządzanie finansami Miasta (ZSI-FK) dla Gminy Miasta Szczecin zostało przeprowadzone w trybie zamówienia z wolnej ręki z naruszeniem przesłanek do jego zastosowania określonych w art. 214 ust. 1 pkt 1 lit. a) i b) Pzp.

(akta kontroli str. 1689-1692, 1747- 1750, 1770-1778, 1734-1746)

Dyrektor Wydziału wyjaśnił, że: *(…) Wybór zastosowanego trybu opierał się na analizach stanu bieżącego opartych o badania ankietowe, rozmowy z interesariuszami projektu, rozmowy z dostawcami poszczególnych rozwiązań i wiedzę ekspertów z Centrum Doradztwa i Analiz Projektowych oraz Szczecińskiego Parku Naukowo Technologicznego. Podstawą wyboru trybu była analiza rynku, która polegała na szeregu czynności zapewniających obiektywną ocenę, w wyniku której ustalono, że z przyczyn technicznych usługa może być świadczona tylko przez jednego wykonawcę. Analiza rynku była prowadzona w okresie od 2018 r. do 2021 r. i obejmowała m.in.*

- szereg spotkań i rozmów z interesariuszami projektu i dostawcami poszczególnych rozwiązań (…) przeprowadzenie badań ankietowych i doradztwo ekspertów z Centrum Doradztwa i Analiz Projektowych Spółka z o.o., którzy przeprowadzili diagnozę stanu jednostek oświatowych Gminy Miasto Szczecin oraz opracowali koncepcję powołania Centrum Usług Wspólnych, w lipcu 2019 r., w trakcie spotkań analizowano możliwość integracji systemów; przeprowadzenie badań ankietowych i doradztwo ekspertów ze Szczecińskiego Parku Naukowo Technologicznego, którzy opracowali w grudniu 2019 r. dokumentację pn. „Koncepcja Systemu Finansowo-Księgowego, etap II dla Gminy Miasto Szczecin"; analiza dotychczas zawartych umów, zwłaszcza w zakresie praw autorskich; analiza rozwiązań w innych gminach; analiza publikacji i rekomendacji na stronach internetowych i w wydawnictwach (…).

Istnieje kilka ważnych zapisów umownych wskazujących na fakt, że Zamawiający nie może powierzyć realizacji umowy innym podmiotom: 1) prawa wyłączne - Zamawiający zapewnił sobie przeniesienie praw autorskich do efektów rozwoju / rozbudowy Systemu tj. Adaptacji i Konwerterów, ale nie do wszystkich warstw Systemu / elementów nabył majątkowe prawa autorskie (problem Systemu i jego

Modułów, które są dystrybuowane na zasadzie licencji). Posiadanie praw autorskich do kodu źródłowego upoważnia Zamawiającego do podejmowania działań wyłącznie we własnym zakresie. Zamawiający nie uzyskał uprawnienia do możliwości tworzenia utworów zależnych, a tak należy traktować rozwijanie przedmiotowego oprogramowania; 2) kody źródłowe - Zamawiającemu udzielono praw do korzystania z Systemu i / lub Modułów (licencji) oraz przeniesiono autorskie prawa majątkowych do Adaptacji i Konwerterów wynika z tego, że na Zamawiającego nie zostały przeniesione autorskie prawa majątkowe do Systemu oraz Modułów (które dystrybuowane były w modelu licencyjnym).(…).

Zamawiający prowadząc pierwsze postępowanie przetargowe na dostawę i wdrożenie Zintegrowanego Systemu Informatycznego wspomagającego zarządzanie finansami Miasta (ZSI-FK), które zakończyło się zawarciem umowy CR 4002/2007, wskutek protestów i odwołań wniesionych na zapisy SIWZ zmuszony był tak ostatecznie ukształtować treść zapisów wzoru umowy. Pozostałe umowy były konsekwencją zapisów umowy pierwotnej.

Prowadząc w 2006 r. pierwsze postępowanie przetargowe na dostawę i wdrożenie Zintegrowanego Systemu Informatycznego wspomagającego zarządzanie finansami Miasta (ZSI-FK), które zakończyło się zawarciem umowy CR 4002/2007, wskutek protestów i odwołań wniesionych na zapisy SIWZ, Zamawiający zmuszony był tak ostatecznie ukształtować treść zapisów wzoru umowy. Zamawiający nie miał zatem swobody w kształtowaniu zapisów stanowiących o uprawnieniach gwarancyjnych. Pozostałe umowy i ich zapisy (w szczególności w zakresie gwarancji i praw autorskich) były więc konsekwencją pierwotnej. Szczegółowe warunki gwarancji ustalane były każdorazowo w toku negocjacji kolejnych umów zawieranych w latach 2010-2018, których przedmiotem była rozbudowa. systemu. Zmiana zapisów gwarancyjnych wiązałaby się z konsekwencjami utraty kontroli nad systemem a tym samych brakiem ciągłości działania. Wykonawca wziął na siebie pełną odpowiedzialność za zapewnienie prawidłowego funkcjonowania systemu, dlatego nie dopuścił możliwości dokonywania jakichkolwiek zmian / modyfikacji przez stronę trzecią. Brak zgody ze strony Zamawiającego na zapisy dotyczące gwarancji wiązałby się z odstąpieniem Wykonawcy od realizacji umowy.

