NAJWYŻSZA IZBA KONTROLI

Delegatura w Krakowie

LKR. 410.017.04.2022
P/22/082

Pani
Elżbieta Fryźlewicz-Chrapisińska
Dyrektor
Małopolskiego Oddziału Wojewódzkiego
Narodowego Funduszu Zdrowia w Krakowie
ul. Ciemna 6
31-053 Kraków

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Małopolski Oddział Wojewódzki Narodowego Funduszu Zdrowia w Krakowie, ul. Ciemna 6, 31-053 Kraków (*Oddział*).
Kierownik jednostki kontrolowanej	Elżbieta Fryźlewicz-Chrapisińska, Dyrektor Oddziału, od 15 marca 2016 r. (akta kontroli str. 3)
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 z wykorzystaniem dowodów sporządzonych przed lub po tym okresie, jeżeli miały one istotny wpływ dla ustaleń i ocen kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Krakowie
Kontroler	Monika Różańska, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/118/2022 z 3 sierpnia 2022 r., LKR/142/2022 z 12 października 2022 r. (akta kontroli str. 1-2)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W ocenie Najwyższej Izby Kontroli Oddział wdrożył mechanizmy kontrolne do sprawowania nadzoru nad oprogramowaniem[3], niemniej jednak nie wszystkie okazały się w pełni skuteczne.

Oddział wdrożył zarządzanie licencjami na oprogramowanie na bazie zasad zarządzania bezpieczeństwem teleinformatycznym wprowadzonych przez Centralę NFZ. Zapewniono kompletność danych dotyczących wszystkich posiadanych i wykorzystywanych licencji oraz prowadzono przeglądy zainstalowanego oprogramowania. NIK zwraca uwagę, że pomimo prowadzonego przez Oddział monitorowana stacji roboczych pod kątem zainstalowanego oprogramowania, w toku kontroli stwierdzono dwa przypadki oprogramowania bez aktualnych licencji, które to oprogramowanie było zainstalowane przez administratorów Oddziału podczas wykonywania przez nich czynności testowych i aktualizacyjnych. Oprogramowanie zostało odinstalowane jeszcze w toku kontroli. Ponadto przeglądom prowadzonym przez Oddział nie podlegały służbowe telefony komórkowe pracowników, na podstawie decyzji podjętych przez Centralę NFZ.
Zakupy licencji wynikały z bieżących potrzeb Oddziału, a ich nabycie było poprzedzone analizą funkcjonalności i bezpieczeństwa. W latach 2019-2022 nabywano oprogramowanie głównie na potrzeby Wydziału Informatyki i służyło ono zapewnieniu bieżącego, bezpiecznego funkcjonowania systemu informatycznego i sprzętowego Oddziału. Objęte kontrolą oprogramowanie użytkowano zgodnie z warunkami licencji.

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

[3] Kontrola NIK obejmowała oprogramowanie zakupione przez Oddział, nie obejmowała oprogramowania zakupionego przez Centralę NFZ użytkowanego w Oddziale, w tym oprogramowania dziedzinowego.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe kontrolowanej działalności

OBSZAR

Opis stanu faktycznego

1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym

1.1. Wydział Informatyki Oddziału, zgodnie z Regulaminem organizacyjnym[4], odpowiadał za budowę, utrzymanie i rozwój systemów informatycznych Funduszu oraz za budowę, utrzymanie i rozwój infrastruktury teleinformatycznej Oddziału, a także za promowanie i wprowadzanie nowych technologii teleinformatycznych. W ramach Wydziału, Dział Infrastruktury Teleinformatycznej odpowiadał m.in. za:

- zarządzanie, realizację i nadzór nad umowami w obszarze technologii informatycznych;
- planowanie finansowe i rzeczowe dla obszaru technologii informatycznych w zakresie potrzeb Oddziału;
- zapewnienie infrastruktury serwerowej, sieciowej oraz stacji roboczych i urządzeń peryferyjnych w kontekście potrzeb i możliwości Oddziału;
- prowadzenie spraw dotyczących użytkowania służbowych telefonów komórkowych;
- kontrolę prawidłowego użytkowania sprzętu komputerowego i oprogramowania przez użytkowników końcowych;
- prowadzenie dokumentacji technicznej systemów informatycznych i sprzętu komputerowego.

