WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI
MAŁGORZATA MOTYLOW

LPO.430.1.2023

Warszawa, 25 sierpnia 2023 r.

Pani
Magdalena Rzeczkowska
Minister Finansów

Szanowna Pani Minister,

w załączeniu przedkładam informację o wynikach kontroli zarządzania oprogramowaniem komputerowym przez administrację publiczną[11].

Najwyższa Izba Kontroli oceniła negatywnie zarządzanie oprogramowaniem komputerowym przez jednostki administracji publicznej. Zarządzanie tym zasobem w przypadku części podmiotów było również niegospodarne. Wyniki kontroli pokazały, że w podmiotach administracji publicznej instalowane było niepożądane oprogramowanie, szczególnie bez wsparcia producenta, w nieaktualnej wersji, w tym bez poprawek krytycznych bądź wymagające pilnej aktualizacji z uwagi na poważne zagrożenie bezpieczeństwa. Stwierdzono również programy nielegalne, a także niedopuszczone do użytkowania w organizacji. Żadna z kontrolowanych jednostek nie monitorowała w pełni posiadanego i wykorzystywanego oprogramowania.

Podmioty administracji publicznej nie w każdym przypadku starannie planowały i decydowały o nabyciu licencji, ponosząc niekiedy zbędne wydatki. W procesie pozyskiwania oprogramowania SaaS[12] nie w każdym przypadku dokonywano oceny spełniania możliwych do weryfikacji parametrów, ograniczających ryzyko zakupu oprogramowania niespełniającego wymogów organizacji. Z istotnymi problemami wiązał się także proces nabywania i wdrażania złożonych systemów informatycznych.

Nie w pełni skuteczne okazały się również działania w celu zapewnienia, efektywnego wykorzystania i monitorowania oprogramowania związanego z realizacją programów i projektów informatycznych zarządzanych przez Ministra Finansów.

Z poważaniem

M. Motylow

[11] Planowa kontrola koordynowana nr P/22/082 – *Zarządzanie oprogramowaniem komputerowym przez administrację publiczną.*
[12] ang. Software as a Service – oprogramowanie jako usługa.

NAJWYŻSZA IZBA KONTROLI

Informacja o wynikach kontroli

ZARZĄDZANIE OPROGRAMOWANIEM KOMPUTEROWYM PRZEZ ADMINISTRACJĘ PUBLICZNĄ

SIERPIEŃ 2023

LPO.430.001.2023
Nr ewid. 15/2023/P/22/082/LPO

Informacja o wynikach kontroli

ZARZĄDZANIE OPROGRAMOWANIEM KOMPUTEROWYM PRZEZ ADMINISTRACJĘ PUBLICZNĄ

DELEGATURA W POZNANIU

MISJĄ
Najwyższej Izby Kontroli jest niezależna, profesjonalna kontrola zadań publicznych w interesie obywateli i państwa

Informacja o wynikach kontroli
Zarządzanie oprogramowaniem komputerowym przez administrację publiczną

p.o. Dyrektor Delegatury NIK w Poznaniu
Karolina Wirszyc-Sitkowska

Karolina Wirszyc-Sitkowska

Akceptuję:
Wiceprezes Najwyższej Izby Kontroli

Małgorzata Motylow

Zatwierdzam:
Prezes Najwyższej Izby Kontroli

Marian Banaś
Warszawa, dnia 12.05.2023

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

SPIS TREŚCI

Zdjęcie na okładce:
stock.adobe.com/pl/Diana

Wykaz stosowanych skrótów, skrótowców i pojęć

aktualizacja oprogramowania	ang. *software update* – jest to zestaw zmian w programie komputerowym lub zestaw danych, zaprojektowany w celu aktualizacji, naprawy lub ulepszenia danego oprogramowania. Obejmuje to naprawę błędów, poprawę funkcjonalności, użyteczności lub wydajności[1];
inventory tool	ang. narzędzie do inwentaryzacji; oprogramowanie pozwalające zarządzać z jednego miejsca serwerami, stacjami roboczymi, laptopami, smartfonami i tabletami; umożliwia sprawdzenie w czasie rzeczywistym liczby zainstalowanych programów oraz porównanie monitorowanych systemów z dostępną liczbą licencji;
inwentaryzacja licencji	sporządzenie spisu używanych programów i aplikacji, wraz z informacjami o związanych z nimi licencjach lub też ich braku. Opiera się na: zebraniu informacji o zainstalowanych aplikacjach, sporządzeniu wykazu licencji, zgromadzeniu dokumentacji umów licencyjnych i faktur, porównaniu listy zainstalowanego oprogramowania z posiadanymi licencjami i analizie rozbieżności;
licencja komputerowa/ licencja na oprogramowanie	umowa określająca warunki korzystania z programów komputerowych; wyróżnia się licencję wyłączną – zastrzega wyłączność korzystania z utworu przez uprawnionego w określony sposób (nie można udzielić licencji innej osobie) oraz licencję niewyłączną – możliwe jest udzielanie licencji na ten sam utwór i w tożsamym zakresie wielu osobom[2];
oprogramowanie komputerowe	zbiór poleceń, które zostały napisane przez programistę (specjalistę) w języku komputerowym[3] (program komputerowy, aplikacja);
przeniesienie praw autorskich do oprogramowania	nabywca autorskich praw majątkowych staje się ich dysponentem, a prawa majątkowe zbywcy, co do zasady, w tym zakresie wygasają;
SaaS	ang. *Software as a Service* – oprogramowanie jako usługa;
SAM	ang. *Software Asset Management* – zarządzanie oprogramowaniem. Proces zapewniający pełną kontrolę nad licencjami oprogramowania, dający pewność, że są one wykorzystywane w sposób zgodny z prawem i korzystny dla organizacji. Proces ten pozwala skutecznie kontrolować i chronić zasoby oprogramowania[4];
systemy MDM/ EMM/UEM	ang. *Mobile Device Management* (oprogramowanie do zarządzania urządzeniami mobilnymi), *Enterprise Mobile Management* (zarządzanie urządzeniami przenośnymi), *Unified Endpoint Management* (zunifikowane zarządzanie punktami końcowymi), klasa narzędzi programowych m.in. do zarządzania urządzeniami mobilnymi;
subskrypcja	system sprzedaży związany ze zobowiązaniem się do zakupu i dokonania przedpłaty (abonament, prenumerata);
urządzenia mobilne	(przenośne) urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią. Dla celów kontroli jako mobilne zostały potraktowane (analogicznie jak w podmiotach kontrolowanych) urządzenia typu smartfon i tablet (z wyłączeniem laptopów).

---

1 Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Aktualizacja_oprogramowania (wg stanu na 15 marca 2023 r.).

2 Art. 67 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawie pokrewnym (Dz.U. z 2022 r., poz. 2509), dalej: ustawa o prawie autorskim.

3 Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Program_komputerowy (wg stanu na 5 lutego 2023 r.).

4 https://www.statlook.com/pl/zarzadzanie-oprogramowaniem/

5 https://dobryslownik.pl/slowo/subskrypcja/53914/

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli
Czy jednostki administracji publicznej prawidłowo i gospodarnie zarządzały oprogramowaniem komputerowym?

Pytania definiujące cele szczegółowe kontroli
1. Czy jednostki administracji publicznej podejmowały skuteczne działania w celu zapewnienia, efektywnego wykorzystania i monitorowania oprogramowania związanego z realizacją programów i projektów informatycznych?
2. Czy jednostki administracji publicznej rzetelnie zorganizowały i skutecznie realizowały proces postępowania z oprogramowaniem, a sposób użytkowania programów komputerowych był prawidłowy?
3. Czy jednostki administracji publicznej podejmowały skuteczne działania w celu optymalizacji wykorzystania oprogramowania, a środki publiczne związane z jego nabyciem i użytkowaniem były wydatkowane gospodarnie?

Jednostki kontrolowane
19[6] jednostek administracji publicznej, w tym dwie jednostki administracji rządowej, trzynaście jednostek samorządu terytorialnego, trzy inne państwowe jednostki organizacyjne i jedna państwowa osoba prawna

Jednostki objęte badaniem kwestionariuszowym
789[7] jednostek, w tym 695 dużych jednostek samorządu terytorialnego i 94 urzędy centralne

Okres objęty kontrolą
Lata 2019–2022 do dnia zakończenia kontroli, tj. 16 listopada 2022 r., z wykorzystaniem dowodów wytworzonych przed i po tym okresie, jeżeli miały one istotny wpływ dla ustaleń i ocen kontroli.

Zarządzanie oprogramowaniem wpływa na prawidłowe wykonywanie zadań przez administrację publiczną. Związane jest z efektywnym administrowaniem, kontrolą i ochroną zasobów. Bieżące monitorowanie oprogramowania oraz stanu uprawnień licencyjnych pozwala zoptymalizować wysokie koszty nabycia i utrzymania oprogramowania, a także minimalizować ryzyko poniesienia nieplanowanych wydatków.

Podobnie jak utwory np. literackie czy muzyczne, oprogramowanie podlega zasadom prawa autorskiego[8]. Powszechnie stosowaną metodą dystrybucji oprogramowania jest licencjonowanie. Dzięki umowom licencyjnym, w których twórca określa warunki użytkowania programu, użytkownik może legalnie korzystać z oprogramowania. Przy okazji należy pamiętać o konsekwencjach dotyczących naruszenia praw autorskich. W przypadku stwierdzenia nielegalnego oprogramowania licencjodawca będzie oczekiwał uiszczenia opłaty za zidentyfikowane rozbieżności. Dodatkowo, w zależności od producenta, może on zażądać opłaty za wsteczne wsparcie dla produktu. Koszty te mogą sięgać w skrajnych przypadkach nawet kilku milionów złotych[9].

Skuteczne gospodarowanie oprogramowaniem jest także ważnym elementem bezpieczeństwa informatycznego oraz ochrony danych osobowych wynikających z RODO[10]. Oprogramowanie może zawierać usterki i posiadać luki bezpieczeństwa. Jednostki powinny weryfikować, w jaki sposób oprogramowanie podatne na cyberataki znalazło się w zasobach organizacji – czy zostało zaktualizowane w odpowiednim momencie, czy w ogóle jest dopuszczone do użytkowania w podmiocie, w jaki sposób użytkownicy instalują je na swoich urządzeniach i wykorzystują w ramach swoich codziennych obowiązków[11]. Urzędy coraz częściej muszą mierzyć się ze skutkami ataków hakerskich.

Z przeprowadzonej analizy przedkontrolnej, w tym pozyskanych informacji, wynikało, że podmioty administracji publicznej rzadko przeprowadzają lub zlecają audyt oprogramowania w celu porównania liczby opłacanych licencji z liczbą licencji faktycznie potrzebnych i wykorzystywanych w jednostce.

---

6 W tym: 18 jednostek administracji publicznej, objętych kontrolą planową P/22/082 Zarządzanie oprogramowaniem komputerowym przez administrację publiczną, a także jedna objęta kontrolą doraźną: I/22/002 Gospodarowanie licencjami komputerowymi przeprowadzonej w II/III kwartale 2022 r.

7 Kwestionariusz wysłano do 993 podmiotów, w tym 893 jednostek samorządu terytorialnego oraz 100 urzędów centralnych. Raport z badania stanowi załącznik do niniejszej informacji o wynikach kontroli.

8 Por. przepisy Rozdziału 7 ustawy o prawie autorskim.

9 https://www2.deloitte.com/pl/pl/pages/technology/articles/Klauzule-audytowe-w-umowach-licencyjnych-czyli-co-licencjobiorca-wiedziec-powinien.html (stan na 10 marca 2023 r.)

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

11 https://www2.deloitte.com/pl/pl/pages/technology/articles/systemy-sam-wspierajacyberbezpieczenstwo.html (stan na 10 marca 2023 r.).

Dotychczas NIK nie podejmowała kontroli poświęconej w całości zarządzaniu oprogramowaniem komputerowym przez administrację publiczną. Elementy przedmiotowego problemu były natomiast objęte kontrolami dotyczącymi zapewnienia sprawności systemów informatycznych i bezpieczeństwa przetwarzanych informacji.

2. OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia negatywnie zarządzanie oprogramowaniem komputerowym przez jednostki administracji publicznej. Zarządzanie tym zasobem w przypadku części podmiotów było również niegospodarne[12].

Nieprawidłowe a niekiedy również niegospodarne zarządzanie oprogramowaniem komputerowym

W 15 z 17 (88%) objętych kontrolą podmiotów administracji publicznej instalowane było nieautoryzowane (niepożądane) oprogramowanie. Głównie były to programy bez wsparcia producenta, w nieaktualnej wersji, w tym bez poprawek krytycznych bądź wymagające pilnej aktualizacji z uwagi na poważne zagrożenie bezpieczeństwa (osiem z 17, tj. 47%). W prawie połowie jednostek zainstalowane było oprogramowanie nielegalne (na które urzędy nie posiadały licencji) (siedem z 17, tj. 41%), a także niedopuszczone do użytkowania w organizacji (siedem z 17, tj. 41%). Ponadto w sześciu podmiotach, tj. 35% stwierdzono występowanie aplikacji EOL (End of Life), wycofanych z uwagi na poważne luki w bezpieczeństwie. Przyczyną był brak wiedzy na temat zasad licencjonowania programów, brak skuteczności mechanizmów blokujących czy też znaczenia zorganizowania i prowadzenia regularnego monitorowania oprogramowania, niezależnie od miejsca jego instalacji. Poza nadzorem pozostawały programy instalowane na urządzeniach mobilnych.

Mimo podejmowania działań w celu optymalizacji wykorzystania oprogramowania w toku kontroli ujawniono przypadki niegospodarności na kwotę 12,5 mln zł. Związane one były głównie z nieprawidłowym planowaniem i nabywaniem licencji. W odniesieniu do tradycyjnego oprogramowania instalowanego na stacjach roboczych nieprawidłowości stwierdzono w dziewięciu na 17 podmiotów (53%). Dotyczyły braku weryfikacji zasadności zakupu, braku instalacji programów bezpośrednio po zakupie oraz dokonania zakupu zbyt dużej liczby, niewykorzystywanych licencji.

Przypadki nieprawidłowości dotyczyły również złożonych systemów informatycznych, np. zintegrowanych[13]. W sześciu z 14 (43%) podmiotów korzystających z ZSI stwierdzono m.in. naruszenia dot. przepisów ustawy o zamówieniach publicznych[14] w zakresie zamówienia w trybie z wolnej ręki oraz utrzymywania niewykorzystywanych modułów oprogramowania. Co więcej, w 10 z nich zidentyfikowano istotny problem dotyczący braku zapewnienia możliwości rozbudowy i utrzymania takiego oprogramowania bez ingerencji jego twórcy. W efekcie doprowadzono de facto do monopolizacji kluczowych, najdroższych rozwiązań IT, tj. sytuacji w której twórca dyktuje podmiotom publicznym warunki wieloletniej współpracy. W procesie nabywania oprogramowania SaaS nie w każdym przypadku (40%) dokonywano oceny spełniania możliwych do weryfikacji parametrów, ograniczających ryzyko zakupu oprogramowania niespełniającego wymogów organizacji.

Nie w pełni skuteczne okazały się także działania związane z realizacją programów i projektów informatycznych zarządzanych przez Ministra Finansów. Minister nie wyegzekwował od podmiotów, którym zlecono wytwarzanie, utrzymanie lub unowocześnianie oprogramowania poprawy terminowości usług i obniżenia stopnia występowania awarii systemów, a także stopnia realizacji umów z dostawcami zewnętrznymi. Nie zapewnił także wdrożenia zasad bezpieczeństwa oprogramowania wytwarzanego i utrzymywanego na jego rzecz, o standardzie nie niższym, od obowiązującego w Ministerstwie i jednostkach resortu finansów.

---

12 Cel szczegółowy nr 1 realizowano w kontroli planowej P/22/082 w Ministerstwie Finansów oraz spółce Aplikacje Krytyczne sp. z o.o., natomiast cele szczegółowe nr 2 i 3 – tożsamy zakres przedmiotowy realizowano w 16 jednostkach w kontroli planowej P/22/082 oraz jednym podmiocie, w którym przeprowadzono kontrolę I/22/002.

13 Dalej: ZSI.

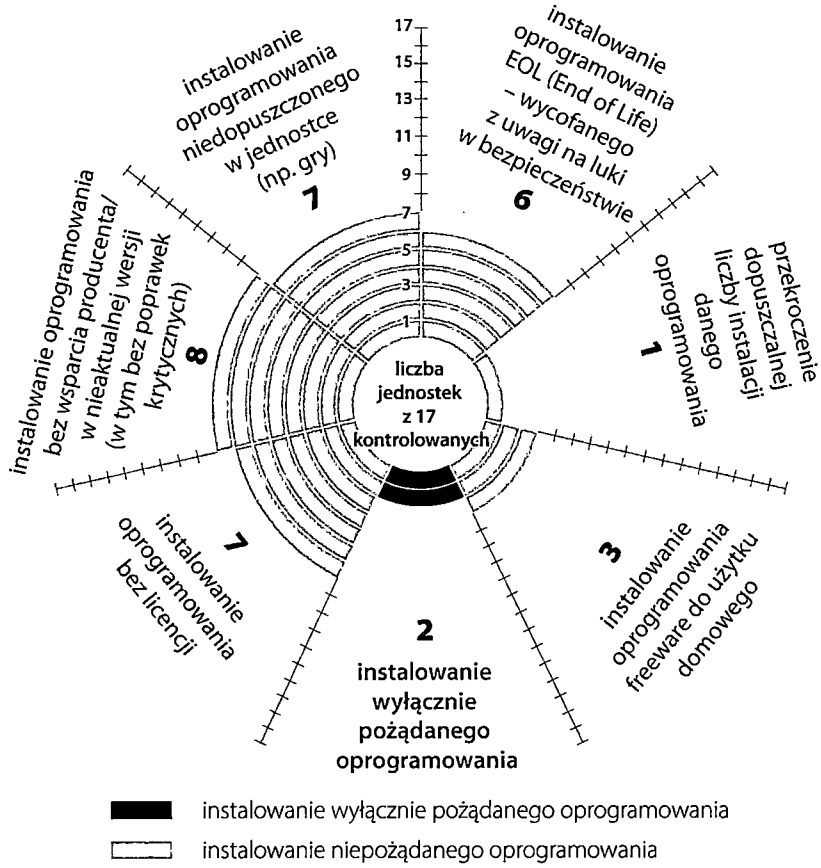
14 W okresie objętym kontrolą obowiązywała ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, ze zm.) oraz – od 1 stycznia 2021 r. – ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, ze zm.), dalej: pzp, ustawa o zamówieniach publicznych.

3. SYNTEZA WYNIKÓW KONTROLI

Instalowanie nieautoryzowanego oprogramowania

W 15 z 17 (88%) kontrolowanych podmiotów stwierdzono instalację nieautoryzowanego (niepożądanego) oprogramowania. Najczęściej występującym problemem było instalowanie oprogramowania bez wsparcia producenta, w nieaktualnej wersji (w tym bez poprawek krytycznych bądź wymagających pilnej aktualizacji z uwagi na poważne zagrożenie bezpieczeństwa) (ośmiu z 17, tj. 47%), nielegalnego (na które urząd nie posiadał licencji) (siedmiu z 17, tj. 41%), a także niedopuszczonego w urzędzie (siedmiu z 17, tj. 41%). W sześciu podmiotach, tj. 35% stwierdzono instalowanie oprogramowania EOL (End of Life), wycofanego z uwagi na poważne luki w bezpieczeństwie. Wyżej wymienionej instalacji dokonywali zarówno informatycy, jak i pracownicy poszczególnych jednostek. Instalacja oprogramowania nie w każdym przypadku uwzględniała weryfikację warunków umowy licencyjnej. Nie w pełni skuteczne okazały się również stosowane mechanizmy blokujące możliwość nieuprawnionej instalacji. [str. 23–24]

Infografika nr 1
Instalowanie nieautoryzowanego (niepożądanego) oprogramowania



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

Brak regularnych przeglądów oprogramowania na urządzeniach stacjonarnych

Żaden z podmiotów nie potwierdził, że na bieżąco i przede wszystkim skutecznie (podejmując adekwatne działania naprawcze) sprawdzał stacje robocze i udostępnione udziały sieciowe użytkowników pod kątem obecności nieautoryzowanego oprogramowania[15]. Część z nich deklarowała

[15] Jedna z jednostek – Urząd Miasta Bydgoszczy – przez osiem miesięcy nie posiadała narzędzia *inventory tool* – w lutym 2022 r., wycofała oprogramowanie w związku z oszacowanym ryzykiem wykorzystania go do ataku na systemy teleinformatyczne.

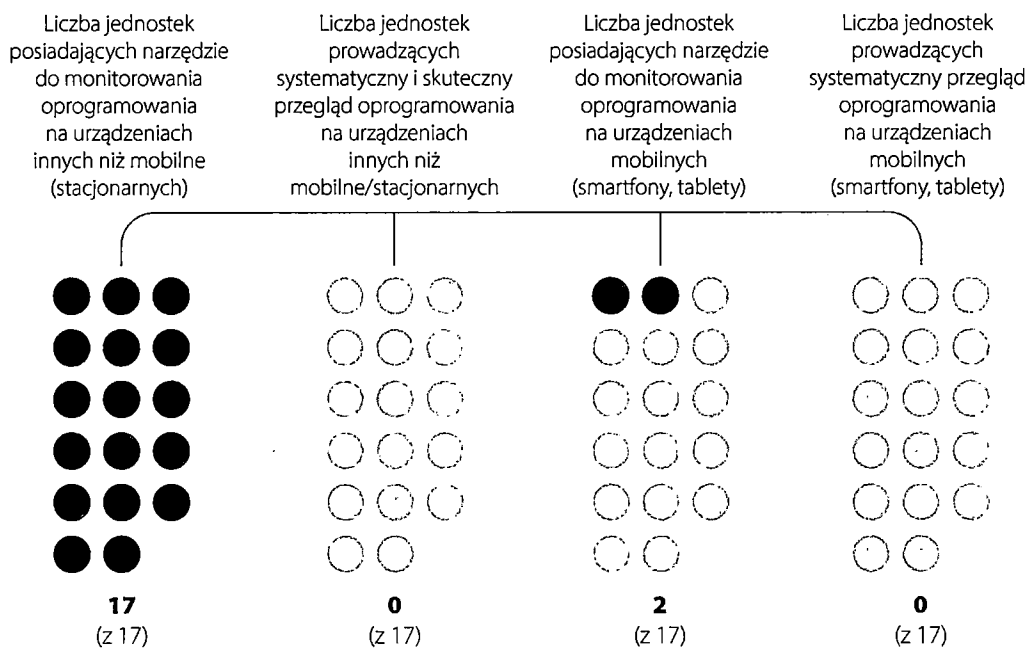
monitorowanie zasobów, niemniej jednak po pierwsze nie były dostępne żadne dowody potwierdzające ten fakt, a po drugie – o braku skuteczności tych działań świadczy zidentyfikowanie w toku kontroli nieautoryzowanego oprogramowania. Na uwagę zasługuje ponadto fakt, iż w zdecydowanej większości jednostek deklarowano stosowanie mechanizmów blokady możliwości samodzielnego instalowania oprogramowania jako optymalnego mechanizmu kontrolnego. [str. 21–22]

Nieefektywne wykorzystanie narzędzi do monitorowania oprogramowania

Brak dowodów potwierdzających wykonywanie regularnych przeglądów mimo posiadania rozwiązań technicznych świadczy o nieefektywnym wykorzystaniu narzędzi *inventory tool* (posiadanych przez wszystkie podmioty), do monitorowania oprogramowania na urządzeniach stacjonarnych.

Z badań ankietowych[16] wynikało, że mniej niż połowa objętych badaniem podmiotów posiadała zdolność do automatycznego potwierdzenia legalności całego posiadanego oprogramowania, niezależnie od miejsca jego instalacji i użytkowania.