Zgodnie z § 10 ust. 3 umowy CRU NR 21/0001796 z dnia 23.06.2021 r.- „Wykonawca może odmówić sprawowania gwarancji na warstwy i elementy Systemu powstałe w wyniku jego rozbudowy w ramach Umowy, gdy Zamawiający dokonał lub zlecił modyfikację w oprogramowaniu Modułów lub Adaptacji."

W umowie obejmującej świadczenie usług asysty technicznej i rozwoju Zintegrowanego Systemu Informatycznego wspomagającego zarządzanie finansami miasta (ZSI-FK) dla Gminy Miasto Szczecin CRU/18/0002674 z dnia 29.06.2018 r. zawarto następujące zapisy dotyczące gwarancji: „§10 Gwarancja. 1. Wykonawca udziela 12 - miesięcznej gwarancji na prawidłowe działanie wykonanych w ramach usług rozwoju rozbudów i rozszerzeń Systemu Dziedzinowego od daty zakończenia Umowy. (…) 3. Wykonawca może odmówić sprawowania gwarancji na warstwy i elementy System powstałe w wyniku jego rozbudowy w ramach Umowy, gdy Zamawiający dokonał modyfikacji w oprogramowaniu Modułów lub Adaptacji bez wiedzy Wykonawcy, chyba, że ingerencja Zamawiającego w kod Modułów lub Adaptacji nastąpiła w wyniku niewywiązywania się Wykonawcy z obowiązków gwarancyjnych lub serwisowych. 4. Wykonawca nie odpowiada za nieprawidłowości działania warstw Systemu wynikające z nieprawidłowego administrowania Platformą Sprzętową Zamawiającego, w tym środowiskami Windows Serwer 2003/2008, MS SQL 2005/2008, MS Dynamics Axapta AX 2009 bądź kolejnych ich wersji rozwojowych eksploatowanych przez Zamawiającego. (…).

Zamawiający zgodził się na takie postanowienia umów, ponieważ Wykonawca nie dopuścił możliwości implementowania zmian przez strony trzecie ze względu na możliwość przejęcia własności intelektualnej Wykonawcy. Natomiast, w przypadku okoliczności losowych np. wycofanie produktu z rynku, zakończenie działalności Wykonawcy itp., w wyniku których doszłoby do zakończenia współpracy, Zamawiający mógłby korzystać z systemu bez dokonywania jakichkolwiek modyfikacji lub zatrudnić/wykształcić pracownika, który takie zmiany mógłby wprowadzić. Modyfikacja systemu we własnym zakresie nie była w tym czasie jednak możliwa i celowa z uwagi na ograniczone możliwości finansowania kosztów osobowych określonych w obowiązującym regulaminie wynagradzania. Jednakże zapis ten zabezpiecza Gminę Miasto Szczecin, w przypadku przyszłych zmian przepisów o wynagrodzeniach pracowników samorządowych i daje możliwość korzystania z zasobów własnych w przyszłości. Jednocześnie zaznaczyć należy, że żaden przepis prawa nie obliguje Zamawiającego do nabywania w całości majątkowych praw autorskich do systemu (…).

(akta kontroli str. 1786-1892)

W ocenie Izby w kontekście wymogów jakie wynikają ze ścisłego interpretowania art. 214 ust. 1 pkt 1 lit. a i b Pzp oraz poglądów doktryny i orzecznictwa, Urząd nie wykazał w sposób dostateczny wystąpienia w badanym postępowaniu okoliczności uzasadniających spełnienie przesłanek określonych w ww. przepisie. Wymaga zauważenia, że kluczową cechą przesłanek wymienionych w art. 214 ust. 1 pkt 1 lit. a i b Pzp jest to, że zamówienie może być wykonane tylko przez jednego wykonawcę. Przytaczane postanowienia dotyczące udzielonej gwarancji nie stanowią przeszkody w rozbudowie przez Zamawiającego. Jeśli Urząd zleci rozbudowę innemu podmiotowi to przecież nowy wykonawca także zobowiązany będzie do udzielenia gwarancji na wykonane prace. Wbrew stanowisku zawartemu w wyjaśnieniu postanowienia dotyczące gwarancji nie uniemożliwiają dokonywania modyfikacji przez podmioty trzecie: Wykonawca wziął na siebie pełną odpowiedzialność za zapewnienie prawidłowego funkcjonowania systemu, dlatego nie dopuścił możliwości dokonywania jakichkolwiek zmian / modyfikacji przez stronę trzecią. Postanowienia gwarancji zwalniają Asseco od odpowiedzialności za ewentualne nieprawidłowości wynikające z działań podmiotu trzeciego, ale nie zabraniają takich modyfikacji.