(akta kontroli str. 4-7)

Zasady nabywania oprogramowania zostały określone w obowiązujących, w latach 2019-2022, regulaminach udzielania zamówień publicznych oraz regulaminach prac komisji przetargowych, wprowadzonych zarządzeniami Prezesa NFZ[5]. Zasady te obowiązywały zarówno w Centrali NFZ jak i w oddziałach NFZ.

Zasady zarządzania oprogramowaniem komputerowym m.in.: wdrażania i utrzymywania systemów, usuwania danych, likwidacji nośników, zarządzania licencjami zostały określone w „Polityce zarządzania bezpieczeństwem teleinformatycznym w NFZ”[6]. Dodatkowo zarządzanie zasobami informatycznym służącymi do przetwarzania danych osobowych zostały określone w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”[7] (PZSZ/011) z 23 maja 2018 r.

(akta kontroli str.7, 11, 176)

Dyrektor Oddziału wyjaśniła, że Polityki zostały przyjęte i wdrożone na szczeblu Centrali NFZ; obowiązują one i są bezpośrednio stosowane w całym Funduszu.

(akta kontroli str. 13)

W Polityce Bezpieczeństwa ustalono następujące zasady zarządzania licencjami (rozdział XX):

---

[4] Załącznik do Zarządzenia Dyrektora Oddziału nr 121/22 z dnia 28 kwietnia 2022 r., https://www.nfz-krakow.pl/gfx/nfz-krakow/userfiles/_public/nasz_oddzial/podstawy_prawne/regulamin_organizacyjny_mow_nfz_2022.pdf, dostęp na dzień 8 sierpnia 2022 r.

[5] Nr 35 z 2015 r., nr 127 z 2021 r., nr 85 z 2022 r.

[6] Polityka zarządzania bezpieczeństwem teleinformatycznym w NFZ (PZSZ/014) została wprowadzona 9 lutego 2018 r. i stanowiła integralną część Polityki Zintegrowanego Systemu Zarzadzania w NFZ zatwierdzonej przez Prezesa NFZ (dalej PZSZ), dalej : *Polityka bezpieczeństwa*.

[7] Instrukcja (PZSZ/011) z 23 maja 2018 r. stanowiła integralną część Polityki Zintegrowanego Systemu Zarzadzania w NFZ zatwierdzonej przez Prezesa NFZ.

- w NFZ może być używane wyłącznie oprogramowanie licencjonowane zgodnie z udzielonymi w licencji prawami;
- dla każdego podsystemu teleinformatycznego w jednostce organizacyjnej NFZ prowadzi się ewidencję posiadanych i zainstalowanych licencji na wykorzystywane oprogramowanie. Sposób ewidencji powinien umożliwiać wykonanie audytu faktycznie zainstalowanego lub użytkowanego oprogramowania;
- eksploatowane oprogramowanie powinno być chronione przed nieautoryzowaną modyfikacją, nieuprawnionym usunięciem oraz kopiowaniem.

(akta kontroli str. 116, 176)

Powołany przez NIK biegły[8] odniósł się do ustanowionych regulacji dotyczących zarzadzaniem licencjami i wskazał na brak uszczegółowienia zasad zarządzania licencjami rekomendując (z poziomem istotności – „średni"[9]) uszczegółowienie poniższych zagadnień, w tym:

- wskazanie referencyjnego narzędzia, gdzie ewidencjonowane są licencje (zarówno dla oprogramowania stacji roboczych, serwerów czy też urządzeń mobilnych (jeśli ma zastosowanie);
- zależności pomiędzy oprogramowaniem stanowiącym ewidencję środków trwałych a oprogramowaniem "inwentory tool";
- sposób wykonywania cyklicznych przeglądów licencji i podsumowywania wyników;
- uwzględnienie zależności licencyjnych od Centrali NFZ;
- sposób przechowywania i zabezpieczania dostępu do nośników instalacyjnych, kluczy licencyjnych i innych dokumentów licencyjnych (w tym przechowywanych w środowiskach chmurowych);
- objęcie szczególnym nadzorem stacji roboczych użytkowników posiadających uprawnienia administracyjne;
- odniesienie się do specyficznych zjawisk licencyjnych pojawiających na rynku oprogramowania np.: monitorowania środowiska JAVA;
- dokonywanie cyklicznego skanowania całego środowiska IT (serwery, stacje robocze, urządzenia mobilne) zarówno pod kątem identyfikacji nieautoryzowanego oprogramowania jaki i danych multimedialnych i innych plików, których przechowywanie prowadzi do naruszenia praw do własności intelektualnej,
- weryfikację oprogramowania pod kątem bezpieczeństwa podczas jego nabywania oraz zasad wycofywania licencji,
- role i odpowiedzialności w procesie.

(akta kontroli str. 105-107,118)

[8] Postanowienie LKR.410.017.04.2022 z 2 września 2022 r. o powołaniu biegłego w dziedzinie audytu systemów informatycznych. Zakres badań: stopień wykorzystania posiadanego oprogramowania, w tym serwerowego (funkcjonalność i efektywność wykorzystania); rzetelność, efektywność i funkcjonalność stosowanego sposobu monitorowania oprogramowania; zgodności użytkowania oprogramowania, w tym serwerowego z warunkami licencji; instalowania nielegalnych programów (przez jednostkę i użytkowników); nabywanie i użytkowanie SaaS.

[9] Do oznaczenia rekomendacji z perspektywy poziomu istotności przyjęto następujące kryteria: wysoka, średnia, niska.

1.2. Oddział dysponował zasobem kadrowym do realizacji poszczególnych zadań w procesie zarządzania oprogramowaniem/licencjami komputerowymi. Zarządzaniem i administrowaniem licencjami/oprogramowaniem, infrastrukturą teleinformatyczną zajmowali się w szczególności kierownicy dwóch działów w Wydziale Informatyki, tj. Działu Infrastruktury i Telekomunikacji oraz Działu Aplikacji i Baz Danych (2 osoby) oraz informatycy Działu Infrastruktury (2 osoby). Odpowiedzialność i zadania w tym zakresie były uwzględnione zakresach czynności tych pracowników. Osoby te były doświadczone zawodowo, z co najmniej 15-letnim stażem pracy w Oddziale. W latach 2019-2022 pracownicy ci nie brali udziału w szkoleniach z zakresu zarządzania oprogramowaniem i licencjami.

Oddział nie korzystał z outsorcingu usług związanych z zarzadzaniem oprogramowaniem/licencjami komputerowymi.

(akta kontroli str. 12, 16-22, 96)

1.3. Oddział posiadał oprogramowanie typu inventory tool ManageEngine ServiceDesk Plus (*ServiceDesk*). Umożliwiał on prowadzenie ewidencji wykorzystywanych licencji, w tym okresy ich ważności, weryfikację rodzaju, wersji oraz licencji oprogramowania zainstalowanego na komputerach pracowników oraz serwerach Oddziału. Oprogramowanie zostało zakupione w 2010 r., koszt zakupu: 105,6 tys. zł brutto. Oprogramowanie było wykorzystywane do monitorowania stacji roboczych użytkowanych przez pracowników Oddziału pod kątem zainstalowanego oprogramowania, wersji oprogramowania, zmian oraz monitoringu. Oprogramowanie było aktualizowane do najnowszy dostępnych wersji. Koszt wsparcia serwisowego dla tego oprogramowania w latach 2019-2021 wyniósł łącznie 72 tys. zł.

(akta kontroli str. 15, 16, 176)

Przeprowadzone badanie przez biegłego potwierdziło, że określone kryteria oceny w zakresie rzetelności, efektywności i funkcjonalności stosowanego narzędzia (ServiceDesk) do monitorowania licencji zostały spełnione przez Oddział, tj.:

- Wydział Informatyki zidentyfikował wszystkie posiadane licencje i oprogramowanie oraz sporządził i dysponuje ewidencją tych licencji i oprogramowania,
- spis licencji i oprogramowania wspiera prowadzenie skutecznego nadzoru w całym ich cyklu życia.