Infografika nr 2
Monitorowanie oprogramowania



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

[str. 21–22]

Brak regularnych przeglądów oprogramowania na urządzeniach mobilnych

W żadnej jednostce nie prowadzono w zaplanowanych odstępach czasu przeglądów urządzeń mobilnych (smartfonów, tabletów) użytkowników pod kątem obecności nieautoryzowanego oprogramowania. Przyczyną tego faktu był brak rozwiązań organizacyjnych (przypisanej odpowiedzialności)

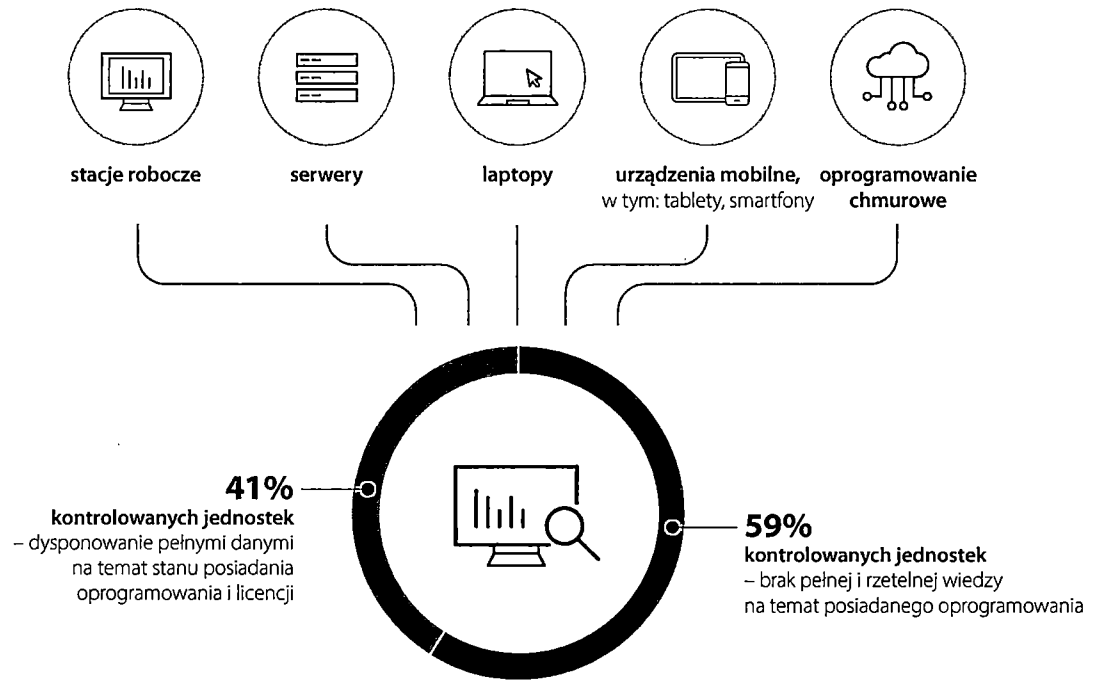
[16] W celu uzyskania informacji dotyczących zarządzania oprogramowaniem komputerowym, Delegatura NIK w Poznaniu wystosowała, korzystając z uprawnień wynikających z art. 29 ust. 1 pkt 2 lit. f ustawy z 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK), zapytanie do 100 urzędów centralnych i 893 jednostek samorządu terytorialnego. Wsparcie informatyczne i analiza danych wynikowych badania były realizowane przez Wydział Wsparcia Informatycznego i Analitycznego w Departamencie Metodyki Kontroli i Rozwoju Zawodowego NIK. Raport stanowi załącznik do niniejszej informacji.

i technicznych (brak odpowiednich narzędzi, np. systemu MDM/EMM/UEM – narzędzia takie posiadały tylko dwa podmioty) w celu prowadzenia stałego i bieżącego monitoringu oprogramowania na tego typu urządzeniach. Ponadto część podmiotów nie miała świadomości zagrożeń i konsekwencji związanych z instalowaniem i użytkowaniem oprogramowania na urządzeniach mobilnych pozostających poza nadzorem, deklarując że urządzenia te służą użytkownikom wyłącznie do realizacji połączeń telefonicznych. [str. 22]

Brak działań w celu ustalenia stanu wolnego oprogramowania

We wszystkich objętych kontrolą jednostkach prowadzone były spisy oprogramowania i licencji. Rejestry pozwalały na identyfikację użytkownika oprogramowania i miejsca jego instalacji, a także liczby wolnych licencji, niemniej jednak w większości przypadków prowadzone ewidencje nie były kompletne (10 z 17, tj. 59%). Nie zawierały bowiem pełnej informacji na temat zainstalowanego i wykorzystywanego oprogramowania. W efekcie niejednokrotnie nie było możliwe ustalenie rzetelnej liczby faktycznie wykorzystanych, zainstalowanych programów, a deklarowany jako możliwy do ustalenia stan wolnego/wykorzystanego oprogramowania dotyczył jedynie pozycji uwzględnionych w spisie. [str. 19–20]

Infografika nr 3
Identyfikacja posiadanego oprogramowania/licencji



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

Brak zasad zarządzania oprogramowaniem

Praktycznie żadna z kontrolowanych jednostek nie ustanowiła i nie wdrożyła formalnych zasad zarządzania oprogramowaniem, obejmujących cały cykl jego życia, w tym określających co najmniej takie kwestie jak: role i odpowiedzialność, nabywanie i wycofywanie licencji, dbałość o dowody zakupu, ewidencjonowanie, zasady dystrybucji i redystrybucji, inwentaryzację i przeglądy, bezpieczeństwo i nośniki instalacyjne, monitorowanie stanu użycia, ważności i legalności licencji, a także konieczność podejmo-

wania ewentualnie działań naprawczych (16 z 17, tj. 94%)[17]. Część podmiotów (3 z 17, tj. 18%) wdrożyła pewne formalne procedury dotyczące zasad postępowania z oprogramowaniem, niemniej jednak kwestie w nich uwzględnione nie obejmowały ww. elementów sprzyjających skuteczności i efektywności zarządzania licencjami (oprogramowaniem).

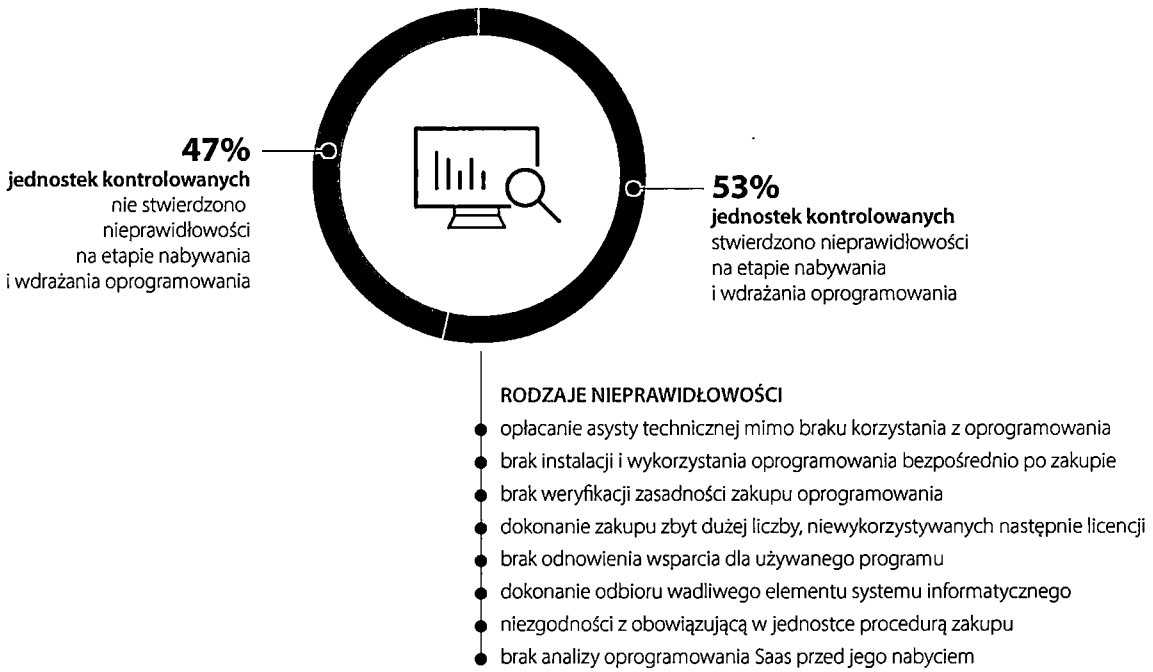
W przeprowadzonym badaniu ankietowym, aż 91,3% ankietowanych podmiotów deklarowało wdrożenie procedur zarządzania oprogramowaniem, niemniej jednak żaden z nich nie ujął w procedurach wszystkich elementów niezbędnych do zapewnienia skuteczności i efektywności tego procesu. [str. 16–17]

Brak uwzględnienia w procesie planowania rzeczywistych potrzeb jednostek

We wszystkich jednostkach proces nabywania licencji był scentralizowany, tzn. uprawnienia do zakupów licencji miała jedna, wyznaczona komórka organizacyjna, we wszystkich przypadkach właściwa ds. informatyzacji albo zakup bądź instalacja oprogramowania wymagała akceptacji tejże komórki. Miało to na celu m.in. zapewnienie pozyskania optymalnej liczby licencji, odpowiedniej do wymaganego zastosowania operacyjnego. W dziewięciu z 17 (53%) podmiotów stwierdzono jednak nieprawidłowości na etapie nabywania lub wdrażania oprogramowania, które wskazywały, że proces ten mógł nie być optymalny. W efekcie m.in. nabyte zostały licencje, które nie były wykorzystywane bądź nawet zainstalowane albo zakupione w liczbie większej niż faktycznie była potrzebna. [str. 26–27]

Przypadki niepełnego wykorzystania posiadanych programów i aplikacji

Infografika nr 4
Nieprawidłowości na etapie nabywania i wdrażania oprogramowania



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

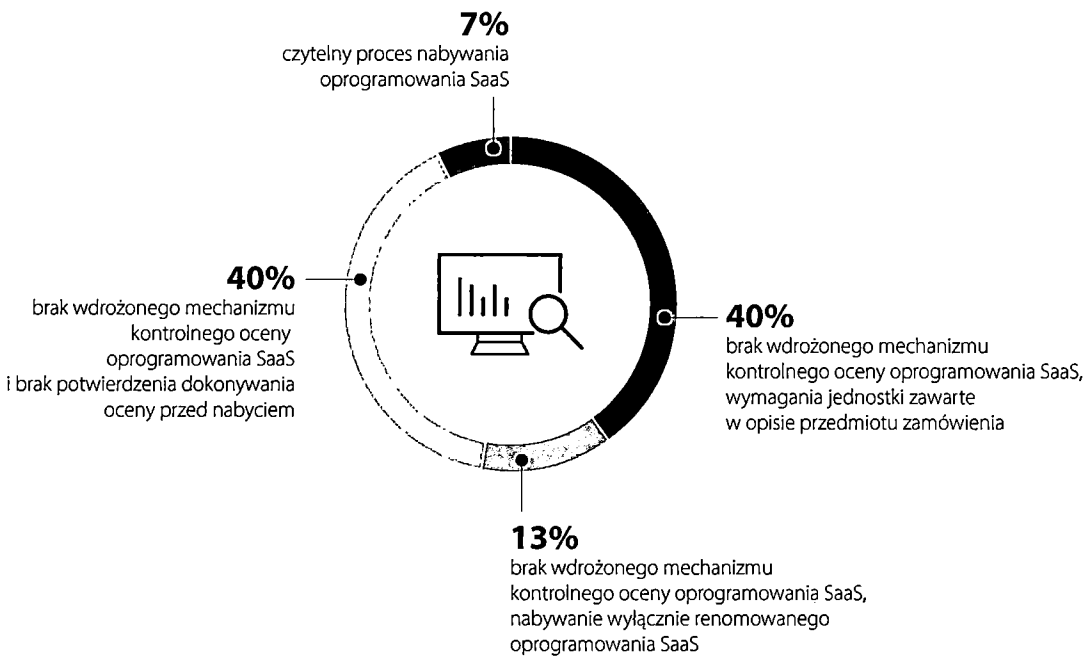
[17] Według najlepszych praktyk zarządzania licencjami opracowanych przez *The International Association of Information Technology Asset Managers, Inc* (tłum. ang. Międzynarodowe Stowarzyszenie Zarządzających Aktywami Technologii Informatycznych). Zakres przedmiotowy kontroli został ustalony na podstawie pozyskanych przez NIK w toku analizy przedkontrolnej materiałów eksperta z dziedziny audytu systemów informatycznych, biegłego sądowego z dziedziny IT.

Przypadki braku zabezpieczenia potrzeb jednostki w procesie nabywania oprogramowania SaaS

Mimo znaczącego rozwoju usług chmurowych[18] w procesie pozyskiwania oprogramowania SaaS nie zawsze ustalono zasady analizy planowanego do zakupu oprogramowania traktowanego jako usługa (93% jednostek), a także nie w każdym przypadku dokonywano oceny możliwych do weryfikacji parametrów, ograniczających na tym etapie ryzyko nabycia oprogramowania niespełniającego wymogów organizacji (40% podmiotów). Podmioty nie sprawdzały każdorazowo, czy np. nabywają oprogramowanie od wiarygodnych dostawców, ani nie weryfikowały dostępności umowy SLA w tym również pod kątem wymogów organizacji, zapewnienia wsparcia technicznego czy bezpieczeństwa. Przedmiotem oceny nie zawsze były również wymagania związane z zarządzaniem danymi czy RODO.

[str. 31–32]

Infografika nr 5
Nabywanie oprogramowania SaaS



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

Połowa ankietowanych wskazała, że nie wdrożyła procedur nabywania oprogramowania, w tym w modelu SaaS, natomiast te które deklarowały ich wdrożenie (23% spośród korzystających z tego rodzaju oprogramowania) nie ujęły w zasadach elementów wskazanych w tym procesie – przez powołanego w toku kontroli biegłego – jako niezbędne. [str. 31–32]

Problematyczne wdrażanie i użytkowanie oprogramowania zintegrowanego

Większość jednostek (14 z 17, tj. 82%) korzystała ze zintegrowanych systemów informatycznych (ZSI). W sześciu na 14 podmiotów (tj. 43%) stwierdzono jednak nieprawidłowości w użytkowaniu tego oprogramowania

[18] Corocznie przeprowadzane badanie Deloitte Global IT Asset Management (ITAM) w edycji 2022 skupia uwagę na trzech filarach procesu zarządzania IT, w tym: powiązaniem między zarządzaniem zasobami IT a cyberbezpieczeństwem; wieloaspektowości chmury i zarządzaniu zasobami IT i zrównoważonym rozwoju; https://www2.deloitte.com/pl/pl/pages/technology/articles/IT_Asset_Management_ITAM_Global_Survey_2022.html (wg stanu na 10 lutego 2023 r.).

polegające m.in. na: naruszeniu przepisów ustawy pzp[19] w zakresie stosowania zamowienia w trybie z wolnej ręki, ponoszeniu opłat za niewykorzystywane moduły oprogramowania, korzystanie z oprogramowania serwerowego bez wsparcia producenta, dokonaniu odbioru i opłaty za wadliwy moduł, zawyżeniu wysokości opłaty za obsługę oprogramowania. Aż w 10 na 14 jednostek (71%) stwierdzono również brak zapewnienia możliwości rozbudowy i utrzymania systemów we własnym zakresie (bez ingerencji ich twórcy). Zważywszy, że były to programy użytkowane i rozbudowywane nawet od trzydziestu lat, realnym był problem uzależnienia się jednostek publicznych od jednego producenta kluczowego, drogiego oprogramowania. Co więcej, w toku kontroli stwierdzono fakt, że w przypadku objętych kontrolą jednostek zdecydowanie dominowali dwaj producenci takiego oprogramowania. [str. 28–30]

Nie w pełni skuteczny nadzór Ministra nad projektami i programami informatycznymi

W Ministerstwie Finansów nie zapewniono w pełni skutecznego nadzoru nad Centrum Informatyki Resortu Finansów[20] i Aplikacje Krytyczne sp. z o.o.[21], w zakresie w jakim podmioty te zajmowały się wytwarzaniem, utrzymaniem lub unowocześnianiem oprogramowania na potrzeby Ministerstwa i pozostałych jednostek resortu finansów. Nie wyegzekwowano od CIRF wykonania działań naprawczych dotyczących zidentyfikowanych problemów w zakresie poprawy terminowości usług i obniżenia stopnia występowania awarii, a także stopnia realizacji umów z dostawcami zewnętrznymi. Nie zapewniono także faktycznego przejęcia przez ten podmiot wszystkich praw i obowiązków wynikających ze stosunków prawnych, w tym umów i porozumień dotyczących zamówień teleinformatycznych. Nie zostało także zapewnione stosowanie przez AKMF zasad bezpieczeństwa teleinformatycznego o standardzie nie niższym, od obowiązującego w Ministerstwie i jednostkach resortu finansów. [str. 38]

Konieczność uiszczenia opłaty za wsteczne wsparcie licencji

Ministerstwo nierzetelnie i niezgodnie z przepisami ustawy pzp[22] przeprowadziło postępowanie o udzielenie zamówienia publicznego na zakup usługi wsparcia i rozwoju systemu Centralny Service Desk. Wskutek powyższego w jednostce podległej – CIRF – wystąpiła konieczność wydatkowania kwoty 1419 tys. zł za sam fakt wznowienia wsparcia w związku z opóźnieniem w zawarciu umowy. [str. 38]

Nie wpełni skuteczny nadzór spółki nad oprogramowaniem

W podmiocie realizującym projekty informatyczne zarządzane przez Ministra Finansów, tj. spółce AKMF nie zautomatyzowano procesu monitorowania posiadanych i użytkowanych licencji, a także nie objęto monitoringiem wszystkich urządzeń, na których instalowane było oprogramowanie.

---

19 Zamawiający nie wykazali każdorazowo spełnienia przesłanek udzielenia zamówienia z wolnej ręki, określonych w art. 214 ust. 1 pkt 1 lit. b pzp lub art. 214 ust. 1 pkt 1 lit. a i b pzp albo art. 67 ust. 1 pkt 1 lit. a lub lit. b (w odniesieniu do obowiązującej do 31 grudnia 2020 r. ustawy z 29 stycznia 2004 r.)

20 Dalej: CIRF.

21 Dalej: AKMF.

22 Krajowa Izba Odwoławcza stwierdziła naruszenia dot. zaniechania wykluczenia z postępowania wykonawców, w związku z brakiem wykazania spełnienia warunku udziału w postępowaniu, a w konsekwencji zaniechaniu odrzucenia złożonej przez nich oferty; dokonanie błędnej oceny oferty złożonej przez wykonawców w zakresie wystąpienia rażąco niskiej ceny oraz złożonych przez tych wykonawców wyjaśnień, co skutkowało zaniechaniem odrzucenia złożonej przez nich oferty jako zawierającej rażąco niską cenę w zakresie Asysty Technicznej; zaniechanie odrzucenia oferty wykonawców ze względu na to, że jej złożenie stanowiło czyn nieuczciwej konkurencji.

Spółka prowadziła ewidencję zakupionych i użytkowanych licencji (w formie zestawienia elektronicznego), która nie była jednak kompletna bowiem nie zawierała informacji na temat wszystkich licencji oraz dat ich wygasania.

Monitoring instalowanego oprogramowania odbywał się z wykorzystaniem specjalistycznego narzędzia, nie był on jednak w pełni skuteczny, gdyż urządzenia końcowe nie były aktualizowane przy pomocy tego narzędzia pod kątem monitorowania zainstalowanych na tych urządzeniach aplikacji. W jednostce nie zapewniono stałego monitorowania części urządzeń mobilnych co do legalności instalowanego i wykorzystywanego oprogramowania (21% użytkowanych smartfonów, a także jeden tablet).

[str. 39–41]

Ryzykowny mechanizm wydłużonego czasu weryfikacji oprogramowania

W spółce Aplikacje Krytyczne sp. z o.o. nie zapewniono bieżącej weryfikacji instalowanego oprogramowania pod kątem warunków licencyjnych oraz bezpieczeństwa. Przyjęty czas weryfikacji zainstalowanych aplikacji był wydłużony, co skutkowało ryzykiem użytkowania nielegalnego oprogramowania, w tym korzystania z aplikacji niebezpiecznych. Przyjęty model postępowania był ryzykowny również ze względu na liczbę pracowników posiadających uprawnienia do instalowania oprogramowania na stacjach roboczych. Przedmiotowe rozwiązanie było wątpliwe zwłaszcza z uwagi na profil działalności Spółki i związane z nim oczekiwanie stosowania najwyższych standardów zarówno pod kątem zarządzania oprogramowaniem, jak i w aspekcie bezpieczeństwa. [str. 39–41]

4. WNIOSKI

Jednostki samorządu terytorialnego oraz inne państwowe jednostki organizacyjne

Najwyższa Izba Kontroli wskazuje na konieczność podejmowania przez kierowników jednostek administracji publicznej niezbędnych działań służących zapewnieniu prawidłowego zarządzania oprogramowaniem komputerowym, w tym w szczególności:

- określenie i wprowadzenie szczegółowych zasad zarządzania oprogramowaniem (licencjami), w tym nabywania oprogramowania SaaS;
- wprowadzenie rozwiązań technicznych zapewniających kompletność danych o posiadanym oprogramowaniu;
- objęcie bieżącym monitorowaniem całego oprogramowania, niezależnie od miejsca jego instalacji i dokumentowanie podejmowanych czynności, w tym działań naprawczych;
- prowadzenie regularnej analizy stopnia wykorzystania poszczególnych aplikacji.

Ministerstwa

Najwyższa Izba Kontroli wskazuje na konieczność podejmowania przez kierowników jednostek zlecających realizację projektów i programów informatycznych niezbędnych i skutecznych działań nadzorczych wobec podmiotów, którym zlecono ich realizację, w celu:

- skutecznego egzekwowania wykonywania działań naprawczych dotyczących zidentyfikowanych problemów, mogących wpływać negatywnie na efektywność działań dotyczących wytwarzanego, utrzymywanego bądź unowocześnianego przez te podmioty oprogramowania na rzecz jednostki zlecającej;
- zapewnienia bezpieczeństwa informatycznego wytwarzanego i utrzymywanego oprogramowania o standardzie nie niższym, od obowiązującego w podmiocie zlecającym;
- opracowania i skutecznego wdrożenia w resorcie katalogu oprogramowania dopuszczonego i niedopuszczonego.

Podmioty publiczne, które zostały utworzone w celu wytwarzania, utrzymania lub unowocześniania oprogramowania na potrzeby ministerstw

W odniesieniu do podmiotów publicznych, utworzonych w celu wytwarzania, utrzymania lub unowocześniania oprogramowania na potrzeby ministerstw Najwyższa Izba Kontroli wskazuje za niezbędne:

- objęcie regularnym monitorowaniem całego oprogramowania, niezależnie od miejsca jego instalacji;
- instalowanie jedynie oprogramowania dopuszczonego do użycia w ramach organizacji.

5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. Organizacja, użytkowanie i nadzór nad oprogramowaniem komputerowym

W objętych kontrolą jednostkach nie określono szczegółowych zasad zarządzania licencjami obejmujących wszystkie elementy i wymagane czynności niezbędne do zarządzania i nadzoru nad pełnym cyklem życia oprogramowania. W większości podmiotów nie zapewniono skutecznego nadzoru nad całym instalowanym i wykorzystywanym oprogramowaniem, ani stałej i bieżącej kompletności danych na temat wszystkich posiadanych i wykorzystywanych licencji w ramach stosowanego narzędzia do ich monitorowania. Wskutek tego, posiadane narzędzia do monitorowania oprogramowania instalowanego na urządzeniach stacjonarnych nie mogły być w pełni efektywnie wykorzystane. Nie potwierdzono wykonywania audytów (przeglądów) pod kątem wykrycia nieautoryzowanego oprogramowania. Z uwagi na brak rozwiązań technicznych niezbędnych do zarządzania urządzeniami mobilnymi i kompletności danych o użytkowanych licencjach jednostki nie mogły wykonywać automatycznego porównania wskazującego na legalność (lub jej brak) całości oprogramowania. W większości kontrolowanych jednostek podejmowane działania dotyczące zarządzania posiadanym oprogramowaniem były nieskuteczne, w toku kontroli stwierdzono bowiem przypadki instalowania nieautoryzowanego oprogramowania.

Brak zasad zarządzania oprogramowaniem

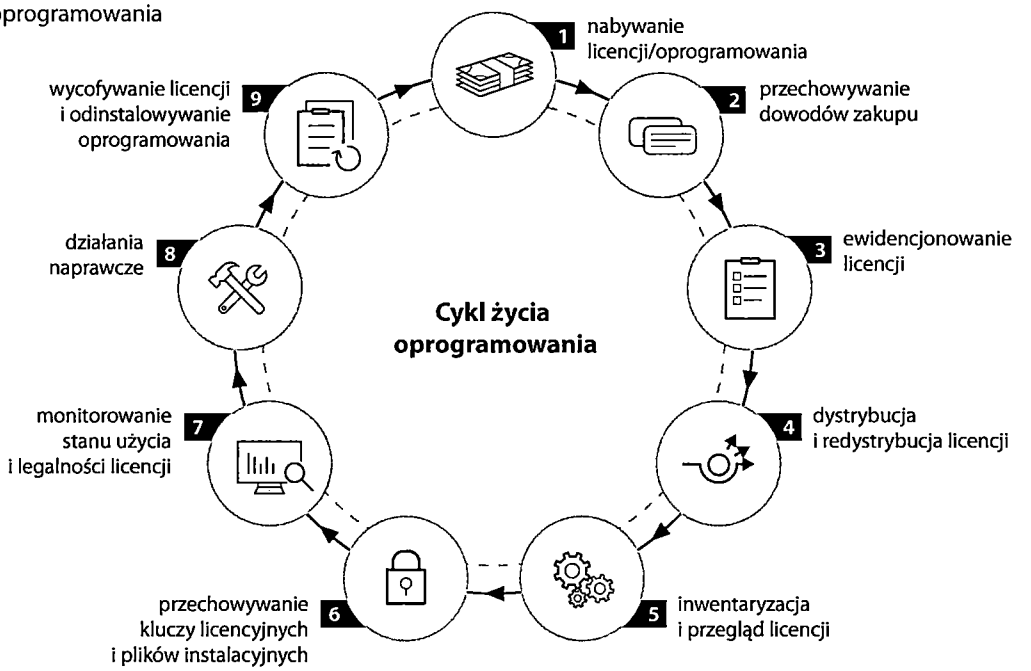
Samorządy oraz państwowe jednostki organizacyjne wyodrębniły w swoich strukturach komórki odpowiedzialne za m.in.: informatyzację urzędu, zapewnienie ciągłości działania systemów informatycznych, prace programistyczne, nadawanie użytkownikom uprawnień do systemów IT, a także administrowanie i nadzór nad licencjami/oprogramowaniem. Pomimo przypisania tym komórkom zadań z zakresu zarządzania i nadzoru nad posiadanymi i wykorzystywanymi licencjami/oprogramowaniem i wprowadzeniem szeregu uregulowań, w 16 z 17 skontrolowanych podmiotów (91,7%)[23] nie ustanowiono i nie wdrożono szczegółowych zasad zarządzania licencjami, które obejmowałyby co najmniej takie kwestie jak: zasady (listę kontrolną) nabywania uwzględniające obowiązek i kryteria (zakres) weryfikacji pod kątem bezpieczeństwa, wsparcia itp., zasady gromadzenia i przechowywania dowodów zakupu, zasady ewidencjonowania (z uwzględnieniem wszystkich rodzajów urządzeń końcowych) i utrzymania kompletności i aktualności, zasady dystrybucji i redystrybucji licencji, zasady wycofywania licencji i odinstalowywania z urządzeń, zasady i częstotliwość okresowych przeglądów, zasady monitorowania stanu użycia i legalności, działania naprawcze i inne zapewniające skuteczność i efektywność zarządzania licencjami. W trzech spośród tych jednostek zasady były uwzględniane, ale wyłącznie częściowo[24]. Aby zapewnić skuteczny nadzór nad instalowanym i wykorzystywanym oprogramowaniem, w ramach działań związanych z zarządzaniem urządzeniami dostępnymi dla użytkownika końcowego oraz oprogramowaniem zainstalowanym na tych zasobach winny być uwzględnione wszelkie zasoby (np. smartfony)

[23] We wszystkich z wyjątkiem Urzędu Miasta Krakowa.