Ponadto aktualna umowa serwisowo - rozwojowa daje możliwość rozwoju i dostosowywania poszczególnych elementów lub całego systemu do realizacji nowych potrzeb zamawiającego bez utraty gwarancji na prace zrealizowane w ramach poprzednich umów, ponieważ gwarancja wygasa w określonym w umowie terminie. Należy też wskazać, że gwarancja, wbrew złożonym wyjaśnieniom, nie dotyczy wszystkich wytworzonych wcześniej produktów. Obejmuje jedynie: prawidłowe działanie wykonanych w ramach usług rozwoju rozbudów i rozszerzeń Systemu. W wyjaśnieniach stwierdzono, że Zamawiający nie uzyskał uprawnienia do możliwości tworzenia utworów zależnych, a tak należy traktować rozwijanie przedmiotowego oprogramowania. Urząd posiada dostęp do kodu źródłowego i możliwość podejmowania działań we własnym zakresie.

Istotne znaczenie ma treść umowy z 2008 r. co do zakresu udzielonej licencji (pola eksploatacji, możliwość rozwoju i dostęp do kodów źródłowych) - Urząd nie musi być właścicielem autorskich praw majątkowych, żeby mieć możliwość samodzielnego serwisu (lub w formie zlecenia podmiotom trzecim) systemu lub jego rozbudowy o nowe moduły (np. poprzez dostawę przez innego wykonawcę modułu współpracującego z posiadanym systemem – kompatybilnego z bazą, na której opiera się system, tj. oprogramowaniu M.D.).

OCENA CZĄSTKOWA

Urząd podejmował działania w celu optymalizacji wykorzystania posiadanego oprogramowania.

Przyjęte przez Urząd rozwiązania w zakresie planowania, finansowania i realizacji działań podejmowanych w ramach zarządzania oprogramowaniem, uwzględniały faktyczne potrzeby Urzędu. Przed planowanym postępowaniem dotyczącym aktualizacji i rozbudowy ZSI-FK została przeprowadzona analiza, o której mowa w art. 83 Pzp. Zapewniono wykorzystanie oprogramowania po okresie trwałości projektu, w ramach którego zostało zakupione. Nie został natomiast określony mechanizm kontrolny zapewniający, aby w procesie pozyskiwania oprogramowania SaaS, dokonywana była weryfikacja spełnienia określonych (np. w ramach listy kontrolnej) wymagań oraz potwierdzenia, że oprogramowanie spełnia oczekiwania Urzędu. NIK negatywnie ocenia przeprowadzenie postępowania publicznego o udzielenie zamówienia publicznego w trybie z wolnej ręki na świadczenie usług asysty technicznej oraz rozwoju Zintegrowanego Systemu Informatycznego wspomagającego zarządzanie finansami Gminy, z naruszeniem przesłanek jego zastosowania. Za jego wykonanie Urząd zapłacił do końca czerwca 2022 r. 1 415 550 zł netto (1 741 126,50 zł brutto).

III. 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), w tym zasad nabywania i wykorzystywania oprogramowania w modelu SaaS.
2. Objęcie regularnym monitorowaniem całego oprogramowania, dokumentowanie podejmowanych czynności, w tym działań naprawczych.
3. Udzielanie zamówień publicznych w trybie z wolnej ręki po spełnieniu przesłanek ustawowych zastosowania tego trybu.

Uwagi

Najwyższa Izba kontroli nie formułuje uwag.

IV. 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 ust. 1 i 2 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 Szczecinie. 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 30 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków 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.

Szczecin, 28 października 2022 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie
Dyrektor

Kontroler:

Radosław Kropiowski
doradca ekonomiczny
/-/

Krzysztof Zawadzki
starszy inspektor kontroli państwowej
/-/

Zmian w wystąpieniu pokontrolnym dokonał:

Elektronicznie podpisany przez Marcin Zdzisław Stefaniak
Data: 2023.01.13 13:52:12 +01'00'

Dyrektor Delegatury