(akta kontroli str. 111)

Zaewidencjonowane oprogramowanie/licencje w ServiceDesk odpowiadało wykazowi oprogramowania i licencji w programie Assets Ninja służącemu do ewidencji m.in. środków trwałych, wartości niematerialnych i prawnych Oddziału.
Równolegle do ewidencji oprogramowania i licencji prowadzonej w ServiceDesku rejestr zakupionego oprogramowania i licencji był prowadzony w użytkowanej przez Oddział platformie MS SharePoint.

(akta kontroli str. 51-81, 83, 85, 100, 176)

Oddział posiadał dowody zakupu nabytych w okresie 2019-2022 licencji.

(akta kontroli str. 51-81, 83, 85, 176)

Dostęp do kluczy licencyjnych posiadali tylko uprawnieni pracownicy Wydziału Informatyki Oddziału.

(akta kontroli str. 82,88)

Analiza wykorzystywania licencjonowanego oprogramowania w przypadku zmiany użytkownika, tj. na próbie pracowników, którzy zakończyli pracę w Oddziale w 2021 r. (22 osoby) wykazała, że stacje robocze z licencjonowanym oprogramowaniem (tj. dostarczonym przez Centralę NFZ – 22 pakiety MS Office oraz jedna licencja na program Intellicad zakupiona przez Oddział) zostały: w przypadku 20 pracowników przydzielone do użytku służbowego innym pracownikom w trakcie 2021 r. i 2022 r., jedna stacja robocza została przekazana do likwidacji, a jedna stacja robocza (z m.in. programem Intellicad) od 31 grudnia 2021 była przygotowana do przekazania pracownikowi, który miał zostać zatrudniony[10]. Dane o stacjach roboczych były aktualizowane w ServiceDesku.

(akta kontroli str. 82-85, 91-93)

Oddział nie posiadał oprogramowania, których autorami byliby pracownicy Oddziału.

(akta kontroli str. 94, 96)

Wydział Informatyki posiadał aktualną informację o stanie zainstalowanych (wykorzystywanych) oraz wolnych licencji. Analiza wykorzystania zakupionych poszczególnych licencji wykazała, że:

- oprogramowania serwerowe (próba: Cortex, McAfee, Splunk) - zostały zainstalowane, poziom ich wykorzystania[11] wynosił odpowiednio: 88%, 80,6%, 76,5 %;
- oprogramowania instalowane na stacjach roboczych (badaniem objęto 10 oprogramowań, tj. 100%): osiem oprogramowań zostało zainstalowanych (przydzielonych) w 100%; oprogramowanie ABBYY FineReader (zakupione 26 kwietnia 2021 r.) - z siedmiu zakupionych licencji wolna pozostawała jedna licencja; oprogramowanie Kofax Express (zakupione 30 maja 2022 r.) - z 10 licencji do przydzielenia pozostawało dziewięć. Licencje te zostały zaplanowane do przydzielenia po zakończeniu procesu zakupu nowych komputerów, zaplanowanego na wrzesień 2022 r.

(akta kontroli str. 82, 85)

1.4. Zasady akceptowalnego użycia służbowych zasobów IT zostały określone w PZSZ, w „Polityce zarządzania bezpieczeństwem teleinformatycznym w NFZ", (rozdziały XV-XVIII), oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w NFZ", które zostały przyjęte i wdrożone na szczeblu Centrali NFZ. Zgodnie z zapisami PZSZ do jej przestrzegania byli zobowiązani wszyscy pracownicy Funduszu. Po wprowadzeniu 9 lutego 2018 r. „Polityki zarządzania bezpieczeństwem teleinformatycznym w NFZ" pracownicy Oddziału otrzymali 15 lutego 2018 r. powiadomienie na skrzynki e-mail od pracownika Oddziału, odpowiedzialnego koordynację zintegrowanego systemu zarzadzania, z prośbą o zapoznanie się z zatwierdzonym dokumentem.