[24] Urząd Marszałkowski Województwa Małopolskiego, Małopolski Oddział Wojewódzki NFZ w Krakowie, Urząd Morski w Szczecinie.

i systemy operacyjne. Brak zasad zarządzania licencjami może utrudniać lub uniemożliwiać skuteczne zarządzanie i nadzór nad oprogramowaniem. Bez ustanowionych reguł (w tym m.in. przypisania odpowiedzialności za poszczególne zadania w tym procesie) istnieje ryzyko zagrożeń związanych z odpowiedzialnością prawną i problemami technicznymi. Istnieje również ryzyko, że gospodarowanie to nie jest optymalne, co może spowodować skutki finansowe (np. konieczność wypłaty odszkodowania i poniesienia kosztów prawnych) oraz skutki niefinansowe (np. utrata reputacji).

Infografika nr 6
Cykl życia oprogramowania



Źródło: opracowanie własne NIK na podstawie pozyskanych w toku kontroli sprawozdań biegłego.

W przeprowadzonym badaniu ankietowym, aż 91,3% ankietowanych podmiotów deklarowało wdrożenie procedur zarządzania oprogramowaniem, niemniej jednak żaden z nich nie ujął w procedurach wszystkich elementów niezbędnych do zapewnienia skuteczności i efektywności tego procesu. Należy w szczególności zwrócić uwagę na fakt, że tylko co trzecia jednostka deklarowała w badaniu, że w procedurach ujęła m.in. sposób realizacji działań naprawczych, a niewiele ponad połowa (56,1%) zasady monitorowania oprogramowania. Większość podmiotów nie uwzględniła ponadto zasad: nabywania licencji, wycofywania i odinstalowywania oprogramowania, sposobu i bezpieczeństwa przechowywania kluczy licencyjnych, dystrybucji i redystrybucji.

Przykłady

W **Urzędzie Miejskim w Koszalinie** w latach 2019–2022 (do 7 października), nie określono szczegółowych zasad zarządzania licencjami obejmujących wszystkie elementy i wymagane czynności niezbędne do zarządzania i nadzoru nad całym cyklem życia oprogramowania, mimo wyznaczenia komórki organizacyjnej odpowiedzialnej za kompleksową obsługę oprogramowania i przypisaniu pracownikom tej komórki zadań nadzoru nad eksploatacją oprogramowania. Oprócz przydziału Wydziałowi Informatyki ogólnego zada-

nia dotyczącego administrowania systemami operacyjnymi i bazami danych oraz sprawowania nadzoru nad eksploatacją oprogramowania nie określono szczegółowych odpowiedzialności i zadań, m.in. w zakresie: zasad (listy kontrolnej) nabywania, w tym weryfikacji pod kątem bezpieczeństwa oraz zasad wycofywania licencji, zasad przechowywania dowodów zakupu, ewidencjonowania, dystrybucji i redystrybucji, inwentaryzacji i przeglądów, bezpieczeństwa i nośników instalacyjnych, monitorowania (stanu użycia i legalności licencji) oraz działań naprawczych.

W **Kujawsko-Pomorskim Urzędzie Wojewódzkim w Bydgoszczy** w Polityce Bezpieczeństwa Informacji nie uwzględniono w szczególności zasad dotyczących: monitorowania i nadzoru nad stanem użycia i legalności oprogramowania oraz nadzoru nad realizacją procedury związanej z zarządzaniem licencjami, w tym na urządzeniach typu smartfony/tablety; zakresu koniecznej weryfikacji pod kątem wymagań bezpieczeństwa w ramach nabywania licencji, w tym oprogramowania w modelu SaaS oraz zasad dopuszczania programów do instalacji np. darmowych; przechowywania i zabezpieczania dostępu do nośników instalacyjnych, jak również kluczy licencyjnych i innych dokumentów licencyjnych, w tym utrzymywanych w środowiskach chmurowych; zasad ewidencjonowania wszystkich posiadanych i używanych licencji, w tym oprogramowania w modelu SaaS, w taki sposób, aby spis zapewniał dostępność aktualnych informacji na temat liczby posiadanych oraz wykorzystywanych licencji dla osób odpowiedzialnych za instalację; wycofywania/odinstalowywania (z uwzględnieniem wszystkich rodzajów urządzeń końcowych) licencjonowanego oprogramowania, którego termin ważności licencji się kończy i konieczności użycia właściwego dla danego oprogramowania narzędzia deinstalacji; odniesienia do zmian licencyjnych pojawiających się na rynku oprogramowania, np. monitorowania środowiska J(...).

Zasoby kadrowe zarządzające oprogramowaniem

Zadania związane z zarządzaniem licencjami/oprogramowaniem sprawowane były przez pracowników zatrudnionych w komórkach informatycznych, a także w komórkach wykonujących zadania z zakresu bezpieczeństwa i zarządzania kryzysowego (m.in. w Urzędzie Miasta Poznania, Kujawsko-Pomorskim Urzędzie Wojewódzkim w Bydgoszczy oraz Kapitanacie Portu w Szczecinie i Wydziale Elektroniki i Łączności (obie w strukturach Urzędu Morskiego w Szczecinie)). Problemy z zapewnieniem właściwego poziomu wykonania zadań wynikały z braków etatów (Urząd Miasta Poznania i Urząd Miasta Tarnowa), a także z trudności związanych zapewnieniem obsady kadrowej (Urząd Morski w Szczecinie, Urząd Miasta Szczecina, Urząd Miasta Krakowa, Urząd Miasta Poznania). Przyczyną takiego stanu była fluktuacja kadr spowodowana głównie niskim poziomem wynagrodzeń, ale także proponowana forma wykonywania pracy (brak możliwości wykonywania pracy w formie zdalnej), czy duża konkurencyjność komercyjnego rynku IT.

Przykłady

W **Urzędzie Miasta Szczecina** Zastępca Wydziału Informatyki jako przyczynę braku zainteresowania naborami podała ograniczone możliwości finansowe w zakresie wysokości proponowanego wynagrodzenia, brak możliwości wykonywania pracy zdalnej i duży popyt rynku komercyjnego IT.

W **Urzędzie Miasta Poznania** w okresie od stycznia 2019 r. do marca 2022 r. z pracy zrezygnowało ośmiu pracowników Wydziału Informatyki, a w przeprowadzonych 24 naborach dziewięciu kandydatów nie podjęło zatrudnienia z uwagi na wysokość proponowanego wynagrodzenia.

W **Urzędzie Miasta Tarnowa** NIK wnioskowała o rozważenie zwiększenia liczby zatrudnionych wykwalifikowanych pracowników w Wydziale Informatyzacji z uwagi na strategiczny charakter wykonywanych zadań.

Podniesienie kompetencji kadr zarządzających licencjami/oprogramowaniem poprzez zapewnienie specjalistycznych szkoleń w tym zakresie zapewniło zaledwie pięć jst[25], przy czym w trzech urzędach pracownicy uczestniczyli w jednym szkoleniu (Urząd Miasta Torunia i Urząd Miasta Szczecin, Urząd Marszałkowski Województwa Zachodniopomorskiego), w Urzędzie Miasta Poznania – w dwóch szkoleniach, a w Urzędzie Miasta Krakowa w większej liczbie szkoleń.

Przykład

W **Urzędzie Marszałkowskim Województwa Podkarpackiego** w badanym okresie nie było szkoleń dla pracowników realizujących zadania w procesie zarządzania oprogramowaniem/licencjami. (...) Zastępca Dyrektora Departamentu Organizacyjno-Prawnego Urzędu wyjaśnił m.in., że *nikt w Urzędzie nie zgłaszał potrzeb w kontrolowanym okresie, co do realizacji szkoleń wewnętrznych (bądź zewnętrznych).*

Posiadanie dowodów legalności oprogramowania

Wszystkie objęte kontrolą jednostki (17) posiadały dowody legalności wybranego do kontroli oprogramowania, a także nośniki/pliki instalacyjne i klucze licencyjne. Zarówno dokumenty, jak i pliki instalacyjne były zabezpieczone przed nieuprawnionym dostępem, modyfikacją i zniszczeniem, przechowywane w odpowiednio przygotowanym miejscu (w szafie bądź na dysku), do którego dostęp mieli wyłącznie upoważnieni pracownicy.

W okresie objętym kontrolą pracownicy podmiotów kontrolowanych wytworzyli oprogramowanie, które następnie było użytkowane w tychże jednostkach. Realizacja takich zadań odbyła się w ramach obowiązków służbowych, a w urzędach dysponowano odpowiednim kodem źródłowym do powstałych aplikacji. Prawa majątkowe do programu stworzonego w wyniku wykonywania obowiązków ze stosunku pracy przysługiwały pracodawcy.

Zasady akceptowalnego użytkowania oprogramowania

We wszystkich jednostkach określono i wdrożono zasady akceptowalnego użycia służbowych zasobów sprzętu komputerowego czy oprogramowania. Pracownicy zapoznawali się z zasadami i potwierdzali ten fakt stosownym oświadczeniem. W każdym przypadku zapewniono, że po ewentualnym odejściu pracownika i związanym z tym zwolnieniem licencjonowanego oprogramowania oprogramowanie to jest zwalniane i dostępne dla innego pracownika albo czeka na instalację (dalszą dystrybucję).

Brak wiedzy o posiadanych licencjach/ oprogramowaniu

Nieprawidłowości w prowadzonych spisach (ewidencjach) licencji/ oprogramowania stwierdzono w 10[26] z 17 jednostek objętych kontrolą (tj. 59%). Z założenia spisy powinny dotyczyć wszystkich posiadanych

[25] Dotyczyło to: Urzędu Miasta Torunia, Urzędu Miasta Krakowa, Urzędu Marszałkowskiego Województwa Zachodniopomorskiego, Urzędu Miasta Szczecin, Urzędu Miasta Poznania.

[26] Były to: Urząd Marszałkowski Województwa Kujawsko-Pomorskiego, Urząd Miasta Bydgoszczy, Urząd Miasta Torunia, Kujawsko-Pomorski Urząd Wojewódzki, Urząd Miasta Tarnowa, Urząd Marszałkowski Województwa Podkarpackiego, Urząd Miejski w Mielcu, Podkarpacki Oddział Wojewódzki NFZ w Rzeszowie, Urząd Marszałkowski Województwa Zachodniopomorskiego, Urząd Morski w Szczecinie.

licencji, na podstawie których możliwa jest identyfikacja użytkownika, właściciela lub miejsce zainstalowania. Powinny także wskazywać daty wygaśnięcia licencji (subskrypcji), uwzględniać przeniesienia licencji pomiędzy użytkownikami (stanowiskami lub serwerami), zawierać informację o wolnych/użytkowanych licencjach, czyli stanowić atrybut pozwalający zarządzać oprogramowaniem, minimalizując ryzyko naruszenia zasad bezpieczeństwa i legalności posiadanych licencji. Nierzetelność ewidencji wynikała z braku jej kompletności, tj. nieujęcia części licencji zainstalowanych na stacjach roboczych lub laptopach lub wszystkich zainstalowanych na urządzeniach mobilnych (typu smartfon lub tablet), a także z atomizacji informacji na temat posiadanych/użytkowanych licencji w kilku i tak niekompletnych ewidencjach. Wyniki kontroli wskazują, że 90% jednostek, których wykazy były wadliwe prowadziły równoległe spisy za pomocą kilku różnych narzędzi (takich jak: ewidencja wartości niematerialnych i prawnych, zestawienia elektroniczne czy oprogramowanie typu *inventory tool*).

Warto zwrócić uwagę, że nie wszystkie ankietowane podmioty deklarowały wdrożenie zasad ewidencjonowania oprogramowania. Zapewnienie w tym zakresie złożyło 69,6% z nich. Zważywszy na fakt, iż nie każde oprogramowanie stanowi wartość niematerialną i prawną (np. oprogramowanie jako usługa), brak prowadzenia spisu licencji (oprogramowania) powodował, że w urzędach nie było jednego rejestru umożliwiającego stałą weryfikację posiadania licencji na każde zainstalowane oprogramowanie.

Przykłady

W **Urzędzie Marszałkowskim Województwa Zachodniopomorskiego** prowadzone spisy licencji i oprogramowania[27] nie obejmowały wszystkich urządzeń wykorzystywanych w Urzędzie. Nie ujmowano w nich oprogramowania instalowanego na telefonach (smartfonach) lub tabletach (poza oprogramowaniem instalowanym przez pracowników Biura Informatyki przed ich przekazaniem użytkownikom[28]).

W **Kujawsko-Pomorskim Urzędzie Wojewódzkim w Bydgoszczy** stosowane w Urzędzie *inventory tool* nie zapewniało kompletności danych odnoszących się do posiadanych i wykorzystywanych licencji, wygenerowane na jego podstawie raporty obarczone były błędami, a zestawienia nie były pełne. W Urzędzie brak było zautomatyzowanych rozwiązań zapewniających dostępność kompletnych i aktualnych informacji o posiadanych i wykorzystywanych licencjach w ramach wszystkich użytkowanych zasobów sprzętowych. W związku z tym w okresie objętym kontrolą Urząd nie posiadał pełnej informacji na temat wszystkich zakupionych licencji. Prowadzone przez pracowników Urzędu rejestry były nierzetelne, żaden z nich nie był kompletny.

W **Podkarpackim Oddziale Wojewódzkim NFZ w Rzeszowie**, pomimo określonemu w § 44 ust. 2 Polityki Zarządzania bezpieczeństwem teleinformatycznym NFZ (PZSZ/014), obowiązkowi prowadzenia dla każdego podsystemu ewidencji posiadanych licencji na wykorzystane oprogramowanie rejestry nie posiadały danych o całym posiadanym oprogramowaniu oraz o dat wygaśnięcia licencji.

[27] Z wykorzystaniem programów: A(...); e(...) oraz uprawnienia.wzp.pl.

[28] e(...) i O(...).

Nieefektywne wykorzystanie narzędzia do ewidencjonowania i monitorowania oprogramowania

Wszystkie urzędy posiadały narzędzia typu *inventory tool*, nabyte zarówno w okresie objętym kontrolą jak i w latach wcześniejszych. Najdłużej takie oprogramowanie, od 2010 r., użytkowane było w Podkarpackim Oddziale Wojewódzkim NFZ w Rzeszowie. Wysokość wydatków na nabycie powyższego oprogramowania w poszczególnych urzędach wyniosła od 19,9 tys. zł. do 201 tys. zł, a wydatki na jego utrzymanie w okresie objętym kontrolą wynosiły od 9,4 tys. zł do 490 tys. zł. W skontrolowanych podmiotach *inventory tool* nie był w pełni efektywnie wykorzystywany. Stwierdzone nieprawidłowości polegały na braku przeprowadzania systematycznego, okresowego audytu licencji i oprogramowania, który potwierdziłby aktualność i kompletność prowadzonych spisów, posiadanie (albo brak) dowodów potwierdzających legalność licencji/oprogramowania. W ocenie powołanych biegłych powyższe stwarzało ryzyko, że urzędy nie dysponowały zdolnością wykrycia nieautoryzowanego oprogramowania i/lub nie miały świadomości istnienia nielegalnego oprogramowania, co w konsekwencji może prowadzić do kar finansowych, ale i utraty wizerunku.

Mimo tego, że 70,8% ankietowanych jednostek zadeklarowało przeprowadzanie w sposób ciągły i automatyczny przeglądu oprogramowania, to tylko 58,7% z nich przyznało, że prowadzony przegląd oprogramowania obejmuje wszystkie urządzenia, na których instalowane i wykorzystywane było oprogramowanie. Ponadto, tylko 45% deklarowało posiadanie dedykowanego temu celowi narzędzia. Znaczy to, że mniej niż połowa objętych badaniem ankietowym podmiotów posiadała zdolność do automatycznego potwierdzenia legalności całego posiadanego oprogramowania, niezależnie od miejsca jego instalacji i użytkowania.

Przykłady

W **Urzędzie Miasta Torunia** nie zbierano danych w trybie rzeczywistym i ciągłym na zasobach, tj. nie monitorowano stanu użycia i legalności licencji poprzez wykonywanie cyklicznych przeglądów licencji (określenie cyklu, monitorowanie poziomu wykorzystania i daty ważności – szczególnie w przypadkach czasowych subskrypcji, wymagany sposób i elementy raportowania). W Urzędzie zakupiono narzędzie *inventory tool* w 2013 r. za kwotę 64,0 tys. zł i wydano, w latach 2019–2021, na przedłużenie umowy i wsparcie techniczne 47,4 tys. zł. Pomimo, że istniały możliwości programowe, nie były one wykorzystywane. Tym samym posiadając profesjonalne narzędzie prowadzono ewidencję w arkuszu kalkulacyjnym.

W **Urzędzie Miasta Poznania** nie w pełni efektywnie wykorzystywano posiadane narzędzie do monitorowania oprogramowania – L(...) – mimo stałego ponoszenia wydatków z tytułu serwisu tego oprogramowania, które w tym okresie wyniosły 161,5 tys. zł (narzędzie było także stosowane jako helpdesk). Nie zapewniono stałej i bieżącej kompletności danych na temat wszystkich posiadanych i wykorzystywanych licencji w ramach tego narzędzia, czego przykładami było:

- wprowadzenie informacji o 55 licencjach oprogramowania pakietu biurowego prawie pół roku po jego nabyciu (niektóre komórki Urzędu samodzielnie nabywały i użytkowały oprogramowanie, w tym zwłaszcza w modelu SaaS i nie przekazywały stosownej informacji Wydziałowi Informatyki, bądź czyniły to ze znaczącym opóźnieniem);
- utrzymywanie wpisów archiwalnych;
- brak monitorowania w sposób ciągły kto w jednostce wykorzystuje lub rozpoczął wykorzystywanie rozwiązania w modelu SaaS.

W **Urzędzie Morskim w Szczecinie** w okresie objętym kontrolą, nie w pełni efektywnie wykorzystywano posiadane narzędzie do monitorowania oprogramowania i zarządzania oprogramowaniem:

a) Pomimo dysponowania wolnymi stanowiskami w ramach posiadanej licencji systemu, nie zainstalowano i nie zarejestrowano go na części urządzeń poza wyłączoną z założenia z monitorowania kancelarią niejawną i siecią separowaną. Uniemożliwiało to objęcie tych stanowisk monitorowaniem z użyciem systemu w kontrolowanym okresie[29].
b) Nie zautoryzowano 115 (21,1%) komputerów z zainstalowanym systemem oraz nie zapewniono właściwej konfiguracji tego systemu, umożliwiającej uzyskiwanie rzetelnych danych o oprogramowaniu z aktualnie użytkowanych komputerów.
c) Nie wykorzystywano funkcjonalności rozliczenia licencji i nie wykonywano inwentaryzacji oprogramowania z wykorzystaniem systemu. Nie wprowadzono do systemu wszystkich danych o posiadanych licencjach, co uniemożliwiało efektywne monitorowanie rozliczenia instalacji w odniesieniu do posiadanych licencji z zastosowaniem tego narzędzia.

Brak zarządzania i nadzoru nad oprogramowaniem instalowanym na urządzeniach mobilnych

Mechanizm służący skutecznemu nadzorowi i zarządzaniu urządzeniami mobilnymi, tj. narzędzie klasy UEM, MDM czy też EMM, posiadał zaledwie jeden urząd (Urząd Miasta Rzeszowa), jednak nie był on wykorzystywany. Również jeden (Urząd Miasta Krakowa) był w trakcie wdrażania takiego oprogramowania. W Oddziałach Wojewódzkich NFZ w Rzeszowie i Krakowie nie dokonywano przeglądów urządzeń mobilnych, w związku z decyzją Prezesa NFZ z 27 września 2021 r., ustanawiającą odstępstwo od zapisów dokumentacji Systemu Zarządzania Bezpieczeństwem. Odstępstwo było związane z trwającymi pracami nad wdrożeniem: zmian organizacyjnych (tj. opracowaniem Polityki zarządzania urządzeniami mobilnymi) i środków technicznych do zarządzania urządzeniami mobilnymi. W jednym urzędzie (Urząd Miasta Szczecin) zarządzanie urządzeniami mobilnymi było wykonywane przez Miejską Jednostkę Obsługi Gospodarczej[30]. W żadnym podmiocie nie potwierdzono dokonywania przeglądu oprogramowania instalowanego bądź wykorzystywanego na urządzeniach mobilnych.

Przykłady

W **Urzędzie Miasta Bydgoszczy** nie zapewniono technicznych rozwiązań umożliwiających skuteczne i rzeczywiste zarządzanie posiadanymi zasobami, takimi jak urządzenia mobilne (np. nie wdrożono narzędzia klasy MDM czy też EMM), tym samym Urząd nie posiadał skutecznych mechanizmów nadzoru i monitorowania instalowania oraz użycia oprogramowania na urządzeniach mobilnych w czasie rzeczywistym i w trybie ciągłym.

Urząd Miasta Tarnowa nie zarządzał skutecznie zasobami sprzętowymi, takimi jak smartfony i tablety pod kątem instalacji i wykorzystywania oprogramowania (brak zarządzania oprogramowaniem znajdującym się na tych zasobach). Urząd nie posiadał narzędzi klasy UEM, MDM czy EMM, nie potwierdził także prowadzenia monitorowania oprogramowania instalowanego na urządzeniach mobilnych w inny sposób, np. manualny.

[29] W trakcie kontroli nie udało się ustalić jaki procent urządzeń, na których była możliwość instalacji narzędzia do monitorowania nie została objęta faktycznym nadzorem w poszczególnych latach kontrolowanego okresu. System swoim działaniem obejmował komputery pracujące w sieci w siedzibie jednostki oraz w komórkach organizacyjnych zlokalizowanych poza jej siedzibą.

[30] Jednostki budżetowa Gminy Miasto Szczecin.

Urząd Miasta Rzeszowa nie monitorował urządzeń mobilnych (smartfony, tablety). Pomimo posiadania dedykowanego narzędzia zawierającego system klasy MDM oraz podpięcia pod ten system służbowych smartfonów, nie objęto monitorowaniem oprogramowania instalowanego na tych urządzeniach. Prezydent wyjaśnił, że urządzenia mobilne typu smartfony i tablety były głównie wykorzystywane do prowadzenia rozmów głosowych oraz ewentualnego mobilnego dostępu do Internetu i nie były wykorzystywane do pracy z systemami teleinformatycznymi Urzędu, w związku z czym nie prowadzono inwentaryzacji oprogramowania na tego typu urządzeniach

W **Urzędzie Miejskim w Koszalinie**, w okresie objętym kontrolą, nie zapewniono organizacyjnych i technicznych rozwiązań umożliwiających skuteczne i rzeczywiste zarządzanie posiadanymi zasobami, takimi jak smartfony czy tablety. Zarządzanie zasobami sprzętowymi dostępnymi dla użytkownika końcowego oraz oprogramowaniem zainstalowanym na tych zasobach ograniczono jedynie do stacji roboczych (komputerów) pracujących pod kontrolą systemu operacyjnego (...).

Instalowanie nieautoryzowanego oprogramowania

Żadna z kontrolowanych jednostek nie poniosła kar z tytułu nielegalnego lub nieprawnie użytkowanego oprogramowania. Z ustaleń kontroli wynika jednak, że na zasobach informatycznych urzędów instalowane były przez indywidualnych użytkowników programy informatyczne w nieaktualnej wersji, bez wsparcia producenta (osiem z 17, tj. 47%), bez licencji (siedem z 17, tj. 41%), niedopuszczonego w urzędzie (siedem z 17, tj. 41%), programy EOL, tzw. End of Life – wycofane z uwagi na luki w bezpieczeństwie (sześć z 17, tj. 35%), instalowano licencje w większej liczbie niż posiadano licencji (jeden z 17, tj. 6%). Nieprawidłowości w tym zakresie stwierdzono w 15[31] skontrolowanych podmiotach (88%). Instalacja oprogramowania nie w każdym przypadku uwzględniała weryfikację warunków umowy licencyjnej. Świadczył o tym m.in. fakt stwierdzenia w toku kontroli przypadków instalowania oprogramowania bez licencji, w tym błędnie uznanego przez podmioty kontrolowane za darmowe, podczas gdy z zasad licencjonowania wynikało, że oprogramowanie to nie jest darmowe dla urzędów (podmiotów publicznych), a także składane wyjaśnienia o braku wiedzy pracowników na temat zasad licencjonowania danego oprogramowania. Ponadto, przykładowo aż 54,3% ankietowanych korzystających z darmowego oprogramowania wskazało, że w jednostce nie jest prowadzona weryfikacja darmowego oprogramowania (nie jest monitorowana i gromadzona dokumentacja w tym zakresie).

Przykłady

W **Urzędzie Morskim w Szczecinie** w wyniku przeprowadzonych podczas kontroli NIK oględzin oprogramowania zainstalowanego na 39 stanowiskach komputerowych pracowników Urzędu, w tym z udziałem biegłego stwierdzono:

a) na dwóch stanowiskach oprogramowanie, które – według informacji zamieszczonych na stronie producenta – w wersji *free* i *professional* oraz – co zostało potwierdzone przez biegłego – było przeznaczone wyłącznie do użytku domowego;

[31] Sytuacja taka nie zaistniała tylko w Urzędzie Miasta Poznania oraz Urzędzie Marszałkowskim Województwa Małopolskiego.

b) na pięciu stanowiskach oprogramowanie, które według informacji zamieszczonych na stronie jego autora było dostarczane jako *freeware*, ale tylko do prywatnego, niekomercyjnego użytku (to znaczy w domu). Program ten był bezpłatny do użytku edukacyjnego (szkoły, uniwersytety, muzea i biblioteki) oraz do użytku w organizacjach charytatywnych lub humanitarnych. Również według opinii biegłego licencja była darmowa, ale tylko do użytku niekomercyjnego i wymagała zakupu licencji dla Urzędu.

W **Urzędzie Miasta Szczecin**, powołany biegły stwierdził, że: *W toku prowadzonych czynności przeprowadzono weryfikację zainstalowanego oprogramowania pod kątem nielegalnych programów na podstawie komputerów wytypowanych z systemu e(...). Z przeprowadzonych testów na wybranej próbie komputerów zidentyfikowano tzry 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 (...) w wersji wyższej niż (...) – której to licencjonowanie przez firmę O (...) zostało zmienione – w efekcie przestaje być darmową do użytku komercyjnego od 16 kwietnia 2019 roku (...).*

W **Urzędzie Miasta Rzeszowa** w wyniku badań przeprowadzonych przez biegłego ujawniono przypadki instalacji oprogramowania w wersji określonej jako EOL[32] (dot. oprogramowania T(...)) czyli takiego, które zostało oficjalnie wycofane ze względu na luki w bezpieczeństwie. Zidentyfikowano również użycie programów np.: T (...), który był zainstalowany na zbyt dużej liczbie stacji lub W (...). Ponadto wystąpiły przypadki braku aktualizacji serwerów (w tym poprawek krytycznych) oraz używania starych wersji aplikacji (bez najnowszych poprawek (np. F (...)). Biegły stwierdził również przypadki użycia aplikacji *portable*[33], a także brak zdefiniowania zasad blokowania na poziomie *Manage Engine/Endpoint Central*[34].

W **Urzędzie Miasta Torunia** w trakcie kontroli ujawniono:

a) na wybranych losowo urządzeniach, przypadki instalacji oprogramowania EOL, czyli takie, które zostało oficjalnie wycofane ze względu na luki w bezpieczeństwie;
b) instalację dwóch programów nieuwzględnionych w wykazie posiadanych licencji;
c) korzystanie ze starych wersji aplikacji, w tym nawet krytycznych, wymagających aktualizacji;
d) aplikacje niezwiązane z pracą. Na poddanych badaniu komputerach zainstalowane było oprogramowanie do odtwarzania plików audio oraz nagrywania płyt CD, w bardzo starej wersji.

Nieskuteczne blokady instalacji oprogramowania oraz brak obowiązku zapoznania się z warunkami licencji

Przyczyną powyższych nieprawidłowości było przekonanie jednostek o skuteczności stosowanych dotychczas narzędzi blokujących możliwość instalacji nieautoryzowanego oprogramowania, ale także brak pewności, że każdorazowo osoba odpowiedzialna za instalacje zapoznała się i faktycznie zaakceptowała warunki licencji.

[32] Oprogramowanie typu End of Life – oprogramowanie, dla którego producent zakończył wsparcie techniczne.

[33] Oprogramowanie niewymagające instalacji.

[34] Oprogramowanie do zarządzania zintegrowane z innymi aplikacjami.

Przykłady

W **Urzędzie Miasta Koszalina** Kierownik Referatu Informatycznej Obsługi Urzędu wyjaśnił, że *dotychczasowo stosowane rozwiązanie dotyczące pozbawienia użytkowników prawa do samodzielnej instalacji oprogramowania uznawaliśmy za wystarczające, co było zgodne z Polityką Bezpieczeństwa Informacji. Wykonany audyt oprogramowania 7 września wykazał jednak, że mogą się zdarzyć niepożądane przypadki. Pracownicy IT zareagowali natychmiastowo, usuwając niepożądane oprogramowanie. Jednocześnie widzimy zasadność okresowego wykonywania i analizowania audytu. Sądzimy, że raz na miesiąc.*

W **Urzędzie Morskim w Szczecinie** w ocenie biegłego powyższe nieprawidłowości mogły wynikać z braku obowiązku zapoznania się osoby odpowiedzialnej za instalację z warunkami licencji, aby wychwycić użytkowane programy *freeware/portable* pod kątem wymogów licencyjnych. Brak mechanizmu kontrolnego zapewniającego, że proces instalacji oprogramowania zawsze uwzględnia konieczność zapoznania się osoby odpowiedzialnej za instalację/udostępnienie z warunkami umowy licencyjnej i zapewnienie z nimi zgodności, stwarza ryzyko naruszenia warunków umów licencyjnych. Pracownicy w wyjaśnieniach podali, że (...) nie znali szczegółowych warunków licencji.

W **Podkarpackim Oddziale Wojewódzkim NFZ w Rzeszowie** nie określono wprost odpowiedzialności za weryfikację umów licencyjnych i utrzymanie zgodności z przepisami praw autorskich i praw pokrewnych na wszystkich zasobach sprzętowych.

W **Urzędzie Marszałkowskim Województwa Podkarpackiego** brak było dokumentów potwierdzających, kto jest odpowiedzialny za weryfikację umów licencyjnych i utrzymanie zgodności z przepisami praw autorskich i praw pokrewnych na wszystkich zasobach sprzętowych oraz monitorowanie urządzeń przenośnych.

Prawidłowe postępowanie z oprogramowaniem zainstalowanym na zbywanych/likwidowanych nośnikach

Przekazywanie do ponownego użycia i zbywanie sprzętu IT w jednostkach odbywało się zgodnie z przyjętymi procedurami (lub praktykami). Oprogramowanie było odinstalowane lub nadpisane. W jednym przypadku, tj. w Urzędzie Miasta Tarnowa, stwierdzono, że nie posiadano procedur oraz dokumentacji potwierdzającej usunięcie danych z dysków przekazanych do ponownego użycia, nie posiadano również dedykowanego oprogramowania do trwałego wymazywania danych z nośników i funkcji wystawiającej certyfikat, który potwierdzałby wymazanie danych na nośniku o danym numerze seryjnym.

Prawidłowe gospodarowanie oprogramowaniem w przypadkach ustania stosunku pracy

Bez zakłóceń i przestojów przebiegało zagospodarowanie licencji zwalnianych, wynikających z ustania stosunku pracy. W zależności od rozwiązań przyjętych przez podmioty, tj. przypisania licencji do stanowisk (stacji roboczych, laptopów) albo do pracowników, licencje były: przekazywane nowozatrudnionym pracownikom, przeinstalowywane na inne urządzenia, stacje trafiały do magazynu albo licencje wracały do puli licencji wolnych. Jedynie w Urzędzie Marszałkowskim Województwa Zachodniopomorskiego dwóm pracownikom[35], z którymi rozwiązano stosunek pracy w sierpniu 2019 r. oraz lutym 2021 r., w toku kontroli NIK nadal przypisana była w spisie licencji odpowiedzialność za sześć licencji. W tym samym Urzędzie stwierdzono, że w przypadku 25 osób nie dotrzymano wymaganych terminów, tj. do trzech dni roboczych przed terminem obowiązywania dotychczasowych warunków zatrudnienia, dotyczących

[35] Badaniem objęto 10 spośród 182 osób, z którymi rozwiązano stosunek pracy.

wysłania wniosku w sprawie wyrejestrowania użytkownika z systemu. Odebranie uprawnień w systemach informatycznych 24 użytkownikom, realizowane było już po terminie obowiązywania dotychczasowych warunków zatrudnienia. Wnioski o odebranie uprawnień 21 użytkownikom wysłano po rozwiązaniu stosunku pracy (od dwóch do ośmiu dni roboczych po ustaniu zatrudnienia), a w dwóch – na jeden i dwa dni robocze przed tym terminem. W jednym przypadku wniosek wysłano 29 września 2022 r. (w toku kontroli NIK), tj. blisko trzy miesiące od daty rozwiązania stosunku pracy. W innej sprawie nie wysłano wymaganego wniosku, mimo upływu blisko dziewięciu miesięcy od daty rozwiązania stosunku pracy. Powyższe miało wpływ na to, że uprawienia użytkownikom odbierane były po ustaniu zatrudnienia w Urzędzie. Dane odnotowane w programie Urzędu nie wykluczyły w dwóch przypadkach możliwości logowania się takich osób do zasobów informatycznych Urzędu.

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

Proces pozyskiwania oprogramowania był najczęściej scentralizowany, zgodny z ustalonymi zasadami zakupowymi. Jednostki podejmowały działania w celu optymalizacji wykorzystania oprogramowania, niemniej jednak w części z nich na etapie jego nabywania i wdrażania stwierdzono nieprawidłowości. Dotyczyły one m.in. braku instalacji oprogramowania bezpośrednio po zakupie, braku weryfikacji zasadności zakupu programów, dokonania zakupu zbyt dużej liczby, niewykorzystywanych licencji. W większości kontrolowanych jednostek korzystających z SaaS z nienależytą starannością zorganizowano proces nabycia tego oprogramowania. W trakcie jego pozyskiwania nie zawsze też (40% podmiotów) dokonywano oceny i weryfikacji spełniania wymagań jednostki. Powyższe miało znaczenie z uwagi na ograniczony wpływ jednostek na eksploatację tego oprogramowania czy prawidłowość przetwarzania danych w toku jego użytkowania, które miało miejsce poza strukturą IT urzędu. Proces rozbudowy i utrzymania ZSI w sześciu jednostkach (43% nabywających ZSI) wiązał się jednak z istotnymi błędami dotyczącymi: naruszenia przepisów ustawy o zamówieniach publicznych w zakresie zamówienia w trybie z wolnej ręki, utrzymywania niewykorzystywanych modułów oprogramowania, niezapewnienia aktualizacji oprogramowania serwerowego czy atrybutu rozliczalności modułu. Ponadto w większości jednostek zidentyfikowano brak zapewnienia możliwości rozbudowy i utrzymania takiego oprogramowania bez ingerencji jego twórcy. W toku kontroli – w części jednostek – stwierdzono przypadki niegospodarnego postępowania z oprogramowaniem na kwotę 11,1 mln zł.

Planowanie środków finansowych na nabycie i utrzymanie licencji

Wszystkie jednostki zaplanowały środki finansowe na zakup licencji i oprogramowania niezbędnego do realizacji zadań. W 16 z 17 urzędów (94%) komórki informatyczne weryfikowały zgłoszone przez poszczególne komórki organizacyjne zapotrzebowania, pod kątem m.in. posiadanych zasobów, rozwiązań technicznych, ofert rynkowych, sposobów licencjonowania. Stanowiło to podstawę sporządzenia planów zakupów poszczególnych licencji/programów oraz projektów budżetów. Jedynie w Urzędzie

Marszałkowskim Województwa Podkarpackiego przed sporządzeniem planów zamówień publicznych nie weryfikowano rzeczywistego stanu posiadania licencji i oprogramowania.

Przypadki nieprawidłowości na etapie nabywania i wdrażania oprogramowania

Pomimo podjętych działań planistycznych, w toku kontroli stwierdzono, że w przypadku dziewięciu na 17 urzędów (53%) wystąpiły przypadki błędów na etapie nabywania i wdrażania oprogramowania. W pięciu podmiotach wydatkowano środki na zakup programów, które nie zostały wykorzystane lub uruchomione, a w jednej nie odnowiono usługi wsparcia dla zakupionego oprogramowania. W dwóch nabyto oprogramowania niezgodnie z obowiązującymi regułami zakupowymi w tym zakresie (pomijając zasadę centralizacji). Również w dwóch zaplanowano środki na utrzymanie niewykorzystanych elementów oprogramowania.

Przykłady

W **Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego** nie wykorzystywano dwóch wieczystych licencji F (...) dla łącznie 400 użytkowników, zakupionych 23 listopada 2021 r. za kwotę 69,2 tys. zł.

W Urzędzie Miasta Poznania przez ponad dwa lata (do 25 kwietnia 2022 r.) nie zainstalowano w Urzędzie 19 z 20 licencji oprogramowania C (...), które zostało zakupione w 2019 r. za kwotę 29,7 tys. zł na potrzeby aktualizacji starszych wersji oprogramowania użytkowanych w Urzędzie.

W **Podkarpackim Oddziale Wojewódzkim NFZ w Rzeszowie** stwierdzono jeden przypadek braku odnowienia wsparcia dla zakupionego programu. Dotyczył on oprogramowania N (...) zakupionego wraz z 2-letnim wsparciem w dniu 1 czerwca 2020 r. za kwotę 4,55 tys. zł. Po 31 maja 2022 r. tego wsparcia Oddział nie odnowił.

Efektywność wykorzystania posiadanych licencji

Kompleksowy pomiar efektywności wykorzystywanego oprogramowania, w tym oprogramowania SaaS dokonywane było w trzech[36] jst, z czego w dwóch kontrolowanych jednostkach (Urzędzie Miasta Krakowa i Urzędzie Miasta Szczecin) do pomiarów efektywności wykorzystywane było dedykowane narzędzie. W Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego w celu bieżącego pomiaru efektywności wykorzystania zasobów informatycznych wykorzystywane były wskaźniki takie jak liczba komputerów, w tym – z systemem operacyjnym w wersji starszej niż W(...)[37], oraz bieżące wykorzystanie licencji na poszczególnych stanowiskach w aplikacjach posiadających konsolę centralnego zarządzania (konsoli takiej, albo aplikacji zarządzania licencjami, nie posiadało jednak 60 używanych w Urzędzie odpłatnych aplikacji i systemów). W sześciu urzędach (Urzędzie Miasta Torunia, Urzędzie Marszałkowskim Województwa Małopolskiego, Urzędzie Miasta Tarnowa, Urzędzie Miejskim w Mielcu, Urzędzie Marszałkowskim Województwa Zachodniopomorskiego, Urzędzie Morskim w Szczecinie) pomiar efektywności dotyczył oprogramowania w modelu SaaS, przy czym jako narzędzia służyły usługi udo-

[36] W Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego, Urzędzie Miasta Krakowa i Urzędzie Miasta Szczecin.

[37] Według stanu na 6 września 2022 r. w Urzędzie używano 206 urządzeń wyposażonych w systemy operacyjne w niewspierane pod względem bezpieczeństwa. Zostały one zabezpieczone przy pomocy oprogramowania *E (...)* (wraz z modułami *L (...)* i *I (...)*), *F (...)* (z modułem *I (...)*) oraz *G (...)*. Wymiana stacji roboczych, na których zainstalowane były powyższe systemy operacyjne, planowana była na rok 2023.

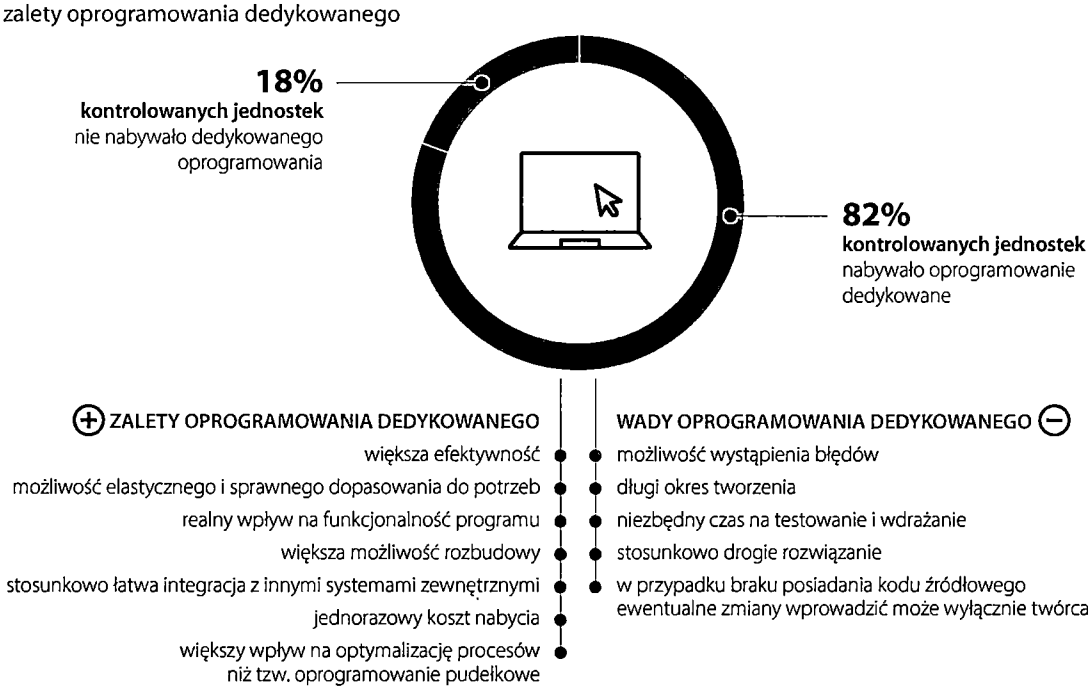
stępnione przez producentów oprogramowania (panele administratorów), a stopień wykorzystania był utożsamiany z przyznaną liczbą dostępów do danego oprogramowania. W Urzędzie Miasta Tarnowa dokonywano pomiaru efektywności wykorzystania dziedzinowego oprogramowania za pomocą prowadzonego modelu wirtualnej chmury dla Urzędu i wszystkich jego jednostek organizacyjnych, która umożliwiała wirtualny przydział i kontrolę dostępu do danych i oprogramowania.

Oprogramowanie dziedzinowe

Oprogramowanie (systemy) dziedzinowe/ZSI było użytkowane przez 16 kontrolowanych podmiotów, jednakże w przypadku Oddziałów NFZ (dwóch jednostek) zarządzającym tego typu oprogramowaniem nie były objęte kontrolą Oddziały, ale Centrala NFZ. W efekcie kontrolą w przedmiotowym zakresie objęto postępowanie 14 podmiotów (82%).

Wyniki kontroli wskazują, że 10 jst[38] (71% podmiotów nabywających ZSI) posiadało oprogramowanie dziedzinowe dedykowane zadaniom wykonywanym przez samorządy, które było wytwarzane przez dwóch producentów. Przy czym w Urzędzie Miasta Rzeszowa użytkowane były dwa oprogramowania dwóch różnych, dominujących, producentów. Systemy dziedzinowe przez cztery kontrolowane jednostki (Urząd Miasta Bydgoszczy, Urząd Miasta Krakowa, Urząd Miasta Rzeszowa oraz Urząd Miasta Poznania) zostały zakupione w latach 90-tych XX wieku (odpowiednio w latach 1995, 1993, 1994 oraz 1997). W pozostałych urzędach oprogramowanie zostało zakupione (od powyżej wskazanych dwóch producentów) na przestrzeni lat 2003–2018.

Infografika nr 7
Wady i zalety oprogramowania dedykowanego



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

[38] Tj. w: Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego, Urzędzie Miasta Bydgoszczy, Urzędzie Miasta Torunia, Urzędzie Miasta Krakowa, Urzędzie Miasta Tarnowa, Urzędzie Marszałkowski Województwa Podkarpackiego, Urzędzie Miasta Rzeszowa, Urzędzie Miejskim w Mielcu, Urzędzie Miasta Szczecin, Urzędzie Miasta Poznania.

Nieprawidłowości dotyczące systemów zintegrowanych

W sześciu na 14 jednostek (43%) stwierdzono jednak nieprawidłowości w użytkowaniu tego oprogramowania polegające m.in. na: naruszeniu przepisów ustawy pzp w zakresie stosowania trybu zamówienia z wolnej ręki, dokonywaniu opłat za niewykorzystywane moduły oprogramowania, korzystaniu z oprogramowania serwerowego bez wsparcia producenta, dokonaniu odbioru i opłaty za wadliwy moduł, zawyżeniu wysokości opłaty za obsługę oprogramowania.

Umowy na rozbudowę i/lub serwis/asystę techniczną/konserwację przez cztery urzędy (Urząd Miasta Tarnowa, Urząd Miasta Szczecin, Urząd Miejski w Koszalinie, Urząd Miasta Poznania) zostały zawarte w trybie zamówienia z wolnej ręki, w tym w dwóch przypadkach (Urząd Miasta Poznania, Urząd Miasta Szczecin) z naruszeniem przesłanek do stosowania tego trybu. Zamawiający nie wykazali spełnienia przesłanek udzielenia zamówienia z wolnej ręki określonych w art. 214 ust. 1 pkt 1 lit. b pzp[39] lub art. 214 ust. 1 pkt 1 lit. a i b pzp[40].

Przykłady

W **Urzędzie Miasta Poznania** w latach 2019–2022 postępowania o udzielenie zamówień publicznych na usługi serwisu i bieżącej konserwacji oraz na rozbudowę ZSI zostały przeprowadzone z naruszeniem obowiązku zapewnienia zachowania uczciwej konkurencji, a zamówienia publiczne w tym zakresie udzielane były z naruszeniem przepisów dotyczących przesłanek stosowania trybu zamówienia z wolnej ręki.

W **Urzędzie Miasta Bydgoszczy** jeden z modułów tego systemu, tj. P(...) dla Przedsiębiorców nie był wystarczająco wykorzystywany przez komórkę merytoryczną, tj.: Wydział Podatków i Opłat Lokalnych. Według umów na asystę techniczną i konserwację ww. modułu przewidziano 50% wynegocjowanej stawki podstawowej, łącznie 96 921,72 zł. Z raportu *Zestawienie pracy użytkowników w wybranych podsystemach, w okresie od 1 stycznia 2019 r. do 5 września 2022 r.* wynikało, że do tego podsystemu zalogowano się 11 razy, w tym w 2019 r. – raz, w 2020 r. – raz, w 2022 r. – dziewięć. Łączny czas pracy w tym podsystemie wynosił 4 godz. 58 min. Uprawnienia do niego posiadało siedmiu pracowników, z czego dwóm pracownikom tego wydziału, którzy zajmowali się pomocą publiczną nadano je 1 września 2022 r.

W **Urzędzie Miejskim w Mielcu** w umowie z 18 lipca 2017 r. na nabycie zintegrowanego systemu informatycznego O(...) nie określono osoby odpowiedzialnej za aktualizację serwerów, na których zainstalowano oprogramowanie dziedzinowe. Zapisy umowy nie precyzowały czy należało to do komórki Urzędu czy do outsourcera. W efekcie według biegłego, serwery *cały czas pracują pod kontrolą dystrybucji L(...), która już dawno utraciła wsparcie.*

Aż w 10[41] na 14 jednostek (71%) stwierdzono również brak zapewnienia możliwości rozbudowy i utrzymania systemów we własnym zakresie (bez ingerencji ich twórcy) z uwagi na uzależnienie się zamawiającego

[39] Do 31 grudnia 2020 r. podstawą udzielania zamówień z wolnej ręki w Urzędzie Miasta Poznania był art. 67 ust. 1 pkt 1 lit. b ustawy z 29 stycznia 2004 r.

[40] W odniesieniu do zamówień udzielanych przez Urząd Miasta Szczecin.