Kierownik Działu Organizacyjnego Oddziału wyjaśniła, że w Oddziale stosowano standardowy mechanizm udostępniania pracownikom tego rodzaju dokumentów – regulacji i zarządzeń – w postaci powiadomień e-mail o obowiązku zapoznania się i o miejscu, w którym taki dokument można znaleźć. Ponadto wyjaśniła i przedłożyła dokumenty, że Zespół Bezpieczeństwa Informacji i Ciągłości Działania (*ZBIiCD*) wielokrotnie wystosowywał do pracowników informacje dotyczące szeroko rozumianego bezpieczeństwa, w tym teleinformatycznego i cyberbezpieczeństwa.

(akta kontroli str. 24-40, 176)

[10] Do września 2022 r. nie została ostatecznie przekazana ze względu na trwający proces zatrudnienia nowego pracownika.

[11] Według stanu na 7 września 2022 r.

Dyrektor Oddziału wyjaśniła m.in., że poza oświadczeniami wynikającymi z PZSZ, każdy pracownik w zakresie czynności (część II – zakres odpowiedzialności) pisemnie potwierdzał, że przyjmuje do wiadomości i stosowania wewnętrzne przepisy i procedury obowiązujące w NFZ.

(akta kontroli str. 13)

Oddział posiadał oprogramowanie ServiceDesk, które zawierało moduł do skanowania stacji roboczych. Zabezpieczenia stacji roboczych przed nieuprawnionym instalowaniem oprogramowania realizowane było za pomocą uprawnień administratorów we wskazanym w toku kontroli NIK oprogramowaniu. Całość wykorzystywanego przez pracowników oprogramowania instalowana była przez administratorów stacji roboczych. Komputery pracowników były zabezpieczone przed możliwością instalowania przez pracowników jakiegokolwiek oprogramowania. Oprogramowanie codziennie skanowało stacje robocze (komputery i laptopy)[12]. Skanowanie wykorzystywano głównie do weryfikacji wersji oprogramowania zainstalowanych na komputerach, do wykrywania instalacji oprogramowania spoza „katalogu" domyślnie instalowanych aplikacji przez Wydział Informatyki.
W Polityce bezpieczeństwa/zarządzeniach nie określono odstępów czasowych przeglądów oprogramowania. Naczelnik Wydziału Informatyki wyjaśnił, że przeglądy były wykonywane raz na miesiąc na podstawie raportu wykonywanego w oprogramowaniu ServiceDesk Plus „Raporty audytu, Historia audytu według stacji roboczej". Raport przedstawiał zebrane dane (instalacji, deinstalacji, zmian w oprogramowaniu i sprzętu) z codziennych skanowań stacji roboczych. Wyjaśnił, że nie wystąpiły przypadki wykrycia nieprawidłowości dotyczących oprogramowania, a tym samym nie wdrażano działań naprawczych.

(akta kontroli str. 14,83, 97-98, 104,116, 125)

W Oddziale administratorzy nie wykonywali skanowania służbowych telefonów komórkowych pod kątem nieautoryzowanego/nielegalnego oprogramowania, z uwagi na odstępstwo od zapisów Polityki Bezpieczeństwa wydane przez Centralę NFZ[13]. Przedmiotowe odstępstwo zostało wydane w związku z trwającymi pracami nad wdrożeniem odpowiednich zasad organizacyjnych i środków technicznych w procesie zarządzania urządzeniami mobilnymi, w tym: wdrożeniem systemu do zarządzania urządzeniami mobilnymi klasy MDM, oraz opracowaniem Polityki zarządzania urządzeniami mobilnymi.
Administratorzy nie mieli również mechanizmu kontrolnego pozwalającego na identyfikację przechowywania na zasobach sieciowych oraz stacjach roboczych plików podlegających ochronie praw autorskich (filmy, e-booki, utwory muzyczne) oraz niedozwolonych polityką bezpieczeństwa treści.

(akta kontroli str. 83, 125, 176)

W latach 2019-2022 nie wygasły żadne licencje/subskrypcje zakupione przez Oddział.

(akta kontroli str. 99, 100-101)

Oddział nie ponosił żadnych kar umownych ani grzywien w związku z nielegalnym lub nieprawnie użytkowanym oprogramowaniem w latach 2019-2022.