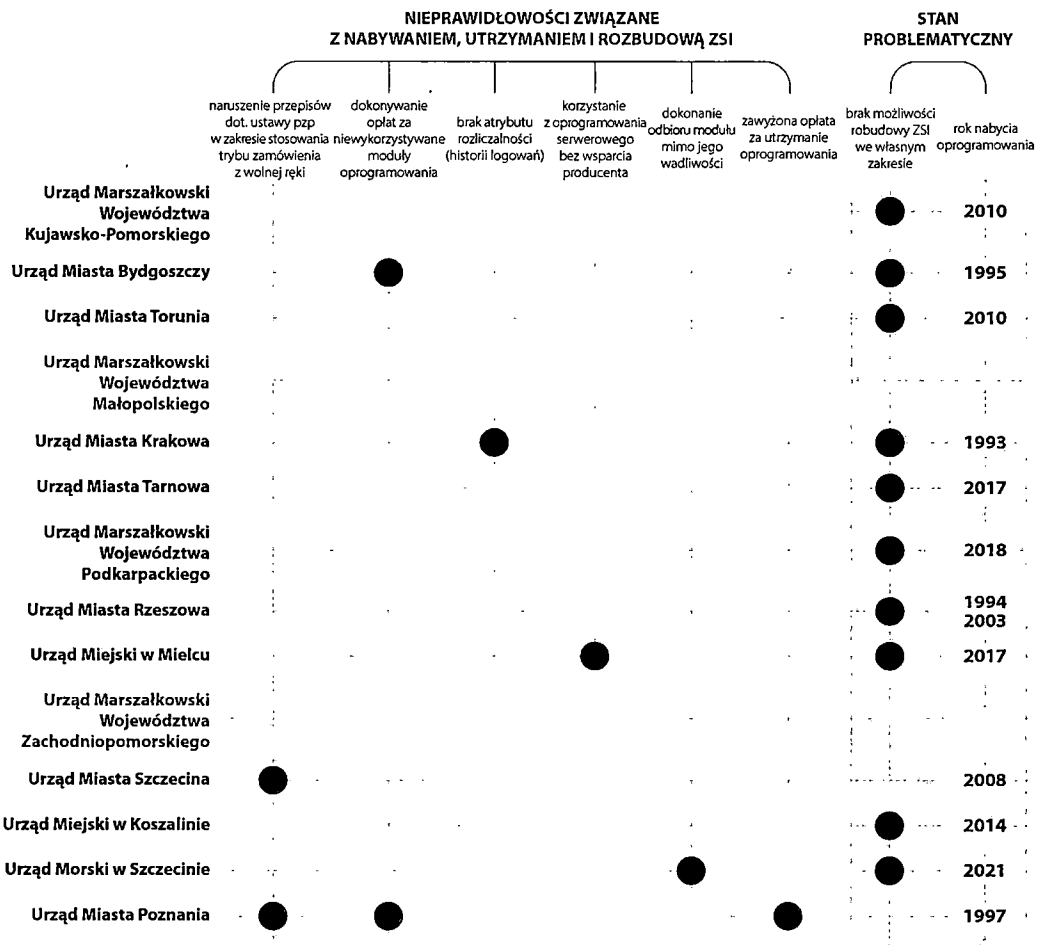
[41] Urząd Marszałkowski Województwa Kujawsko-Pomorskiego, Urząd Miasta Bydgoszczy, Urząd Miasta Torunia, Urząd Marszałkowski Województwa Małopolskiego, Urząd Miasta Krakowa, Urząd Marszałkowski Województwa Podkarpackiego, Urząd Miasta Rzeszowa, Urząd Miejski w Mielcu, Urząd Marszałkowski Województwa Zachodniopomorskiego, Urząd Miejski w Koszalinie.

od produktów lub usług dostawcy w sposób, który uniemożliwia zmianę tego dostawcy bez poniesienia dodatkowych kosztów lub znacznych niedogodności po stronie zamawiającego. Zważywszy, że były to programy użytkowane i rozbudowywane nawet od trzydziestu lat realny staje się problem uzależnienia się podmiotów publicznych od jednego producenta kluczowego, drogiego oprogramowania.

Przykład

W **Urzędzie Miasta Bydgoszczy** dostawca systemu nie udostępnił zamawiającemu kodów źródłowych umożliwiających rozbudowę tego systemu, a także jego utrzymanie w sposób niezależny od wykonawcy. 15 lipca 2019 r. powołano w Urzędzie Zespół ds. przygotowania wymagań dla zintegrowanego systemu informatycznego (ZSI) – etap I – sprawozdawczość i ewidencja księgowa[42]. Powołany zespół nie wypracował ostatecznych rekomendacji celem przedstawienia ich Prezydentowi. Jak wskazał Dyrektor WI, *doświadczenie zdobyte przez inne samorządy pokazały, że przygotowanie szczegółowego opisu zamówienia przy obecnym składzie osobowym Zespołu Merytorycznego jest niewykonalne, gdyż powołany do tego zespół musiałby wiele miesięcy poświęcić się jedynie temu zadaniu.*

Infografika nr 8
Użytkowanie zintegrowanych systemów informatycznych



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

[42] Zarządzenie nr 497/2019 Prezydenta Miasta Bydgoszczy z dnia 15 lipca 2019 r. w sprawie powołania i zasad działania Zespołu ds. przygotowania wymagań dla zintegrowanego systemu informatycznego (ZSI) – etap I – sprawozdawczość i ewidencja księgowa.

Oprogramowanie SaaS

Praktycznie we wszystkich jednostkach nabywających i użytkujących oprogramowanie w modelu SaaS nie zostały określone zasady nabywania tego rodzaju oprogramowania (14 z 15, tj. 93%). W trakcie kontroli NIK, w przypadku sześciu z 15 podmiotów (40%) nie potwierdzono także, że w procesie pozyskiwania tego oprogramowania dokonywana była każdorazowo kompleksowa ocena i weryfikacja spełniania wymagań organizacji, w tym, m.in.:

- wiarygodności dostawcy, również pod kątem zapewnienia przez dostawcę wsparcia technicznego (serwisu w wymaganym przez podmiot czasie) i bezpieczeństwa;
- dostępności SLA;
- spełniania wymagań związanych z zarządzaniem danymi (śledzenie zmian na poziomie rekordów bazy danych);
- zapewnienia możliwości eksportu danych w popularnych formatach, zasady rozdzielania danych (*multi-tenancy*);
- zapewnienia szyfrowania data-in-transit w oparciu o bezpieczne protokoły i algorytmy, polityki kopii zapasowych, w tym częstotliwości wykonywania kopii i okresu retencji oraz przechowywania;
- spełniania wymagań kontroli dostępu, itp.

W pozostałych urzędach, w których korzystano z oprogramowania SaaS, ocena wyboru najkorzystniejszych rozwiązań, w tym pod kątem bezpieczeństwa i poufności danych, wiarygodności dostawcy, zapewnienia wsparcia technicznego dokonywana była w trakcie procesu zakupowego (w opisie przedmiotu zamówienia), a brak szczegółowej weryfikacji wynikał z przedłużania korzystania z licencji znanych jednostce, wykorzystywanych od wielu lat (bez niekorzystnych incydentów). Dobre praktyki dotyczące efektywności korzystania ze środowiska wirtualnego stwierdzono w jednym z podmiotów, który utrzymywał model wirtualnej chmury dla urzędu i wszystkich jego jednostek, umożliwiający wirtualny przydział i kontrolę dostępu do danych i oprogramowania[43]. Brak szczegółowej weryfikacji oprogramowania SaaS przed jego nabyciem, jak wskazali w toku kontroli biegli, może powodować utratę ciągłości usług, w tym usług wsparcia technicznego i bezpieczeństwa, utratę ciągłości działalności, naruszenie przepisów prawa (np. ochrony danych osobowych).

Warto nadmienić, że połowa ankietowanych wskazała, że nie wdrożyła procedur nabywania oprogramowania, w tym w modelu SaaS, natomiast te które deklarowały ich wdrożenie (15,1%) nie ujęły w zasadach elementów wskazanych w tym procesie – przez powołanego w toku kontroli biegłego – jako niezbędne. Pozostałych 35% ankietowanych deklarowało, że nie korzysta z tego rodzaju oprogramowania. Oznacza to, że spośród faktyczne korzystających z oprogramowania SaaS, 23,1% wprowadziło pewne zasady jego nabywania, niemniej jednak nie w pełnym zakresie, gwarantującym nabycie oprogramowania spełniającego wymogi podmiotu.

[43] Urząd Miasta Tarnowa.

Przykład

W **Urzędzie Miasta Torunia** badanie sześciu[44] wybranych programów[45] SaaS wykazało, że w Urzędzie przed zakupem:

- każdorazowo dokonywano oceny procesu nabycia oprogramowania, uwzględniającej wiarygodność dostawcy pod kątem zapewnienia ciągłości usługi oraz zapewnienia wsparcia technicznego i bezpieczeństwa;
- weryfikowano dostępność umowy SLA, a także oceniano, że umowa ta była korzystna dla jednostki;
- weryfikowano projekty umów, zapewniając w ten sposób m.in. możliwość wcześniejszego powiadomienia o pracach serwisowych, zgłaszania błędów aplikacji.

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

Wydatki na zakup i utrzymanie licencji i oprogramowania

Jedynie w Małopolskim Oddziale Wojewódzkim NFZ w Krakowie nie korzystano z oprogramowania chmurowego.

W analizowanym okresie wydatki na zakup i utrzymanie oprogramowania[46] w poszczególnych jednostkach wyniosły:

- Urzędzie Marszałkowskim Województwa Kujawsko-Pomorskiego – 6428,10 tys. zł[47],
- Urzędzie Miasta Bydgoszczy – 19 896,40 tys. zł,
- Urzędzie Miasta Torunia – 6142,50 tys. zł,
- Kujawsko-Pomorskim Urzędzie Wojewódzkim w Bydgoszczy – 2411,10 tys. zł,
- Urzędzie Marszałkowskim Województwa Małopolskiego – 44 483,20 tys. zł,
- Urzędzie Miasta Krakowa – 74 534,20 tys. zł,
- Urzędzie Miasta Tarnowa – 6312,70 tys. zł,
- Małopolskim Oddziale Wojewódzkim NFZ w Krakowie – 4186,60 tys. zł,
- Urzędzie Marszałkowskim Województwa Podkarpackiego – 19 094,30 tys. zł,
- Urzędzie Miasta Rzeszowa – 13 998,10 tys. zł,
- Urzędzie Miejski w Mielcu – 2441,30 tys. zł,
- Podkarpackim Oddziale NFZ w Rzeszowie – 1311,40 tys. zł,
- Urzędzie Marszałkowskim Województwa Zachodniopomorskiego – 5162,00 tys. zł,
- Urzędzie Miasta Szczecina – 12 578,2 tys. zł,
- Urzędzie Miejskim w Koszalinie – 7073,60 tys. zł,
- Urzędzie Morski w Szczecinie – 4801,30 tys. zł,
- Urzędzie Miasta Poznania – 19 988,00 tys. zł.

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

[45] System informacji prawnej, dostęp do internetowej platformy informatycznej, system do zarządzania stroną podmiotową BIP, dostęp do systemu kalkulatorów.

[46] Bez wydatków obejmujących zakupione urządzenia wraz z oprogramowaniem.

[47] W tym przypadku wydatki do 16 sierpnia 2022 r.

5.3. Zapewnienie, użytkowanie i monitorowanie oprogramowania w ramach programów i projektów informatycznych zarządzanych przez Ministerstwo Finansów

W latach 2019–2022 Minister podejmował działania dotyczące zapewnienia, monitorowania i prawidłowego użytkowania oprogramowania w ramach programów i projektów informatycznych zarządzanych przez Ministerstwo Finansów, jednak realizacja powyższych zadań nie była w pełni skuteczna. Nie zapewniono w pełni skutecznego nadzoru nad Centrum Informatyki Resortu Finansów i Aplikacje Krytyczne sp. z o.o., w zakresie w jakim podmioty te zajmowały się wytwarzaniem, utrzymaniem lub unowocześnianiem oprogramowania na potrzeby Ministerstwa i pozostałych jednostek resortu finansów. Do czasu zakończenia kontroli NIK nie wyegzekwowano od CIRF wykonania działań naprawczych dotyczących zidentyfikowanych problemów w zakresie poprawy terminowości usług i obniżenia stopnia występowania awarii, a także stopnia realizacji umów z dostawcami zewnętrznymi. Nie zapewniono także faktycznego przejęcia przez CIRF wszystkich praw i obowiązków wynikających ze stosunków prawnych, w tym umów i porozumień dotyczących zamówień teleinformatycznych. Ponadto, nie opracowano i nie wdrożono w resorcie finansów katalogu oprogramowania dopuszczonego i niedopuszczonego. Nie zostało także zapewnione stosowanie przez AKMF, w ramach działalności związanej z budową, rozbudową lub unowocześnianiem systemów lub rozwiązań teleinformatycznych na rzecz Ministerstwa, zasad bezpieczeństwa teleinformatycznego o standardzie nie niższym, od obowiązującego w Ministerstwie i jednostkach resortu finansów.

5.3.1. Ministerstwo Finansów

Organizacja obsługi informatycznej resortu finansów

W resorcie finansów zadania informatyczne były realizowane przez Ministerstwo, CIRF, AKMF, a także – na podstawie umów – przez podmioty zewnętrzne. Zapewniono funkcjonowanie zespołów i rad, których zadania polegały, m.in. na: zarządzaniu grupą programów i projektów, zarządzaniu sprzętem komputerowym i licencjami, prowadzeniu centralnej analizy wydatków informatycznych, czy też proponowaniu strategicznych kierunków informatyzacji resortu finansów. Powołano także Pełnomocnika Ministra do spraw informatyzacji.

Stan realizacji projektów informatycznych

W latach 2019–2022 Ministerstwo Finansów zarządzało 118 projektami informatycznymi[48], o których mowa w zarządzeniu Ministra Finansów z dnia 28 grudnia 2018 r. w sprawie zarządzania portfelem programów i projektów w działach administracji rządowej: budżet, finanse publiczne, instytucje finansowe[49]. Ze 118 projektów 58 zakończyło się[50] w latach

[48] Liczba uwzględnia projekty rozpoczęte, trwające i zakończone w latach 2019–2022.

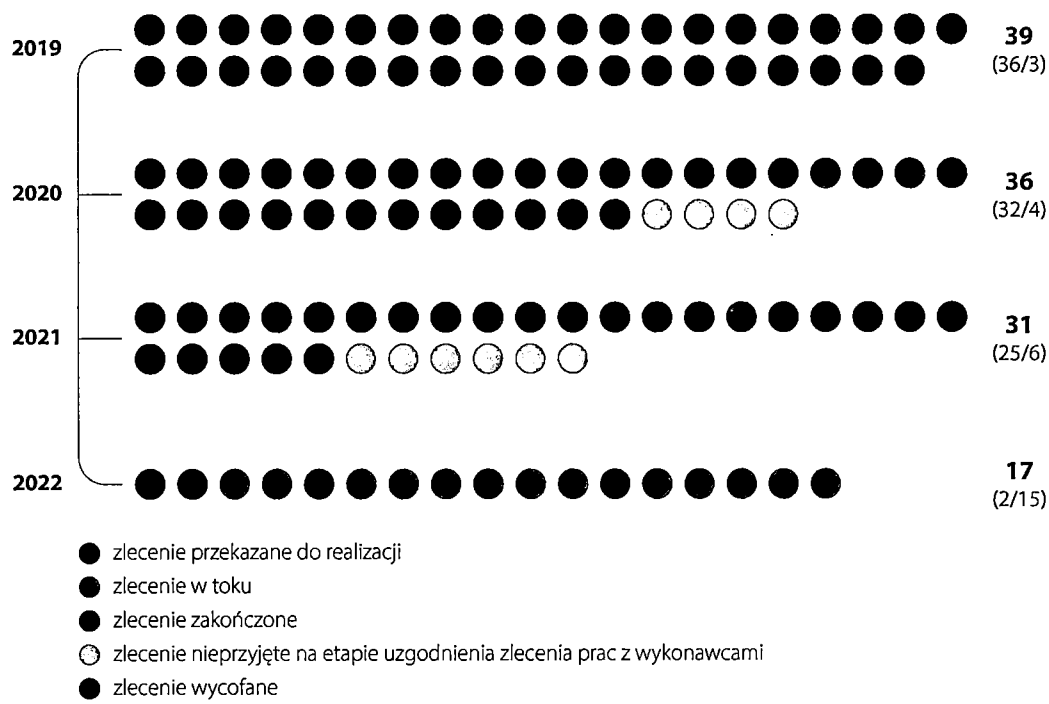
[49] Dz. Urz. MFFiPR z 2020 r. poz. 25 ze zm., dalej: zarządzenie w sprawie zarzadzania portfelem programów i projektów. Zarządzenie z grudnia 2018 r. zastąpiło zarządzenie o takiej samej nazwie z 25 maja 2017 r. (Dz. Urz. MRiF z 2017 r. poz. 108, ze zm.).

[50] Zamknięcie projektu odbywa się zgodnie z terminem wyznaczonym w Karcie Projektu lub w ostatnim zatwierdzonym wniosku o zmianę w projekcie.

2019–2022[51], 42 były nadal w toku, a 18 kolejnych było w fazie planowania, uruchamiania lub zamykania. Źródłem finansowania realizowanych projektów były środki europejskie (13 projektów)[52], Krajowy Fundusz Drogowy (dwa) oraz środki z budżetu państwa (98)[53]. Dostawcami 81 ze 106 (76%) projektów były: spółka celowa oraz CIRF. W przypadku pozostałych 24 – dostawcami były podmioty zewnętrzne. Część prac związanych z wytworzeniem oprogramowania była realizowana poza formułą projektową, w ramach bieżących działań komórek i jednostek organizacyjnych lub w formie zleceń prac spółce celowej, które z punktu widzenia spółki traktowane były jako projekty, dlatego ww. dane nie ujmowały tego zakresu prac.

W latach 2019–2022 Ministerstwo przekazało łącznie 123 wstępne zlecenia prac.

Infografika nr 9
Wstępne zlecenia prac Ministra Finansów w latach 2019–2022 (do lipca)



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

Ponadto w 2018 r. Ministerstwo złożyło 13 wstępnych zleceń pracy, które realizowano i zakończono w okresie objętym kontrolą.

Według stanu na sierpień 2022 r. w portfelu programów i projektów resortu finansów było 57 aktywnych przedsięwzięć, tj.:

– dwa programy, w których realizowanych było łącznie 21 projektów;

[51] Pięćdziesiąt cztery zakończyły się w 2019 r., po jednym w latach 2020–2021 oraz dwa w 2022 r., 12 projektów w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014–2020 oraz jeden projekt finansowany z Krajowego Funduszu Drogowego.

[52] W ramach Programu Operacyjnego Wiedza, Edukacja, Rozwój 2014–2020. Pozostałe 12 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014–2020.

[53] Odnośnie do pozostałych pięć projektów, będących w fazie planowania, nie ustalono kosztów i źródła finansowania. Liczba 103 uwzględnia także projekty zakończone.

- 12 projektów w ramach programu Platforma Usług Elektronicznych Skarbowo-Celnych (PUESC);
- dziewięć projektów w ramach programu Klient w centrum uwagi KAS (Klient KAS)
- oraz 34 projekty realizowane indywidualnie.

W okresie od 1 stycznia 2022 r. do 30 czerwca 2022 r. Ministerstwo, na podstawie 13 umów z kontrahentami zewnętrznymi (poza AKMF i CIRF), zleciło łącznie 76 zmian w oprogramowaniu podmiotom, które były autorami dotychczasowych rozwiązań informatycznych. W latach 2019–2022 Ministerstwo udzieliło 121 zamówień na dostawę oprogramowania, w tym 45 w roku 2019, 53 w roku 2020, 21 w roku 2021 i dwa w roku 2022[54].

Zakres sprawowanego nadzoru nad realizacją projektów i programów informatycznych

W okresie objętym kontrolą nadzór strategiczny nad realizacją programów i projektów wchodzących w skład portfela programów i projektów sprawował Minister. Zakres związanych z tym nadzorem działań obejmował, m.in. powoływanie i zatwierdzanie zmian w składach rad programów i komitetów sterujących projektami, a także podejmowanie decyzji w przedmiocie uruchomienia programu (projektu) oraz odstąpienia od realizacji programu (projektu). W Ministerstwie funkcjonowały zespoły i rady, których zadania polegały, m.in. na: zarządzaniu grupą programów i projektów, zarządzaniu sprzętem komputerowym i licencjami, prowadzeniu centralnej analizy wydatków informatycznych, czy też proponowaniu strategicznych kierunków informatyzacji resortu finansów.

Prace zespołu SAM

W lipcu 2018 r. w Ministerstwie utworzono Projekt SAM[55] – Centralny System Zarządzania Majątkiem IT[56], który funkcjonował do czerwca 2019 r. Prace Projektu SAM miały dostarczyć resortowi wiedzy i narzędzi niezbędnych do nowoczesnego zarządzania składnikami majątku IT, szczególnie licencjami. Utworzenie i wdrożenie CSZM IT ułatwić miało monitorowanie i kontrolę organizacji nad wykorzystaniem dostępnych składników majątku IT oraz celowością zakupu nowych. W ramach realizacji Projektu SAM zakładano udostępnienie usługi wspierającej inwentaryzację majątku IT, a następnie usługi wspierającej jego zarządzanie. Docelowo funkcjonować miała jedna usługa wspierająca zarządzanie majątkiem IT, która zapewniałaby także wspieranie jego inwentaryzacji.

Ponad pół roku później Pełnomocnik IT powołał Zespół SAM – zespół do spraw zarządzania sprzętem komputerowym, oprogramowaniem oraz licencjami w resorcie finansów[57]. Do zadań zespołu SAM przypisano, m.in.: informowanie jednostek resortu o wygaśnięciu terminu ważności licencji przez nich wykorzystywanych, przygotowywanie raportów i analiz o bieżącym stanie posiadania licencji oprogramowania w resorcie. Zespół funkcjonował do końca roku 2020 lecz nie opracowano raportu końcowego z jego prac.

---

[54] Według zestawienia przekazanego kontrolerom 26 sierpnia 2022 r.

[55] Z ang.: *Software Assets Management* (zarządzanie oprogramowaniem w organizacji).

[56] dalej: CSZM IT.

[57] Resort finansów – komórki organizacyjne MF, Krajowej Administracji Skarbowej oraz CIRF.

W maju 2020 r. Pełnomocnik IT powołał również zespół do spraw analizy wydatków informatycznych w jednostkach KAS[58]. Podstawowym zadaniem zespołu CAW była poprawa świadczenia usług informatycznych poprzez scentralizowanie i ujednolicenie procesów związanych z realizacją zadań oraz gospodarowaniem środkami przeznaczonymi na informatyzację w jednostkach KAS, w szczególności związanych z bieżącymi ich potrzebami. Powstanie zespołu CAW było kontynuacją prowadzonych w resorcie finansów prac w ramach projektu Transformacji Służb Informatycznych Resortu Finansów, którego głównym celem było uporządkowanie oraz standaryzacja systemów i procesów informatycznych.

Brak wykorzystania wypracowanych doświadczeń zespołu SAM

Nie wykorzystywano w sposób efektywny wyników działalności Projektu SAM oraz Zespołu SAM, funkcjonujących w MF w latach 2019–2020, w zakresie wypracowanych zaleceń i rozwiązań usprawniających zarządzanie oprogramowaniem w resorcie finansów. Przykładowo brak opracowania i wdrożenia katalogu oprogramowania dopuszczonego i niedopuszczonego w resorcie finansów. Potrzebę wprowadzenia takiego katalogu zgłoszono już w dokumencie[59] Zespołu SAM z maja 2020 r. oraz raporcie z prac zespołu za czwarty kwartał 2020 r.

Wydatki na nabycie licencji i oprogramowania

W latach 2019–2022 wydatki związane z nabyciem bądź wytworzeniem oprogramowania wyniosły łącznie 235 544 tys. zł na 264 zadania zakupowe. W 2019 r. wydatkowano 26 952 tys. zł na 53 zadania, w roku 2020 wydatki wyniosły 31 691 tys. zł na 73 zadania, w roku 2021 było to 126 734 tys. zł i dotyczyło 104 zadań, zaś w pierwszej połowie 2022 r. wydatki wyniosły 50 167 tys. zł na 34 zadania. Na 40 niezrealizowanych zadań (o planowanej wartości 110 603 tys. zł) w 35 przypadkach zgłoszono je do wydatków niewygasających i zrealizowano w kolejnym roku. Planowane wydatki na II półrocze 2022 r. wynosiły 38 630 tys. zł i dotyczyły 23 zadań.

Zadania CIRF

W okresie od 1 października 2017 r. do 31 grudnia 2020 r. zasadniczym zadaniem CIRF było zapewnianie usługi centralnej infrastruktury teleinformatycznej dla resortu finansów. Polegało ono, m.in. na administrowaniu i rozwijaniu, a także dostarczaniu i utrzymywaniu centralnej infrastruktury teleinformatycznej, zarządzaniu dostępnością, ciągłością i pojemnością usług infrastruktury teleinformatycznej CIRF oraz realizacją zamówień publicznych dotyczących utrzymania i rozwoju elementów centralnej infrastruktury teleinformatycznej dla resortu finansów.

Od 1 stycznia 2021 r. celem działania CIRF było zapewnianie usług informatycznych na rzecz MF i jednostek organizacyjnych podległych Ministrowi lub przez niego nadzorowanych[60], a do podstawowej

[58] Decyzja Pełnomocnika Ministra Finansów ds. informatyzacji w sprawie powołania Zespołu do sprawy analizy wydatków informatycznych w jednostkach Krajowej Administracji Skarbowej. Dalej: zespół CAW.

[59] Zarządzanie Elementami Bezpieczeństwa Zasobów IT przy pomocy Centralnego Systemu Zarządzania Majątkiem IT – Ogólna koncepcja.

[60] W tym: Krajowej Informacji Skarbowej, izbom administracji skarbowej, urzędom skarbowym, urzędom celno-skarbowym, Krajowej Szkole Skarbowości i Polskiej Agencji Nadzoru Audytowego.

działalności należało, m.in. dostarczanie i utrzymanie usług informatycznych w MF i resorcie finansów, dostarczanie, wdrażanie i utrzymywanie rozwiązań w zakresie robotyzacji i automatyzacji procesów w resorcie finansów, administrowanie i rozwijanie usług informatycznych, zapewnienie bezpieczeństwa systemów informatycznych oraz bezpieczeństwa cyberprzestrzeni w MF i resorcie finansów we współpracy z kierownikami jednostek organizacyjnych resortu finansów oraz komórką organizacyjną MF właściwą w sprawach bezpieczeństwa i ochrony informacji.

Brak przejęcia przez CIRF wszystkich praw i obowiązków

Zarządzeniem z 27 listopada 2020 r. Minister Finansów[61] nadając nowy statut CIRF zobowiązał dyrektora tej jednostki do przejęcia[62], do końca maja 2021 r., składników rzeczowych majątku ruchomego niezbędnego do wykonywania przejętych przez CIRF zadań z zakresu IT, przejęcia praw i obowiązków wynikających ze stosunków prawnych, w tym umów i porozumień dotyczących zamówień teleinformatycznych oraz ustalenia zasad współpracy w obszarach koniecznych do współdziałania w zakresie wykonywania przez CIRF odpowiednio na rzecz MF, Krajowej Informacji Skarbowej, Krajowej Szkoły Skarbowości albo izb administracji skarbowej zadań z zakresu IT. Mimo upływu 16 miesięcy od wyznaczonej daty nie sfinalizowano przejęcia przez CIRF wszystkich praw i obowiązków, o których mowa w § 2 pkt 2 zarządzenia w sprawie nadania statutu CIRF z 27 listopada 2020 r.

W związku z przejęciem przez CIRF roli podmiotu zapewniającego usługi informatyczne na rzecz MF i całego resortu do Centrum przeniesieni zostali także pracownicy resortu (np. izb administracji skarbowych) wchodzący w skład Zespołu SAM, który opracował i wdrożył Centralny System ds. Zarządzania Majątkiem IT[63]. Na system CSZM IT składały się trzy komponenty:

- SIOSK (System Inwentaryzacji Oprogramowania i Sprzętu Komputerowego), do wykrywania sprzętu i zainstalowanego na nim oprogramowania;
- SiO (Sprzęt i Oprogramowanie), wykorzystywany w 19 jednostkach resortu finansów na potrzeby wykonywania bilansów lokalnych;
- CZESiO (Centralna Zintegrowana Ewidencja Sprzętu i Oprogramowania), aplikacja użytkowa agregująca dane z 20 podmiotów resortu finansów, dostarczająca informacji statystycznych, analitycznych i detalicznych w formie raportów, umożliwiająca wspomaganie centralnego zarządzania majątkiem IT w resorcie.

---

61 Ówcześnie: Minister Finansów, Funduszy i Polityki Regionalnej.

62 W porozumieniu z Dyrektorem Generalnym MF, Dyrektorem Krajowej Informacji Skarbowej, Dyrektorem Krajowej Szkoły Skarbowości oraz dyrektorami izb administracji skarbowej.

63 Dalej: CSZM IT.

Nierzetelne i niezgodne z ustawą pzp postępowanie na zakup usługi wsparcia i rozwoju systemu

Ministerstwo nierzetelnie i niezgodnie z przepisami ustawy pzp przeprowadziło postępowanie o udzielenie zamówienia publicznego[64], którego przedmiotem był zakup usługi wsparcia i rozwoju systemu Centralny Service Desk. W efekcie w CIRF wystąpiła konieczność wydatkowania kwoty 1418,6 tys. zł za sam fakt wznowienia wsparcia w związku z opóźnieniem w zawarciu umowy.

Nie w pełni skuteczny nadzór Ministra nad AKMF i CIRF

W latach 2019–2022 Ministerstwo nie sprawowało w pełni skutecznego nadzoru nad CIRF i AKMF, w zakresie w jakim podmioty te zajmowały się wytwarzaniem, utrzymaniem lub unowocześnianiem oprogramowania na potrzeby Ministerstwa i pozostałych jednostek resortu finansów; dotyczyło to:

- niezapewnienia faktycznego przejęcia przez CIRF wszystkich praw i obowiązków wynikających ze stosunków prawnych, w tym umów i porozumień dotyczących zamówień teleinformatycznych w terminie do 31 maja 2021 r.;
- nieskutecznego egzekwowania od CIRF wykonania działań naprawczych dotyczących zidentyfikowanych problemów w zakresie poprawy terminowości usług i obniżenia stopnia występowania awarii, a także stopnia realizacji umów z dostawcami zewnętrznymi;
- przyjętego modelu zarządzania oprogramowaniem w spółce celowej, wynikającego, m.in. z braku zobowiązania spółki do stosowania zasad bezpieczeństwa teleinformatycznego, co najmniej w standardzie, jaki wynikał z polityki bezpieczeństwa teleinformatycznego stosowanej w Ministerstwie oraz jednostkach organizacyjnych resortu finansów.

5.3.2. Aplikacje Krytyczne sp. z o.o.

Cel powołania Spółki

Spółka została powołana na mocy ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne[65], w celu realizacji zadań publicznych polegających na budowie systemów lub rozwiązań teleinformatycznych, rozbudowie lub unowocześnianiu istniejących systemów lub rozwiązań teleinformatycznych, utrzymanie systemów lub rozwiązań teleinformatycznych. Powierzenie Spółce zadań określone zostało w umowie z 15 września 2016 r.[66] zawartej pomiędzy Spółką a Ministrem Finansów. Spółka również tworzyła i nabywała oprogramowanie w ramach realizowanych na rzecz MF zadań, określonych

---

[64] Krajowa Izba Odwoławcza stwierdziła naruszenie przez Zamawiającego:
- art. 24 ust. 1 pkt 12 w zw. z art. 24 ust. 4 oraz art. 24 ust. 1 pkt 16 i 17 w zw. z art. 24 ust. 4 ustawy z 29 stycznia 2004 r. poprzez zaniechanie wykluczenia z postępowania wykonawców, w związku z brakiem wykazania spełnienia warunku udziału w postępowaniu, a w konsekwencji zaniechaniu odrzucenia złożonej przez nich oferty;
- art. 89 ust. 1 pkt 4 w zw. z art. 90 ust. 2 i 3 ww. ustawy poprzez dokonanie błędnej oceny oferty złożonej przez wykonawców w zakresie wystąpienia rażąco niskiej ceny oraz złożonych przez tych wykonawców wyjaśnień, co skutkowało zaniechaniem odrzucenia złożonej przez nich oferty jako zawierającej rażąco niską cenę w zakresie Asysty Technicznej;
- art. 89 ust. 1 pkt 3 ww. ustawy poprzez zaniechanie odrzucenia oferty wykonawców ze względu na to, że jej złożenie stanowiło czyn nieuczciwej konkurencji w rozumieniu art. 3 ust. 1 ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233, ze zm.).

[65] Dz. U. z 2021 r. poz. 186.

[66] Zmienionej aneksami nr 1 z 27 kwietnia 2018 r., nr 2 z 14 września 2018 r., nr 3 z 28 czerwca 2019 r. i nr 4 z 18 listopada 2019 r.

w umowie z 2 lipca 2021 r.[67] o świadczenie usług utrzymania i modyfikacji systemu poboru opłat drogowych e-Toll. Na podstawie powyższej umowy Spółka świadczyła usługi utrzymania oraz małego rozwoju.

Skala realizowanych zleceń

W okresie objętym kontrolą Spółka realizowała 136 zleceń[68] powierzonych przez Ministra Finansów w ramach umowy z 2016 r. Według stanu na 26 lipca 2022 r., 84 zlecenia zostały zakończone, jedno posiadało status odebrane, 10 było w trakcie odbioru, 21 było w trakcie realizacji, w stosunku do 20 przygotowywana lub procesowana była analiza wstępnego zlecenia pracy (odpowiednio 14 i 6).

W wyniku badania realizacji czterech zleceń w ramach projektów: JPK_VAT_ OUT – Lunetka, Krajowy System eFaktur (KSeF), Usprawnienie pracy komórek rachunkowości w urzędach skarbowych (Witraż) oraz Podatnik Bezgotówkowy stwierdzono, że tylko zlecenie w ramach ostatniego z wymienionych projektów zostało wykonane w zakładanym terminie. W przypadku pozostałych opóźnienia w realizacji wynikały głównie ze zmian legislacyjnych czy zmian priorytetów po stronie Ministerstwa Finansów. W badanych projektach Spółka nie dokonywała zakupów licencji związanych wyłącznie z danym zleceniem. W wyjaśnieniach Zarząd Spółki podał, że zgodnie z art. 2 ust. 4 ustawy o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne, Spółka w celu budowy, rozbudowy, unowocześnienia lub utrzymania systemów lub rozwiązań teleinformatycznych nabywa urządzenia informatyczne i oprogramowanie na własny rachunek. W zdecydowanej większości koszty zakupów oprogramowania związane były ze wszystkimi realizowanymi zleceniami na rzecz Skarbu Państwa reprezentowanego przez ministra właściwego do spraw finansów publicznych, a przyporządkowanie kosztów do danego zlecenia następowało w oparciu o przyjęty rachunek kosztów.

Zarządzanie licencjami i oprogramowaniem w Spółce

W grudniu 2021 r. w Spółce wprowadzony został dokument regulujący, m.in. budżetowanie i planowanie zakupu licencji, zakup nowych licencji, obsługę wniosków o instalację oprogramowania wymagającego licencji, obsługę posiadanych licencji. W okresie poprzedzającym wprowadzenie ww. dokumentu, kwestie te były zorganizowane następująco: w 2019 roku poszczególne komórki merytoryczne planowały zakup odpowiedniego oprogramowania zgłaszając swoje zapotrzebowanie do właściwego zespołu, który ujmował planowany zakup licencji w budżecie. Proces zakupu licencji zgłaszany był przez komórki merytoryczne do działu realizującego zakupy. Zespół ten odpowiadał za aspekty techniczne, w tym instalację oprogramowania. Od 1 czerwca 2019 roku zostało utworzone stanowisko, do którego przydzielono zakres obowiązków związany z zarządzaniem aktywami IT. Stanowisko to funkcjonowało – w ramach różnych zespołów wraz ze zmianami organizacyjnymi w Spółce – do 31 sierpnia 2021 roku. Od 1 lipca 2021 roku w Spółce utworzono nowe stanowisko, w którym skoncentrowano funkcję zarządzania licencjami w jednym miej-

[67] Zmieniona aneksem nr 1 z 15 grudnia 2021 r. oraz nr 2 z 17 sierpnia 2022 r.

[68] Do 12 lipca 2022 r.

scu. Od tego czasu proces zarządzania licencjami przebiegał w sposób zbliżony do zasad zawartych w dokumencie określającym reguły zarządzania i nabywania licencji.

Niekompletne spisy licencji

Spółka prowadziła spis licencji, w tym także tzw. subskrypcji, w formie zestawienia elektronicznego. W spisie zawarte były, m.in. informacje o dacie ich wygasania, liczbie posiadanych licencji, liczbie wykorzystanych/wolnych licencji oraz dane ich użytkownika. W trakcie kontroli ustalono, że prowadzony spis nie był jednak kompletny pod względem dat wygasania licencji (dotyczyło to 11 z użytkowanych w Spółce) oraz nie zawierał wszystkich posiadanych i użytkowanych przez Spółkę licencji (dotyczyło jednej licencji).

W celu usprawnienia i zautomatyzowania procesu zarządzania licencjami, w maju 2022 r. Spółka zakupiła 400 licencji oprogramowania służącego do zarządzania infrastrukturą IT, inwentaryzacji i kontroli sprzętu komputerowego, oprogramowania oraz licencji. Zakup tego narzędzia nastąpił w modelu subskrypcyjnym na 12 miesięcy, przedłużonym we wrześniu 2022 r. do 15 miesięcy. Według stanu na 29 lipca 2022 r., zainstalowane zostały trzy licencje (co stanowiło 0,75% ogółu). Zgodnie z przyjętym harmonogramem zakończenie wdrożenia oprogramowania zaplanowane zostało na koniec września 2022 r. Według stanu na 2 września 2022 r. zainstalowanych zostało 268 licencji (67% ogółu), a na 25 października 2022 r. zainstalowano już wszystkie licencje.

Nadanie uprawnień lokalnychadministratorów zbyt szerokiemu gronu pracowników

W Spółce przyjęto rozwiązanie, zgodnie z którym uprawnienia lokalnych administratorów pozwalające na samodzielną instalację oprogramowania nadano aż 118 osobom, w tym m.in. 117 informatykom (programistom). Weryfikacja zainstalowanego oprogramowania pod względem bezpieczeństwa i warunków licencyjnych dokonywana była w przyjętym przez Spółkę, wydłużonym, przedziale czasowym. Do czasu weryfikacji i ewentualnej deinstalacji oprogramowanie znajdowało się na urządzeniach. W przypadku niespełnienia warunków licencyjnych lub bezpieczeństwa było dodawane do listy oprogramowania niedopuszczonego (tzw. czarnej listy programów niedopuszczonych do użytkowania). Według stanu na 29 lipca 2022 r. lista tego typu oprogramowania liczyła 849 pozycji. Powołany w toku kontroli NIK biegły w dziedzinie audytu systemów informatycznych, w wydanej opinii stwierdził, że przyjęte przez Spółkę rozwiązanie dopuszczające szerokiemu gronu pracowników instalację oprogramowania nieobjętego tzw. czarną listą stwarzało ryzyko wykorzystania do celów służbowych nielegalnych bibliotek lub wręcz nielegalnego oprogramowania, zwłaszcza biorąc pod uwagę liczbę pracowników posiadających uprawnienia do samodzielnego instalowania oprogramowania Działanie takie może również być przyczyną wystąpienia incydentów bezpieczeństwa informacji.

Nieobjęcie bieżącym monitoringiem wszystkich posiadanych zasobów IT

Spółka posiadała specjalistyczne narzędzie (oprogramowanie) służące m.in. do przeglądu i audytu instalowanego oprogramowania na urządzeniach końcowych (stacje robocze i laptopy). Jednak w okresie od 10 czerwca 2022 r. do 31 sierpnia 2022 r. urządzenia końcowe w zakresie instalowanych aplikacji nie były aktualizowane w tym narzędziu. Spółka

posiadała również specjalistyczne narzędzie (oprogramowanie typu MDM), służące monitorowaniu urządzeń mobilnych. Pomimo to, w toku kontroli ustalono, że nie objęto systemem stałego monitoringu 26 smartfonów (21% telefonów przekazanych użytkownikom), jednego laptopa (0,3% urządzeń przekazanych użytkownikom) i jednego urządzenia typu tablet (100% ogółu).

Planowanie środków finansowych na nabycie i utrzymanie licencji

W ramach przygotowania planów operacyjnych na lata 2019–2022, Spółka zaplanowała wysokość środków finansowych przeznaczonych na nabycie i utrzymanie licencji komputerowych (zarówno licencji zaliczanych przez Spółkę do wartości niematerialnych i prawnych[69] jak i niezaliczanych do tych wartości). Wysokość zaplanowanych środków uwzględniała m.in. zakładany wzrost zatrudnienia w Spółce oraz przewidywane do realizacji zlecenia na rzecz MF. W Spółce, według stanu na koniec 2020 r., zatrudnione były 182 osoby, a w 2021 r. – 228 osób. Planowany do osiągniecia w 2022 r. poziom zatrudnienia wynosił 300 osób. W poszczególnych latach objętych kontrolą wysokość zrealizowanych zakupów licencji odbiegała od zaplanowanych (występowały odchylenia dodatnie i ujemne), na co w szczególności wpłynęły: oferowane w postępowaniach zakupowych ceny, zwiększenie wymogów w zakresie bezpieczeństwa i związane z tym zwiększone potrzeby, wprowadzane w trakcie roku nowych inicjatyw i działań, poziom zatrudnienia w poszczególnych zespołach realizujących zadania.

Wydatki na nabycie licencji i oprogramowania

W latach 2019–2022 (I półrocze) wydatki Spółki na zakup oprogramowania oraz odnowienia licencji wyniosły odpowiednio 1889,5 tys. zł, 2688 tys. zł, 2495,6 tys. zł, 519,1 tys. zł.

[69] O wartości jednostkowej powyżej 10 tys. zł i o przewidywanym okresie ekonomicznej użyteczności powyżej jednego roku.

6. ZAŁĄCZNIKI

6.1. Metodyka kontroli i informacje dodatkowe

Dane identyfikacyjne kontroli

Kontrola nr P/22/082 Zarządzanie oprogramowaniem komputerowym przez administrację publiczną.

Pytanie definiujące cel główny kontroli

Czy jednostki administracji publicznej prawidłowo i gospodarnie zarządzały oprogramowaniem komputerowym?

Pytania definiujące cele szczegółowe kontroli

W ramach kontroli założono, że badania kontrolne umożliwią udzielenie odpowiedzi na następujące pytania szczegółowe:

1. Czy jednostki administracji publicznej podejmowały skuteczne działania w celu zapewnienia, efektywnego wykorzystania i monitorowania oprogramowania związanego z realizacją programów i projektów informatycznych?
2. Czy jednostki administracji publicznej rzetelnie zorganizowały i skutecznie realizowały proces postępowania z oprogramowaniem, a sposób użytkowania programów komputerowych był prawidłowy?
3. Czy jednostki administracji publicznej podejmowały skuteczne działania w celu optymalizacji wykorzystania oprogramowania, a środki publiczne związane z jego nabyciem i użytkowaniem były wydatkowane gospodarnie?

Zakres podmiotowy

Kontrolami (planową i doraźną) objęto łącznie 19 podmiotów administracji publicznej, w tym dwie jednostki administracji rządowej, dwanaście jednostek samorządu terytorialnego, trzy inne państwowej jednostki organizacyjne i jedną państwową osobę prawną. Jeden z ww. urzędów (jst) został objęty kontrolą doraźną I/22/002 *Gospodarowanie licencjami komputerowymi* przeprowadzoną w Urzędzie Miasta Poznania w okresie poprzedzającym kontrolę planową, tj. od 11 kwietnia 2022 r. do 8 lipca 2022 r., natomiast pozostałych 18 – kontrolą planową P/22/082 *Zarządzanie oprogramowaniem komputerowym przez administrację publiczną*. Celowy dobór podmiotów miał służyć diagnozie poszczególnych elementów procesu zarządzania oprogramowaniem, zwłaszcza gdy liczba i różnorodność aplikacji stanowić może wyzwanie pod kątem inwentaryzacji, ale także oceny funkcjonalności, jak i monitorowania efektywności ich wykorzystania.

Okres objęty kontrolą

Kontrolą objęto lata 2019–2022 do dnia zakończenia kontroli[70], z wykorzystaniem dowodów wytworzonych przed i po tym okresie, jeżeli miały one istotny wpływ dla ustaleń i ocen kontroli.

Kryteria kontroli

W podmiotach administracji rządowej, innych państwowych jednostkach organizacyjnych oraz państwowych osobach prawnych kontrolę przeprowadzono na podstawie art. 2 ust. 1 ustawy o NIK, z uwzględnieniem kryteriów: legalności, gospodarności, celowości i rzetelności. W jednostkach samorządu terytorialnego podstawą przeprowadzenia kontroli był art. 2 ust. 2 ustawy o NIK, z uwzględnieniem kryteriów: legalności, gospodarności i rzetelności.

Działania na podstawie art. 29 ustawy o NIK

W toku postępowania kontrolnego, w trybie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK, uzyskano: od 789 podmiotów administracji publicznej – w tym 695 jednostek samorządu terytorialnego, a także 94 centralnych jednostek

[70] Tj. do 16 listopada 2022 r.

administracji publicznej, informacje, w formie kwestionariusza ankiety na temat wdrożonych zasad i działań dotyczących zarządzania oprogramowaniem.

Pozostałe informacje

Czynności kontrolne przeprowadzono: w kontroli doraźnej I/22/002 w terminie od 11 kwietnia 2022 r. do 8 lipca 2022 r., natomiast w kontroli planowej P/22/082 – od 1 lipca 2022 r. do 16 listopada 2022 r. W toku ww. kontroli, w 18 z 19 jednostek (z wyjątkiem kontroli prowadzonej w Ministerstwie Finansów) powołano biegłych z dziedziny audytu systemów informatycznych. Po zakończeniu kontroli, NIK skierowała do kierowników skontrolowanych urzędów wystąpienia pokontrolne, w których sformułowała łącznie 85 wniosków pokontrolnych, w tym w ramach kontroli planowej – 76, a w ramach kontroli doraźnej – dziewięć. Z otrzymanych informacji o sposobie wykonania wniosków pokontrolnych – wg stanu na 15 marca 2023 r. – wynikało, że w ramach kontroli planowej zrealizowano 38 wniosków, 32 były w trakcie realizacji, natomiast sześć nie zostało zrealizowanych. Natomiast wnioski pokontrolne w kontroli doraźnej (dziewięć) nie zostało do ww. dnia zrealizowanych.

Wnioski pokontrolne dotyczyły przede wszystkim: określenia szczegółowych zasad zarządzania oprogramowaniem, z ustaleniem częstotliwości realizacji konkretnych czynności, wprowadzenia rozwiązań organizacyjnych i technicznych zapewniających kompletność danych o posiadanym oprogramowaniu, w tym instalowanym i wykorzystywanym na urządzeniach mobilnych; objęcie regularnym monitorowaniem całego oprogramowania, dokumentowanie podejmowanych czynności; określenie i wdrożenie szczegółowych zasad nabywania oprogramowania w modelu SaaS; odinstalowanie nieautoryzowanego oprogramowania.

Kierownicy skontrolowanych jednostek w ośmiu przypadkach zgłosili zastrzeżenia do wystąpień pokontrolnych (siedem w kontroli planowej i w kontroli doraźnej). Łącznie zgłoszone zostały 74 zastrzeżenia, w tym 59 do kontroli P/22/082 i 15 do kontroli I/22/002). W wyniku podjęcia rozstrzygnięć przez zespoły orzekające komisji rozstrzygającej 15 zastrzeżeń zostało uwzględnionych w całości (w kontroli planowej), osiem – w części (sześć w kontroli planowej i dwa w kontroli doraźnej), a 51 zostało odrzuconych (38 w kontroli planowej i 13 w kontroli doraźnej).

W wyniku kontroli ujawniono finansowe rezultaty kontroli – wg stanu na 20 marca 2023 r. – w łącznej wysokości 12 470 tys. zł. W kontroli planowej P/22/082 ujawniono kwotę 4445 tys. zł, w tym: kwoty wydatkowane z naruszeniem prawa – 1741 tys. zł, kwoty wydatkowane w następstwie działań stanowiących naruszenie prawa – 1419 tys. zł, potencjalne finansowe lub sprawozdawcze skutki nieprawidłowości – 1217,2 tys. zł, kwoty wydatkowane z naruszeniem zasad należytego zarządzania finansami – 54,3 tys. zł i sprawozdawcze skutki nieprawidłowości – 13 tys. zł. W kontroli doraźnej natomiast ujawniono kwotę 8026 tys. zł, w tym kwoty wydatkowane z naruszeniem prawa – 7943 tys. zł i kwoty wydatkowane z naruszeniem zasad należytego zarządzania finansami – 83 tys. zł.

W związku z zaniechaniem prowadzenia audytu wewnętrznego w Urzędzie Miasta Torunia, wskutek niezatrudniania audytora wewnętrznego[71] albo niezawierania umowy z usługodawcą, tj. o czyn z art. 18a ustawy z 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych[72], Najwyższa Izba Kontroli skierowała jedno zawiadomienie do rzecznika dyscypliny finansów publicznych. Ponadto, w związku z naruszeniem przepisów pzp określających przesłanki stosowania trybu zamówienia z wolnej ręki skierowane zostały cztery kolejne zawiadomienia do rzecznika dyscypliny finansów publicznych o popełnieniu czynu z art. 17 ust. 1b pkt 2 uondfp (trzy po kontroli w Urzędzie Miasta Poznania i jedno w Urzędzie Miasta Szczecin). Naruszeniem dyscypliny finansów publicznych jest udzielenie zamówienia publicznego z naruszeniem przepisów pzp dotyczących przesłanek stosowania zamówienia z wolnej ręki, zaś ww. zamawiający nie wykazali spełnienia przesłanek udzielenia zamówienia z wolnej ręki określonych w art. 214 ust. 1 pkt 1 lit. b pzp[73] lub art. 214 ust. 1 pkt 1 lit. a i b pzp[74].