(akta kontroli str. 44)

[12] Oddział nie posiadał tabletów.
[13] Pismo Prezesa NFZ z 27 września 2021 r.

Zasady dotyczące zbywania i przekazywania sprzętu/oprogramowania do ponownego użycia zostały uregulowane w:

- Polityce bezpieczeństwa, w rozdziale XI - Minimalne wymagania dotyczące usuwania danych i w rozdziale XII – Likwidacja nośników;
- zarządzeniu nr 45/2015/BAG Prezesa NFZ, z 7 sierpnia 2015 r., w sprawie zasad gospodarowania składnikami majątkowymi w NFZ;
- zarządzeniu nr 162/2021/BAG Prezesa NFZ, z 7 października 2021 r., w sprawie zasad gospodarowania służbowymi telefonami komórkowymi oraz Internetem mobilnym w NFZ.

W kontrolowanym okresie Oddział nie przekazywał sprzętu IT innym jednostkom zewnętrznym. Nośniki danych z zużytego sprzętu (dyski z komputerów stacjonarnych oraz laptopów) były rejestrowane w rejestrze nośników danych przeznaczonych do kasacji prowadzonego przez Wydział Informatyki w formie elektronicznej. Rejestr zawierał dane identyfikacyjne każdego nośnika danych w postaci liczby porządkowej (wpisanej na obudowie dysku) oraz numeru seryjnego dysku (512 sztuk). Wydział Informatyki, po procedurze czyszczenia dysków z danych za pomocą dedykowanego oprogramowania zbierał nośniki danych i je przechowywał w zabezpieczonym miejscu, bez dostępu osób nieuprawnionych. Dyski nie były jeszcze przekazane do zniszczenia do wyspecjalizowanej firmy posiadającej odpowiednie uprawnienia do niszczenia nośników danych.

Oddział nie wycofywał oprogramowania w ciągu ostatniego roku.

(akta kontroli str. 82-83, 92, 99, 176)

1.5. Analiza nabycia i wykorzystania wybranych oprogramowań[14], zakupionych przez Oddział w kontrolowanym okresie, wykazała, że korzystano z oprogramowania zgodnie z warunkami licencji.

Badanie oprogramowania na stacjach roboczych pracowników Oddziału, pod kątem możliwości dobrowolnego instalowania programów/aplikacji przez pracowników, przeprowadzone przez biegłego powołanego przez NIK, zidentyfikowało przypadki nielegalnych programów. Podczas badania wykonano niezależne testy identyfikujące z wykorzystaniem dostępnego w Oddziale oprogramowania ServiceDesk. Wykorzystując słowa kluczowe popularnych oprogramowań lub aplikacji, narzędzie wyszukiwało nieautoryzowane oprogramowanie na całej populacji stacji roboczych. Na 14 identyfikacji stwierdzono pojedyncze przypadki dla dwóch oprogramowań, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*. Zidentyfikowany przypadek instalacji Spotify na jednej stacji roboczej, jak wyjaśnił Naczelnik Wydziału Informatyki, był darmowym rozszerzeniem do przeglądarki chrome, a nie aplikacją na system Windows, jednak zostało niezwłocznie usunięte z komputera pracownika

(akta kontroli str.82-83, 85,109-120)

Oddział poza zakupionym oprogramowaniem korzystał także z dziewięciu darmowych oprogramowań, które nie były obwarowane dodatkowymi warunkami związanymi z użytkowaniem lub okresem użytkowania.

(akta kontroli str. 130)

[14] PaloAltoNetworks, McAfee, CorelDraw.

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:
Na stacjach roboczych pracowników Oddziału wykryto dwa przypadki instalacji oprogramowania WinRAR oraz dwa przypadki instalacji Java, na które Oddział nie posiadał aktualnych licencji.

(akta kontroli str. 83,85, 119)

Naczelnik Wydziału Informatyki wyjaśnił, że: wykryte w toku oględzin oprogramowanie WinRAR zostało zainstalowane przez administratorów na ich stacjach roboczych, celem wykonana testów porównawczych z oprogramowaniem 7-zip. Przez niedopatrzenie oraz dużą ilość zadań, sami nie odinstalowali oprogramowania po skończonych testach. Oprogramowanie Java zostało omyłkowo zaktualizowane przez administratorów do wersji wyższej niż 202, w chwili wgrywania nowego certyfikatu kwalifikowanego na kartę kryptograficzną cryptoCertum. Procedura instalacji certyfikatu użytkownika (podpisu kwalifikowanego) na karcie kryptograficznej wymagała zainstalowanego oprogramowania Java. Dla oprogramowania WinRAR Oddział dysponował licencją, jednakże nie na wersję, która była zainstalowana. Dla oprogramowania java Oddział nie dysponował stosownymi licencjami.
Wykryte w toku oględzin oprogramowanie WinRAR i Java zostało odinstalowane z komputerów pracowników niezwłocznie po oględzinach.

(akta kontroli str. 121-124, 126)

OCENA CZĄSTKOWA

W Oddziale obowiązywały procedury zarządzania i postępowania z oprogramowaniem ustanowione przez Centralę NFZ. Pracownikom zostały przydzielone zadania w tym zakresie. Oddział posiadał i korzystał z narzędzia do inwentaryzacji oprogramowania. Zapewniono stałą i bieżącą informację na temat wszystkich posiadanych i wykorzystywanych licencji oraz dokonywano przeglądów posiadanego oprogramowania, przy czym monitorowaniu nie podlegały telefony służbowe. Stwierdzono jednak dwa przypadki zainstalowania przez administratorów nowszych wersji oprogramowania bez aktualnych licencji. Oprogramowania te odinstalowano w toku kontroli NIK.

OBSZAR

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

Opis stanu faktycznego

2.1. Oddział dysponował corocznie kwotą przeznaczoną na zakup oprogramowania narzędziowego, w ramach którego realizowane były bieżące potrzeby zgłaszane przez komórki merytoryczne. Zapotrzebowanie na oprogramowanie użytkowe od komórek organizacyjnych zbierał Wydział Informatyki. W ramach rzeczowego planu wydatków inwestycyjnych każde oprogramowanie powyżej kwoty 20 tys. zł było wpisywane do rocznego planu inwestycyjnego, który podlegał zatwierdzeniu przez Radę Centrali NFZ.

Analiza dziewięciu zakupionych licencji w okresie 2019-2022 wykazała, że liczba nabytych licencji była zgodna ze zgłoszonym zapotrzebowaniem komórek merytorycznych.
Oddział nie nabywał modułów do systemów zintegrowanych.
Nie było przypadku w Oddziale, aby otrzymał fakturę za nadmierne korzystanie z zakupionej wcześniej licencji.

W latach 2019-2022 Oddział wnioskował o zmiany w planie inwestycyjnym, które dotyczyły zakupu czterech oprogramowań. Były to oprogramowania: graficzne (2019 r.), oprogramowanie sieciowe do łączenia pracy zdalnej, oprogramowanie do skanowania dokumentów (2020 r.) oraz licencja na dodatkową pojemność systemu do zarządzania logami i bezpieczeństwem (2020 r. i 2021 r.). Przedmiotowe zmiany wynikały z zapotrzebowania na dodatkowe licencje wynikłe w toku użytkowania funkcjonujących oprogramowani, a trudne do przewidzenia na etapie pierwotnego planowania rocznego budżetu inwestycyjnego (np. konieczność pracy zdalnej).

(akta kontroli str. 130-171)

Naczelnik Wydziału Informatyki, wyjaśnił, że na podstawie opisu funkcjonalności jakiego potrzebowali pracownicy komórek merytorycznych, pracownicy Wydziału analizowali potrzebę zakupu i dobierali stosowne oprogramowanie kierując się efektywnością i bezpieczeństwem oprogramowania. Każdorazowo i dla każdego wytypowanego oprogramowania sprawdzany był poziom i typ licencji, tak aby optymalnie dopasować wartość zakupu do potrzebnych funkcjonalności. Pracownicy użytkujący oprogramowanie lub kierownicy komórek mogli zgłaszać problemy z funkcjonowaniem zakupionego oprogramowania, jednakże takie problemy nie były zgłaszane. Przykładem analiz zapotrzebowania oraz rozmów z użytkownikami był zakup rozszerzonej wersji programu Lex.