Wykaz jednostek kontrolowanych

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Delegatura NIK w Bydgoszczy	Urząd Marszałkowski Województwa Kujawsko-Pomorskiego	Piotr Całbecki
2.		Urząd Miasta Bydgoszczy	Rafał Bruski
3.		Urząd Miasta Torunia	Michał Zaleski
4.		Kujawsko-Pomorski Urząd Wojewódzki w Bydgoszczy	Mikołaj Bogdanowicz
5.	Delegatura NIK w Krakowie	Urząd Marszałkowski Województwa Małopolskiego	Witold Kozłowski
6.		Urząd Miasta Krakowa	Jacek Majchrowski
7.		Urząd Miasta Tarnowa	Roman Ciepiela
8.		Małopolski Oddział Wojewódzki NFZ w Krakowie	Elżbieta Fryźlewicz-Chrapisińska

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

[72] Dz. U. z 2021 r. poz. 289, ze zm., dalej: uondfp. Naruszeniem dyscypliny finansów publicznych jest zaniechanie prowadzenia audytu wewnętrznego w jednostce sektora finansów publicznych, zgodnie z art. 274 ust. 3 ufp, wskutek niezatrudniania audytora wewnętrznego albo niezawierania umowy z usługodawcą.

[73] Do 31 grudnia 2020 r. podstawą udzielania zamówień z wolnej ręki w Urzędzie Miasta Poznania był art. 67 ust. 1 pkt 1 lit. b ustawy z 29 stycznia 2004 r.

[74] W odniesieniu do zamówień udzielanych przez Urząd Miasta Szczecin.

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
9.	Delegatura NIK w Poznaniu	Ministerstwo Finansów	Magdalena Rzeczkowska
10.		Aplikacje Krytyczne sp. z o.o.	Maciej Wardaszko
11.	Delegatura NIK w Rzeszowie	Urząd Marszałkowski Województwa Podkarpackiego	Władysław Ortyl
12.		Urząd Miasta Rzeszowa	Konrad Fijołek
13.		Urząd Miejski w Mielcu	Jacek Wiśniewski
14.		Podkarpacki Oddział NFZ w Rzeszowie	Robert Bugaj
15.	Delegatura NIK w Szczecinie	Urząd Marszałkowski Województwa Zachodniopomorskiego	Olgierd Geblewicz
16.		Urząd Miasta Szczecin	Piotr Krzystek
17.		Urząd Miejski w Koszalinie	Piotr Jedliński
18.		Urząd Morski w Szczecinie	Wojciech Zdanowicz
19.*	Delegatura NIK w Poznaniu	Urząd Miasta Poznania	Jacek Jaśkowiak

* jednostka objęta kontrolą doraźną I/22/002 *Gospodarowanie licencjami komputerowymi*

Wykaz ocen kontrolowanych jednostek[75]

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
1.	Urząd Marszałkowski Województwa Kujawsko-Pomorskiego	w formie opisowej	– prawidłowa redystrybucja licencji po zwolnieniu stanowiska; – posiadanie dowodów legalności nabytego oprogramowania; – prowadzenie pomiaru efektywności wykorzystania zasobów IT;	– brak szczegółowych zasad zarządzania oprogramowaniem; – niewystarczające wykorzystanie zakupionego oprogramowania; – brak wykonywania przeglądów oprogramowania; – brak rozwiązań technicznych umożliwiających monitorowanie urządzeń mobilnych pod kątem zainstalowanego oprogramowania; – instalowanie niedopuszczonych programów oraz aplikacji wycofanej z uwagi na luki w bezpieczeństwie; – niekompletny spis licencji i oprogramowania; – brak określenia i wdrożenia zasad nabywania SaaS;
2.	Urząd Miasta Bydgoszczy	w formie opisowej	– prawidłowa redystrybucja licencji po zwolnieniu stanowiska; – możliwość ustalenia stanu wolnego/wykorzystanego oprogramowania; – posiadanie dowodów legalności nabytego oprogramowania;	– brak szczegółowych zasad zarządzania oprogramowaniem; – niewystarczające wykorzystanie zakupionego modułu oprogramowania; – brak potwierdzenia wykonywania przeglądów oprogramowania; – brak rozwiązań technicznych umożliwiających monitorowanie urządzeń mobilnych pod kątem zainstalowanego oprogramowania; – nierzetelnie prowadzony rejestr licencji; – instalowanie aplikacji niedopuszczonych w jednostce;
3.	Urząd Miasta Torunia	negatywna	– sprawowano nadzór nad nośnikami instalacyjnymi; posiadano atrybuty legalności nabytego oprogramowania; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska; – możliwość ustalenia stanu wolnego/ niewykorzystanego oprogramowania;	– brak szczegółowych zasad zarządzania oprogramowaniem; – brak dokonywania analiz funkcjonalności i efektywności posiadanego oprogramowania; – brak kompletnej wiedzy na temat posiadanego oprogramowania; – brak regularnych przeglądów oprogramowania; – brak zatrudnienia audytora wewnętrznego; – instalacja oprogramowania typu EOL (wycofanego), wersji nieaktualnych oraz aplikacji niezwiązanych z realizacją obowiązków służbowych; – brak rozwiązań technicznych dot. monitorowania oprogramowania na urządzeniach mobilnych; – brak analiz zasadności nabycia oprogramowania;

[75] W brzmieniu pisma okólnego nr 1/2019 Prezesa Najwyższej Izby Kontroli z dnia 19 lutego 2019 r. zmieniającego pismo okólne w sprawie wzoru informacji o wynikach kontroli.

4.	Kujawsko-Pomorski Urząd Wojewódzki w Bydgoszczy	w formie opisowej	– posiadanie dowodów legalności nabytej licencji; – korzystanie z oprogramowania zgodnie z warunkami licencji; – zabezpieczenie kluczy licencyjnych; – nabywanie wyłącznie niezbędnego oprogramowania; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska;	– brak szczegółowych zasad zarządzania oprogramowaniem; – brak potwierdzenia wykonywania przeglądów oprogramowania; – brak rozwiązań technicznych umożliwiających monitorowanie urządzeń mobilnych pod kątem zainstalowanego oprogramowania; – instalowanie oprogramowania wycofanego z użycia, wymagającego aktualizacji i niezwiązanego z realizacją obowiązków służbowych; – brak kompletności danych o licencjach;
5.	Urząd Marszałkowski Województwa Małopolskiego	w formie opisowej	– rzetelnie prowadzony spis licencji; – posiadanie dowodów legalności nabytych licencji; – zabezpieczenie kluczy licencyjnych; – prowadzenie analiz potrzeb przed nabyciem oprogramowania; – możliwość ustalenia stanu wolnego/ niewykorzystywanego oprogramowania; – nabywanie wyłącznie niezbędnego oprogramowania;	– brak szczegółowych zasad zarządzania oprogramowaniem; – brak monitorowania pod kątem instalowanego oprogramowania urządzeń mobilnych; – brak potwierdzenia prowadzenia regularnych przeglądów oprogramowania;
6.	Urząd Miasta Krakowa	w formie opisowej	– wdrożenie zasad zarządzania oprogramowaniem; – kompletny rejestr posiadanych licencji; – prowadzenie analiz optymalizacji rozwiązań dot. oprogramowania; – możliwość ustalenia stanu wolnego/ niewykorzystywanego oprogramowania; – rzetelny nadzór nad dokumentacją licencyjną i nośnikami oprogramowania; – posiadanie dowodów legalności nabytych licencji;	– brak prowadzenia przeglądów oprogramowania; – instalowanie nieautoryzowanego oprogramowania; – brak wykorzystania nabytego oprogramowania; – niezapewnienie atrybutu rozliczalności trzech modułów oprogramowania;
7.	Urząd Miasta Tarnowa	negatywna	– posiadanie dowodów legalności nabytych licencji; – zabezpieczenie nośników i plików instalacyjnych; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska;	– brak szczegółowych zasad zarządzania oprogramowaniem; – brak wystarczającej obsady kadrowej przewidzianej do zadań dot. zarządzania oprogramowaniem; – brak potwierdzenia wykonywania przeglądów oprogramowania; – brak rozwiązań technicznych umożliwiających monitorowanie urządzeń mobilnych pod kątem zainstalowanego oprogramowania; – brak kompletności danych dot. licencji; – nieefektywne wykorzystanie narzędzia do monitorowania oprogramowania; – brak dokonywania weryfikacji wymogów jednostki w toku nabywania SaaS; – instalacja większej liczby oprogramowania niż wynikała z nabytej licencji; – brak analiz dot. zasadności nabywania oprogramowania;

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
8.	Małopolski Oddział Wojewódzki NFZ w Krakowie	w formie opisowej	– rzetelnie prowadzony spis licencji; – prowadzenie analiz potrzeb przed nabyciem oprogramowania; – posiadanie dowodów nabycia licencji, – zabezpieczenie kluczy licencyjnych; – instalowanie wyłącznie wykorzystywanego oprogramowania; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska; – posiadanie dowodów legalności nabytych licencji;	– brak szczegółowych zasad zarządzania oprogramowaniem; – przypadki instalowania oprogramowania bez licencji;
9.	Ministerstwo Finansów	w formie opisowej	– zapewniono funkcjonowanie odpowiednich zespołów i rad; – na bieżąco monitorowano przebieg prac związanych z realizacją zlecanych zadań informatycznych; – w 2022 r. zintensyfikowano i usystematyzowano – czynności nadzorcze nad CIRF i AKMF;	– niezapewnienie w pełni skutecznego nadzoru nad podmiotami, którym zlecano realizację zadań dot. projektów informatycznych; – nie wyegzekwowano od CIRF wykonania działań naprawczych dot. poprawy terminowości usług i obniżenia stopnia występowania awarii, a także stopnia realizacji umów z dostawcami zewnętrznymi; – nie zapewniono przejęcia przez CIRF wszystkich praw i obowiązków wynikających ze stosunków prawnych, w tym umów i porozumień dotyczących zamówień teleinformatycznych; – nie opracowano i nie wdrożono katalogu oprogramowania dopuszczonego i niedopuszczonego; – nie zapewniono stosowanie przez AKMF zasad bezpieczeństwa teleinformatycznego o standardzie nie niższym, od obowiązującego w Ministerstwie i jednostkach resortu finansów; – brak wykorzystania w sposób efektywny wyników projektów SAM (dot. zarządzania oprogramowaniem); – naruszenie przepisów ustawy pzp i w konsekwencji konieczność uregulowania tzw. wstecznego wsparcia licencji;
10.	Aplikacje Krytyczne sp. z o.o.	w formie opisowej	– do końca kontroli wdrożono narzędzie (oprogramowanie) służące, m.in. do wspierania ewidencjonowania i monitorowania stanu posiadania i użycia licencji; – każdorazowo dokonywano oceny i weryfikacji spełnienia wymagań jednostki dot. nabywanego oprogramowania; – objęte kontrolą oprogramowanie użytkowano zgodnie z warunkami licencji; – w toku kontroli nie stwierdzono przypadków użycia nielegalnego oprogramowania;	– brakiem zautomatyzowania procesu monitorowania posiadanych i użytkowanych licencji; – nieobjęcie monitoringiem wszystkich urządzeń, na których instalowane było oprogramowanie; – niekompletna ewidencja zakupionych i użytkowanych licencji; – brak stałego monitorowania części urządzeń mobilnych pod kątem legalności instalowanego i wykorzystywanego oprogramowania; – nie zapewniono bieżącej weryfikacji instalowanego oprogramowania pod kątem warunków licencyjnych oraz bezpieczeństwa;

11.	Urząd Marszałkowski Województwa Podkarpackiego	w formie opisowej	– nabywano wyłącznie niezbędne wykorzystywane oprogramowanie; – prowadzono nadzór nad dowodami legalności nabytego oprogramowania oraz kluczami licencyjnymi; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska;	– brak szczegółowych zasad zarządzania oprogramowaniem, – brak kompletności danych na temat wykorzystywanego oprogramowania; – brak monitorowanie wszystkich urządzeń, na których może być instalowane oprogramowanie; – przypadek oprogramowania bez licencji; – brak rozwiązań technicznych dot. monitorowania urządzeń mobilnych; – przypadki instalowania nieautoryzowanego oprogramowania;
12.	Urząd Miasta Rzeszowa	w formie opisowej	– nabywanie wyłącznie niezbędnego oprogramowania; – prawidłowe korzystanie z nabytego oprogramowania; – prowadzono nadzór nad dowodami legalności nabytego oprogramowania oraz kluczami licencyjnymi; – ustalono rzeczywisty stan posiadania oprogramowania i licencji; – uwzględnianie wymagań jednostki dot. SaaS w opisie przedmiotu zamówienia; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska;	– brak szczegółowych zasad zarządzania oprogramowaniem; – brak zapoznania pracowników z wewnętrznymi zasadami dot. postępowania z oprogramowaniem; – brak monitorowania urządzeń mobilnych; – przypadki instalowanie oprogramowania typu EOL (wycofanego) oraz nieaktualizowanego; – brak efektywnego wykorzystania oprogramowania;
13.	Urząd Miejski w Mielcu	w formie opisowej	– zakupione oprogramowanie użytkowano zgodnie z warunkami licencji; – posiadano dowody potwierdzające legalność kontrolowanego oprogramowania oraz klucze licencyjne; – zabezpieczono przechowywanie kluczy licencyjnych; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska;	– brak szczegółowych zasad zarządzania oprogramowaniem, – brak wykonywania przeglądów oprogramowania, w tym na urządzeniach mobilnych – brak kompletności danych na temat wykorzystywanego oprogramowania; – niewdrożenie posiadanego narzędzia do monitorowania oprogramowania; – brak określenia i wdrożenia zasad weryfikacji oprogramowania SaaS; – brak zapewnienia aktualizacji oprogramowania serwerowego;
14.	Podkarpacki Oddział NFZ w Rzeszowie	w formie opisowej	– w procesie nabywania oprogramowania uwzględniane były faktyczne potrzeby jednostki; – posiadanie dowodów legalności nabywanych licencji, – instalowanie wyłącznie wykorzystywanego oprogramowania; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska;	– brak szczegółowych zasad zarządzania oprogramowaniem, w tym nabywania oprogramowania w modelu SaaS; – brak kompletności danych na temat wykorzystywanego oprogramowania; – brak monitorowania oprogramowania – przypadki instalacji niedozwolonego oprogramowania (darmowego do użytku prywatnego oraz w wersji EOL, bez licencji, bez wsparcia); – przypadek nieodnowienia wsparcia dla oprogramowania;

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności*)	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
15.	Urząd Marszałkowski Województwa Zachodniopomorskiego	w formie opisowej	– dokonywanie weryfikacji wymagań jednostki przy nabywaniu oprogramowania, w tym SaaS; – zakupione oprogramowanie użytkowano zgodnie z warunkami licencji; – posiadano dowody potwierdzające legalność nabytego oprogramowania oraz klucze licencyjne; – posiadano wiedzę na temat liczby wolnych/ wykorzystywanych licencji;	– brak szczegółowych zasad zarządzania oprogramowaniem, w tym nabywania oprogramowania w modelu SaaS; – brak kompletności danych na temat wykorzystywanego oprogramowania; – brak monitorowania całości oprogramowania – przypadek nabycia zbyt dużej liczby instalacji danego oprogramowania; – obecność nieautoryzowanego oprogramowania;
16.	Urząd Miasta Szczecin	w formie opisowej	– rzetelnie prowadzony spis licencji; – dokonywanie zakupu wyłącznie niezbędnego i wykorzystywanego oprogramowania; – zabezpieczenie kluczy licencyjnych; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska; – posiadanie dowodów legalności nabytych licencji;	– brak szczegółowych zasad zarządzania oprogramowaniem, – brak dokonywania regularnego przeglądu oprogramowania; – przypadki programów bez licencji; – brak zasad i faktycznej weryfikacji oprogramowania w modelu SaaS; – naruszenie ustawy pzp. dot. stosowania zamówienia w trybie z wolnej ręki;
17.	Urząd Miejski w Koszalinie	w formie opisowej	– rzetelnie prowadzony spis licencji; – dokonywanie zakupu wyłącznie niezbędnego i wykorzystywanego oprogramowania; – zabezpieczenie kluczy licencyjnych; – określenie wymagań jednostki dot. SaaS w opisie przedmiotu zamówienia; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska; – posiadanie dowodów legalności nabytych licencji;	– brak szczegółowych zasad zarządzania oprogramowaniem, – brak dokonywania regularnego przeglądu oprogramowania; – brak rozwiązań organizacyjnych i technicznych do zarządzania urządzeniami mobilnymi; – instalowanie oprogramowania bez licencji;
18.	Urząd Morski w Szczecinie	w formie opisowej	– zabezpieczenie kluczy licencyjnych; – posiadanie atrybutów legalności zakupionego oprogramowania; – prowadzenie analizy stopnia wykorzystania oprogramowana, w tym SaaS; – uwzględnienie wymagań jednostki dot. SaaS w opisie przedmiotu zamówienia; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska;	– brak szczegółowych zasad zarządzania oprogramowaniem, – brak rozwiązań organizacyjnych i technicznych do zarządzania urządzeniami mobilnymi; – instalowanie nieautoryzowanego oprogramowania; – brak efektywnego wykorzystania narzędzia do monitorowania oprogramowania; – brak realizacji przeglądów oprogramowania; – brak rzetelności spisu oprogramowania; – brak analizy możliwości wykorzystania ujętych w ewidencji wartości niematerialnych i prawnych; – brak wykorzystania w całości nabytego oprogramowania; – nierzetelny odbiór modułu systemu informatycznego;

19.*[76]	Urząd Miasta Poznania	negatywna	– oprogramowanie użytkowano zgodnie z warunkami licencji; – prawidłowa redystrybucja licencji po zwolnieniu stanowiska; – posiadanie dowodów legalności nabytych licencji.	– brak szczegółowych zasad zarządzania oprogramowaniem, – brak dokonywania regularnego przeglądu oprogramowania; – brak rozwiązań organizacyjnych i technicznych do zarządzania urządzeniami mobilnymi; – brak rzetelności spisu oprogramowania; – nie zainstalowano oprogramowania bezpośrednio po nabyciu; – wydatkowanie środków na niewykorzystywane moduły oprogramowania; – naruszenie przepisów ustawy pzp. dot. trybu zamówienia z wolnej ręki; – zawyżenie wydatków na utrzymanie oprogramowania; – nie określono zasad nabywania oprogramowania w modelu SaaS.

*) pozytywna/negatywna/w formie opisowej

[76] Jednostka objęta kontrolą doraźną I/22/002 *Gospodarowanie licencjami komputerowymi*

6.2. Wyniki z badania kwestionariuszowego

Wyniki z badania kwestionariuszowego dotyczącego zarządzania oprogramowaniem komputerowym przez administrację publiczną

1. Ogólna charakterystyka badania

W celu uzyskania informacji dotyczących zarządzania oprogramowaniem komputerowym, Delegatura NIK w Poznaniu wystosowała, korzystając z uprawnień wynikających z art. 29 ust. 1 pkt 2 lit. f ustawy o NIK, zapytanie do 100 Urzędów Centralnych (UC) i 893 Jednostek Samorządu Terytorialnego (JST), zwanych dalej łącznie jednostkami. Wsparcie informatyczne i analiza danych wynikowych badania były realizowane przez Wydział Wsparcia Informatycznego i Analitycznego w Departamencie Metodyki Kontroli i Rozwoju Zawodowego NIK.

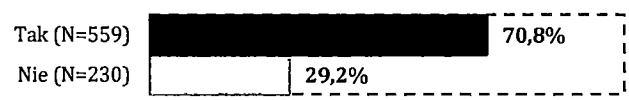
Zapytanie zostało przygotowane w postaci elektronicznego kwestionariusza i skierowane w systemie badań internetowych PS QUAESTIO PRO. Badanie było prowadzone w dniach od 12 do 28 października 2022 r.

Kwestionariusz został wypełniony przez 789 urzędów, tj. 79,5% jednostek objętych badaniem.

Rodzaj jednostki	Liczba		Odsetek odpowiedzi
	wysłanych zapytań	odpowiedzi	
Ogółem	**993**	**789**	**79,5%**
Jednostki Samorządu Terytorialnego (JST)	893	695	77,8%
Urzędy Centralne (UC)	100	94	94,0%

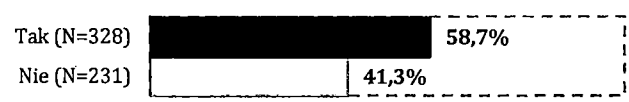
2. Zestawienie zbiorcze wyników

2.1. Czy w jednostce przeprowadza się w sposób ciągły (automatyczny) przegląd (inwentaryzację) oprogramowania obejmujący urządzenia, na których możliwe jest instalowanie i wykorzystywanie oprogramowania? *(N=789)*



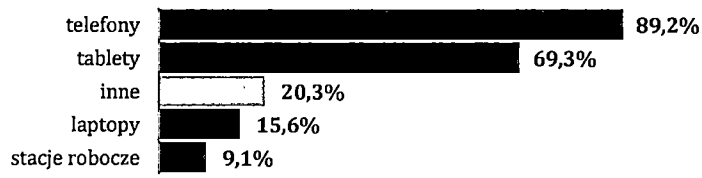
	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Tak	559	70,6%	72,3%	**70,8%**
Nie	230	29,4%	27,7%	**29,2%**

2.2. Czy przegląd obejmuje wszystkie urządzenia, na których instalowane i wykorzystywane jest oprogramowanie? *(N=559)*



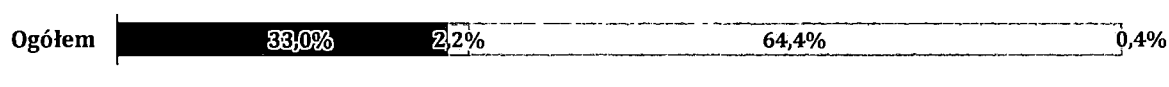
	Liczba odpowiedzi	Odsetek		
		JST (N=491)	UC (N=68)	ogółem (N=559)
Tak	328	61,7%	36,8%	58,7%
Nie	231	38,3%	63,2%	41,3%

2.3. Urządzenia, na których nie jest przeprowadzany stały przegląd oprogramowania: *(N=231)*



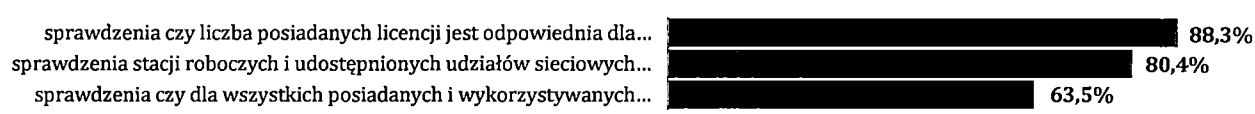
	Liczba odpowiedzi	Odsetek		
		JST (N=188)	UC (N=43)	ogółem (N=231)
stacje robocze	21	8,0%	14,0%	9,1%
tablety	160	68,6%	72,1%	69,3%
telefony	206	90,4%	83,7%	89,2%
laptopy	36	16,0%	14,0%	15,6%
inne	47	17,0%	34,9%	20,3%

2.4. Jak często przeprowadza się przegląd oprogramowania (nie w sposób ciągły)? *(N=230)*



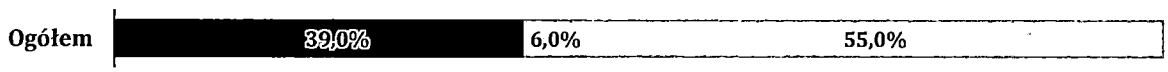
	Liczba odpowiedzi	Odsetek		
		JST (N=204)	UC (N=26)	ogółem (N=230)
Raz w roku	76	34,8%	19,2%	33,0%
Rzadziej niż raz w roku	5	2,5%	0,0%	2,2%
W miarę potrzeb	148	62,3%	80,8%	64,4%
Nie przeprowadza się żadnego przeglądu	1	0,4%	0,0%	0,4%

2.5. Realizowane (nie w sposób ciągły) przeglądy dotyczą: *(N=230)*



	Liczba odpowiedzi	Odsetek		
		JST (N=204)	UC (N=26)	ogółem (N=230)
sprawdzenia czy liczba posiadanych licencji jest odpowiednia dla zainstalowanego oprogramowania, które jest wykorzystywane na wszystkich urządzeniach	203	88,2%	88,5%	**88,3%**
sprawdzenia stacji roboczych i udostępnionych udziałów sieciowych użytkowników pod kątem obecności nieautoryzowanego oprogramowania	185	82,4%	65,4%	**80,4%**
sprawdzenia czy dla wszystkich posiadanych i wykorzystywanych licencji jednostka posiada dowody zakupu (*legalności*)	146	65,7%	46,2%	**63,5%**

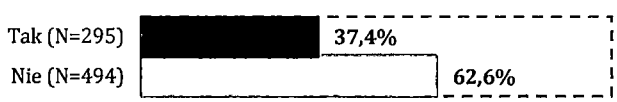
2.6. Sposób w jaki jednostka dokonuje automatycznej weryfikacji legalności oprogramowania *(N=789)*



- Za pomocą dedykowanego zakupionego narzędzia
- Za pomocą dedykowanego darmowego narzędzia
- Nie jest możliwa automatyczna weryfikacja, monitorowanie odbywa się w sposób manualny