Oddział nie dysponował specjalistycznym oprogramowaniem, które umożliwiało systemowe monitorowanie efektywności wykorzystywania oprogramowania, jego faktycznego wykorzystania przez pracowników (np. po historii logowań). Posiadane oprogramowanie ServiceDesk nie posiada funkcjonalności pozwalającej na taki monitoring. Naczelnik wyjaśnił, że oprogramowanie narzędziowe zakupione w latach 2019-2022 na potrzeby pracowników miało jednostkowo „niską" wartość, natomiast sam zakup wyspecjalizowanego systemu do monitoringu wykorzystania aplikacji, byłby wysoki. Stosunek wartości systemu a korzyści płynące z przenoszenia aplikacji pomiędzy użytkownikami byłby niewspółmiernie wysoki.

(akta kontroli str. 134-135)

2.2. W latach 2019-2022 (do 30 czerwca 2022 r.) na zakup nowego oprogramowania komputerowego[15] Oddział wydatkował, odpowiednio: 252 tys. zł; 282,4 tys. zł; 668,5 tys. zł; 387,6 tys. zł. Na zakup wsparcia serwisowego, asysty technicznej, subskrypcji wydatkował w tym okresie, odpowiednio: 885,7 tys. zł; 119,5 tys. zł; 131,5 tys. zł; 1 459,4 tys. zł. Oddział wskazał czterech głównych producentów oprogramowania wykorzystywanego w Oddziale.

Oddział nie zakupywał oprogramowania w ramach projektów współfinasowanych ze środków UE.
Oddział nie zakupywał oprogramowania SaaS[16].

(akta kontroli str. 96-97, 43-50)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Oddział dokonywał zakupów oprogramowania wynikających z bieżących potrzeb głównie związanych z przyjętą organizacją pracy. Zmiany w planie inwestycyjnym dotyczące zakupu dodatkowych licencji w trakcie roku były jednostkowe i w części podyktowane czynnikami zewnętrznymi, jak dostosowanie Oddziału do pracy zdalnej. Analizy funkcjonalności zainstalowanego oprogramowania były prowadzone przez

[15] Łącznie 17 pozycji oprogramowania, w tym siedem oprogramowania serwerowego.
[16] SaaS - oprogramowanie jako usługa (Software as a Service, SaaS) 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

Wydział Informatyki Oddziału w trybie roboczym, między innymi poprzez rozmowy z pracownikami użytkującymi oprogramowanie.

IV. Uwagi i wnioski

W związku ze stwierdzoną nieprawidłowością, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następującą uwagę i wniosek:

Uwagi

Najwyższa Izba Kontroli zauważa, iż obowiązujące Oddział regulacje dotyczące zarządzania licencjami nie wprowadzały szczegółowych zasad zarządzania oprogramowaniem. W efekcie braku tych zasad m.in. nie określono częstotliwości prowadzenia monitorowania urządzeń pod kątem legalności oprogramowania, sporządzania raportów w tym zakresie, itp. W wyniku kontroli stwierdzono jednak przypadek instalacji oprogramowania, na które jednostka nie posiadała licencji. Wskazuje to na potrzebę bieżącego i skutecznego monitorowania oprogramowania, tak aby nie dochodziło do korzystania z nielegalnego oprogramowania.

Wnioski

Zakwestionowane oprogramowanie zostało odinstalowane w toku czynności kontrolnych, zatem Najwyższa Izba Kontroli nie formułuje wniosku w tym zakresie. NIK wnosi o podjęcie działań (współpracy z Centralą NFZ) mających na celu ustalenie szczegółowych zasad zarządzania licencjami określających m.in. częstotliwość monitorowania oprogramowania i sporządzania raportów w tym zakresie.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Krakowie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwagi i wykonania wniosku pokontrolnego oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Kraków, października 2022 r.

Kontroler
Monika Różańska
Główny specjalista kontroli
państwowej