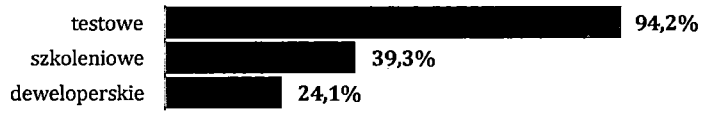
	Liczba odpowiedzi	Odsetek		
		JST (N=695)	UC (N=94)	ogółem (N=789)
Za pomocą dedykowanego zakupionego narzędzia	308	38,7%	41,5%	**39,0%**
Za pomocą dedykowanego darmowego narzędzia	47	6,3%	3,2%	**6,0%**
Nie jest możliwa automatyczna weryfikacja, monitorowanie odbywa się w sposób manualny	434	55,0%	55,3%	**55,0%**

2.7. Czy w jednostce są użytkowane inne środowiska (deweloperskie, testowe, szkoleniowe)? *(N=789)*



	Liczba odpowiedzi	Odsetek		
		JST (N=695)	UC (N=94)	ogółem (N=789)
Tak	295	30,9%	85,1%	**37,4%**
Nie	494	69,1%	14,9%	**62,6%**

2.8. Środowiska użytkowane w jednostce (poza produkcyjnym): *(N=295)*

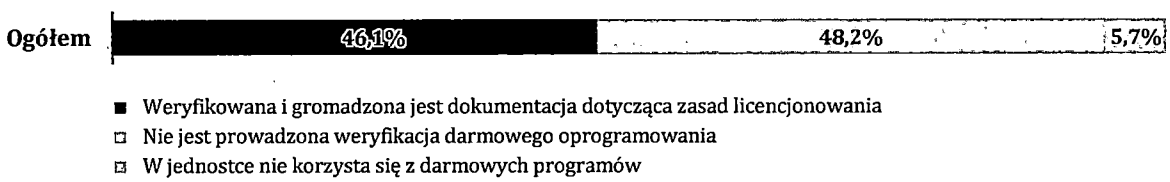


	Liczba odpowiedzi	Odsetek		
		JST *(N=215)*	UC *(N=80)*	ogółem *(N=295)*
deweloperskie	71	10,7%	60,0%	**24,1%**
testowe	278	93,5%	96,3%	**94,2%**
szkoleniowe	116	29,8%	65,0%	**93,3%**

2.9. Środowiska, w których dokonuje się przeglądu pod kątem obecności nieautoryzowanego oprogramowania: *(N=295)*

	Liczba odpowiedzi	Odsetek		
		JST *(N=215)*	UC *(N=80)*	ogółem *(N=295)*
deweloperskie	58	82,6%	81,3%	**81,7%**
testowe	240	87,6%	83,1%	**86,3%**
szkoleniowe	102	92,2%	82,7%	**87,9%**

2.10. Czy dokonywana jest weryfikacja użytkowanego darmowego oprogramowania? *(N=789)*

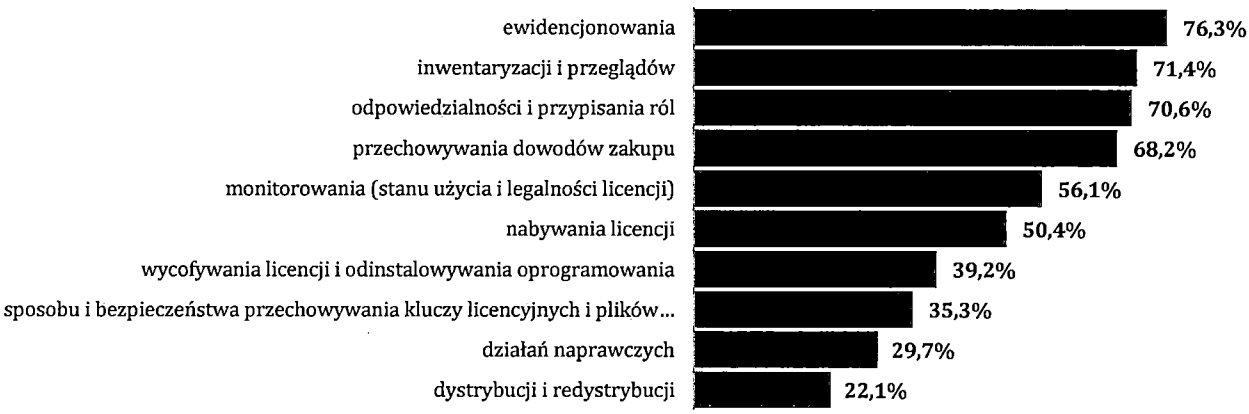


	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Weryfikowana i gromadzona jest dokumentacja dotycząca zasad licencjonowania	364	43,6%	64,9%	**46,1%**
Nie jest prowadzona weryfikacja darmowego oprogramowania	380	50,1%	34,0%	**48,2%**
W jednostce nie korzysta się z darmowych programów	45	6,3%	1,1%	**5,7%**

2.11. Czy w jednostce wdrożono procedury zarządzania oprogramowaniem? *(N=789)*

	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Tak	720	91,4%	90,4%	**91,3%**
Nie	69	8,6%	9,6%	**8,7%**

2.12. Wdrożono w jednostce procedury zarządzania oprogramowaniem obejmujące zasady: *(N=720)*

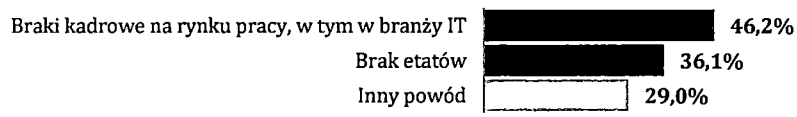


	Liczba odpowiedzi	Odsetek		
		JST *(N=635)*	UC *(N=85)*	ogółem *(N=720)*
odpowiedzialności i przypisania ról	508	69,6%	77,6%	**70,6%**
nabywania licencji	363	46,5%	80,0%	**50,4%**
wycofywania licencji i odinstalowywania oprogramowania	282	35,7%	64,7%	**39,2%**
przechowywania dowodów zakupu	491	65,2%	90,6%	**68,2%**
ewidencjonowania	549	73,5%	96,5%	**76,3%**
dystrybucji i redystrybucji	159	17,2%	58,8%	**22,1%**
inwentaryzacji i przeglądów	514	69,3%	87,1%	**71,4%**
sposobu i bezpieczeństwa przechowywania kluczy licencyjnych i plików instalacyjnych	254	33,1%	51,8%	**35,3%**
monitorowania *(stanu użycia i legalności licencji)*	404	54,2%	70,6%	**56,1%**
działań naprawczych	214	27,9%	43,5%	**29,7%**

2.13. Czy w jednostce wyznaczono pracownika (grupę pracowników) odpowiedzialnego za realizację zadań określonych w procedurach zarządzania oprogramowaniem? *(N=720)*

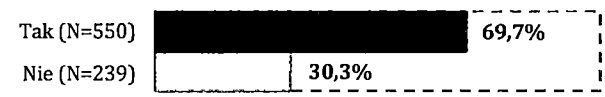
	Liczba odpowiedzi	Odsetek		
		JST *(N=635)*	UC *(N=85)*	ogółem *(N=720)*
Tak, przypisano wszystkie zadania wyznaczonemu pracownikowi/grupie pracowników	551	77,7%	68,3%	**76,5%**
Tak, przypisano część zadań wyznaczonemu pracownikowi/grupie pracowników	120	15,7%	23,5%	**16,7%**
Nie, zadania nie są formalnie przypisane	49	6,6%	8,2%	**6,8%**

2.14. Przyczyna nieprzypisania zadań *(N=169)*



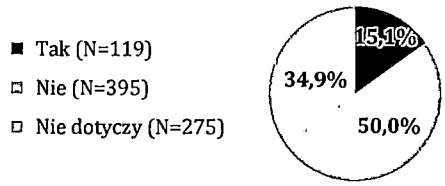
	Liczba odpowiedzi	Odsetek		
		JST *(N=142)*	UC *(N=27)*	ogółem *(N=169)*
Brak etatów	61	35,2%	40,7%	**36,1%**
Braki kadrowe na rynku pracy, w tym w branży IT	78	45,8%	48,1%	**46,2%**
Inny powód	49	25,4%	48,1%	**29,0%**

2.15. Czy zakupy oprogramowania są scentralizowane? *(N=789)*



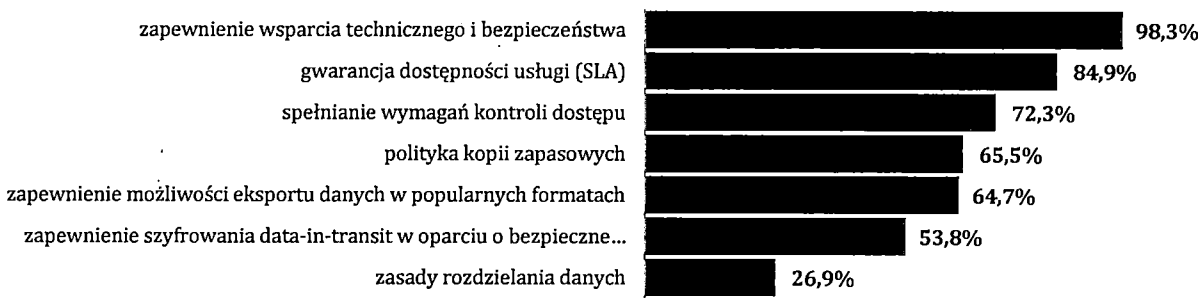
	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Tak, w dziale IT	494	62,9%	60,6%	**62,6%**
Tak, w dziale innym niż IT	56	7,1%	7,4%	**7,1%**
Nie, ale wymagana jest akceptacja działu odpowiedzialnego za zakup oprogramowania	129	15,8%	20,2%	**16,3%**
Nie, w razie potrzeby po akceptacji działu odpowiedzialnego za zakup oprogramowania	78	9,9%	9,7%	**9,9%**
Nie i nie jest wymagana akceptacja działu odpowiedzialnego za zakup oprogramowania	32	4,3%	2,1%	**4,1%**

2.16. Czy w jednostce wdrożono procedury nabywania oprogramowania, w tym w modelu Saas, obejmujące ocenę i weryfikację spełniania wymagań organizacji? *(N=789)*



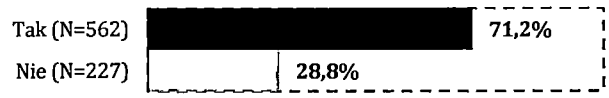
	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Tak	119	12,7%	33,0%	**15,1%**
Nie	395	50,9%	43,6%	**50,0%**
Nie dotyczy	275	36,4%	23,4%	**34,9%**

2.17. Zasady, które uwzględniono przy procedurze nabywania oprogramowania: *(N=119)*



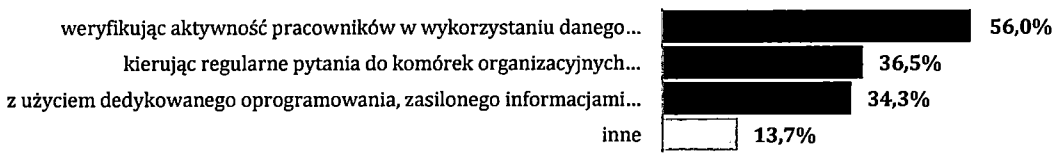
	Liczba odpowiedzi	Odsetek		
		JST *(N=88)*	UC *(N=31)*	ogółem *(N=119)*
zapewnienie wsparcia technicznego i bezpieczeństwa	117	97,7%	100,0%	**98,3%**
gwarancja dostępności usługi (SLA)	101	79,5%	100,0%	**84,9%**
zapewnienie możliwości eksportu danych w popularnych formatach	77	64,8%	64,5%	**64,7%**
zasady rozdzielania danych	32	21,6%	41,9%	**26,9%**
zapewnienie szyfrowania data-in-transit w oparciu o bezpieczne protokoły i algorytmy	64	47,7%	71,0%	**53,8%**
polityka kopii zapasowych	78	62,5%	74,2%	**65,5%**
spełnianie wymagań kontroli dostępu	86	68,2%	83,9%	**72,3%**

2.18. Czy w jednostce regularnie analizuje się faktyczne wykorzystanie danego oprogramowania, w tym rozwiązań chmurowych? *(N=789)*



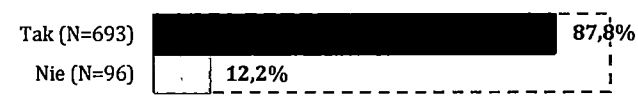
	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Tak	562	70,2%	78,7%	**71,2%**
Nie	227	29,8%	21,3%	**28,8%**

2.19. Sposób w jaki ustala się faktyczne wykorzystanie danego oprogramowania, w tym rozwiązań chmurowych: *(N=562)*



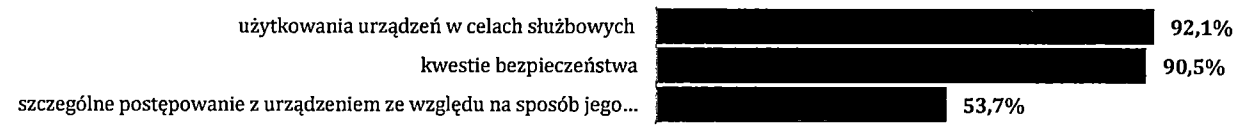
	Liczba odpowiedzi	Odsetek		
		JST *(N=488)*	UC *(N=74)*	ogółem *(N=562)*
z użyciem dedykowanego oprogramowania, zasilonego informacjami o wszystkich posiadanych licencjach	193	32,8%	44,6%	**34,3%**
weryfikując aktywność pracowników w wykorzystaniu danego oprogramowania	315	55,3%	60,8%	**56,0%**
kierując regularne pytania do komórek organizacyjnych dysponujących danym oprogramowaniem	205	37,5%	29,7%	**36,5%**
inne	77	13,1%	17,6%	**13,7%**

2.20. Czy w jednostce zdefiniowano i wdrożono zasady akceptowalnego (dopuszczalnego) użycia aktywów IT w siedzibie i poza nią? *(N=789)*



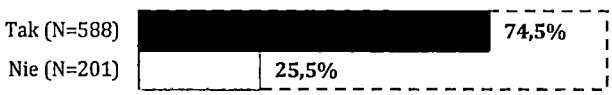
	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Tak	693	86,6%	96,8%	**87,8%**
Nie	96	13,4%	3,2%	**12,2%**

2.21. Zasady akceptowalnego (dopuszczalnego) użycia aktywów IT w siedzibie i poza nią obejmujące kwestie: *(N=693)*



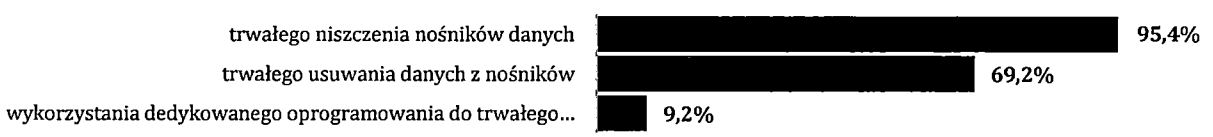
	Liczba odpowiedzi	Odsetek		
		JST *(N=602)*	UC *(N=91)*	ogółem *(N=693)*
użytkowania urządzeń w celach służbowych	638	91,5%	95,6%	**92,1%**
kwestie bezpieczeństwa	627	89,4%	97,8%	**90,5%**
szczególne postępowanie z urządzeniem ze względu na sposób jego wykorzystania	372	50,7%	73,6%	**53,7%**

2.22. Czy jednostka określiła i wdrożyła zasady zbywania sprzętu IT? *(N=789)*



	Liczba odpowiedzi	Odsetek		
		JST *(N=695)*	UC *(N=94)*	ogółem *(N=789)*
Tak	588	72,4%	90,4%	**74,5%**
Nie	201	27,6%	9,6%	**25,5%**

2.23. Zasady zbywania sprzętu IT, jakie jednostka określiła i wdrożyła: *(N=588)*



	Liczba odpowiedzi	Odsetek		
		JST *(N=503)*	UC *(N=85)*	ogółem *(N=588)*
trwałego niszczenia nośników danych	561	95,0%	97,6%	**95,4%**
trwałego usuwania danych z nośników	407	67,4%	80,0%	**69,2%**
wykorzystania dedykowanego oprogramowania do trwałego wymazywania danych z nośników i funkcji wystawiającej certyfikat, który potwierdza wymazanie danych na nośniku o danym numerze seryjnym	54	8,3%	14,1%	**9,2%**

6.3. Analiza stanu prawnego

Prawa autorskie i prawa pokrewne

Przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór) – art. 1 ust. 1 ustawy o prawie autorskim. W szczególności przedmiotem prawa autorskiego są utwory wyrażone słowem, symbolami matematycznymi, znakami graficznymi (literackie, publicystyczne, naukowe, kartograficzne oraz programy komputerowe) – art. 1 ust. 2 pkt 1 ww. ustawy. Utwór jest przedmiotem prawa autorskiego od chwili ustalenia, chociażby miał postać nieukończoną. Ochrona przysługuje twórcy niezależnie od spełnienia jakichkolwiek formalności (art. 1 ust. 2 pkt 3 i 4 ww. ustawy). Informacjami na temat zarządzania prawami autorskimi są informacje identyfikujące utwór, twórcę, podmiot praw autorskich lub informacje o warunkach eksploatacji utworu, o ile zostały one dołączone do egzemplarza utworu lub są przekazywane w związku z jego rozpowszechnianiem, w tym kody identyfikacyjne (art. 6 ust. 1 pkt 12 ustawy o prawie autorskim).

Prawo autorskie przysługuje twórcy, o ile ustawa nie stanowi inaczej (art. 8 ust. 1).

Jeżeli ustawa lub umowa o pracę nie stanowią inaczej, pracodawca, którego pracownik stworzył utwór w wyniku wykonywania obowiązków ze stosunku pracy, nabywa z chwilą przyjęcia utworu autorskie prawa majątkowe w granicach wynikających z celu umowy o pracę i zgodnego zamiaru stron (art. 12 ust. 1). Jeżeli umowa o pracę nie stanowi inaczej, z chwilą przyjęcia utworu pracodawca nabywa własność przedmiotu, na którym utwór utrwalono (art. 12 ust. 3).

Jeżeli ustawa nie stanowi inaczej, twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu (art. 17).

Jeżeli ustawa nie stanowi inaczej autorskie prawa majątkowe mogą przejść na inne osoby w drodze dziedziczenia lub na podstawie umowy. Nabywca autorskich praw majątkowych może przenieść je na inne osoby, chyba że umowa stanowi inaczej (art. 41 ust. 1 pkt 1 i 2).

Umowa o przeniesienie autorskich praw majątkowych lub umowa o korzystanie z utworu, zwana dalej *licencją*, obejmuje pola eksploatacji wyraźnie w niej wymienione. Nieważna jest umowa w części dotyczącej wszystkich utworów lub wszystkich utworów określonego rodzaju tego samego twórcy mających powstać w przyszłości. Umowa może dotyczyć tylko pól eksploatacji, które są znane w chwili jej zawarcia (ar. 43 ust. 2–4). Jeżeli z umowy nie wynika, że przeniesienie autorskich praw majątkowych lub udzielenie licencji nastąpiło nieodpłatnie, twórcy przysługuje prawo do wynagrodzenia. Jeżeli w umowie nie określono wysokości wynagrodzenia autorskiego, wysokość wynagrodzenia określa się z uwzględnieniem zakresu udzielonego prawa oraz korzyści wynikających z korzystania z utworu (art. 43 ust. 1 i 2). Jeżeli umowa nie stanowi inaczej, twórcy przysługuje odrębne wynagrodzenie za korzystanie z utworu na każdym odrębnym polu eksploatacji (art. 45).

Jeżeli w umowie nie określono sposobu korzystania z utworu, powinien on być zgodny z charakterem i przeznaczeniem utworu oraz przyjętymi zwyczajami. Następca prawny, choćby nabył całość autorskich praw majątkowych, nie może, bez zgody twórcy, czynić zmian w utworze, chyba że są one spowodowane oczywistą koniecznością, a twórca nie miałby słusznej podstawy im się sprzeciwić. Dotyczy to odpowiednio utworów, których czas ochrony autorskich praw majątkowych upłynął (art. 49 ust. 1 i 2). Umowa o przeniesienie autorskich praw majątkowych wymaga zachowania formy pisemnej pod rygorem nieważności (art. 53).

Twórca jest obowiązany dostarczyć utwór w terminie określonym w umowie, a jeżeli termin nie został oznaczony – niezwłocznie po ukończeniu utworu. Jeżeli twórca nie dostarczył utworu w przewidzianym terminie, zamawiający może wyznaczyć twórcy odpowiedni dodatkowy termin z zagrożeniem odstąpienia od umowy, a po jego bezskutecznym upływie może od umowy odstąpić (art. 54 ust. 1 i 2).

Jeżeli zamówiony utwór ma usterki, zamawiający może wyznaczyć twórcy odpowiedni termin do ich usunięcia, a po jego bezskutecznym upływie może od umowy odstąpić lub żądać odpowiedniego obniżenia umówionego wynagrodzenia, chyba że usterki są wynikiem okoliczności, za które twórca nie ponosi odpowiedzialności. Twórca zachowuje w każdym razie prawo do otrzymanej części wynagrodzenia, nie wyższej niż 25% wynagrodzenia umownego (art. 55 ust. 1). Jeżeli utwór ma wady prawne, zamawiający może od umowy odstąpić i żądać naprawienia poniesionej szkody (art. 55 ust. 2). Roszczenia, o których mowa w ust. 1, wygasają z chwilą przyjęcia utworu. Jeżeli zamawiający nie zawiadomi twórcy w terminie sześciu miesięcy od dostarczenia utworu o jego przyjęciu, nieprzyjęciu lub uzależnieniu przyjęcia od dokonania określonych zmian w wyznaczonym w tym celu odpowiednim terminie, uważa się, że utwór został przyjęty bez zastrzeżeń. Strony mogą określić inny termin (art. 55 ust. 3–4).

W braku wyraźnego postanowienia o przeniesieniu prawa, uważa się, że twórca udzielił licencji (ar. 65). Umowa licencyjna uprawnia do korzystania z utworu w okresie pięciu lat na terytorium państwa, w którym licencjobiorca ma swoją siedzibę, chyba że w umowie postanowiono inaczej. Po upływie terminu, o którym mowa w ust. 1, prawo uzyskane na podstawie umowy licencyjnej wygasa (art. 66 ust. 1–2).

Twórca może udzielić upoważnienia do korzystania z utworu na wymienionych w umowie polach eksploatacji z określeniem zakresu, miejsca i czasu tego korzystania. Jeżeli umowa nie zastrzega wyłączności korzystania z utworu w określony sposób (licencja wyłączna), udzielenie licencji nie ogranicza udzielenia przez twórcę upoważnienia innym osobom do korzystania z utworu na tym samym polu eksploatacji (licencja niewyłączna). Jeżeli umowa nie stanowi inaczej, licencjobiorca nie może upoważnić innej osoby do korzystania z utworu w zakresie uzyskanej licencji. Jeżeli umowa nie stanowi inaczej, uprawniony z licencji wyłącznej może dochodzić roszczeń z tytułu naruszenia autorskich praw majątkowych, w zakresie objętym umową licencyjną. Umowa licencyjna wyłączna wymaga zachowania formy pisemnej pod rygorem nieważności (art. 67 ust. 1–5).

Jeżeli umowa nie stanowi inaczej, a licencji udzielono na czas nieoznaczony, twórca może ją wypowiedzieć z zachowaniem terminów umownych, a w ich braku na rok naprzód, na koniec roku kalendarzowego. Licencję udzieloną na okres dłuższy niż pięć lat uważa się, po upływie tego terminu, za udzieloną na czas nieoznaczony (art. 68 ust. 1–2).

Programy komputerowe podlegają ochronie jak utwory literackie, o ile przepisy ich dotyczące nie stanowią inaczej. Ochrona przyznana programowi komputerowemu obejmuje wszystkie formy jego wyrażenia. Idee i zasady będące podstawą jakiegokolwiek elementu programu komputerowego, w tym podstawą łączy, nie podlegają ochronie. Prawa majątkowe do programu komputerowego stworzonego przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy przysługują pracodawcy, o ile umowa nie stanowi inaczej. Autorskie prawa majątkowe do programu komputerowego, z zastrzeżeniem przepisów art. 75 ust. 2 i 3, obejmują prawo do:

- trwałego lub czasowego zwielokrotnienia programu komputerowego w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie; w zakresie, w którym dla wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania programu komputerowego niezbędne jest jego zwielokrotnienie, czynności te wymagają zgody uprawnionego;
- tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym, z zachowaniem praw osoby, która tych zmian dokonała;
- rozpowszechniania, w tym użyczenia lub najmu, programu komputerowego lub jego kopii (art. 74 ust. 1–4).

Jeżeli umowa nie stanowi inaczej, czynności trwałego lub czasowego zwielokrotnienia programu komputerowego oraz tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian w programie komputerowym, o których mowa wyżej, nie wymagają zgody uprawnionego, jeżeli są niezbędne do korzystania z programu komputerowego zgodnie z jego przeznaczeniem, w tym do poprawiania błędów przez osobę, która legalnie weszła w jego posiadanie (art. 75 ust. 1). Nie wymaga zezwolenia uprawnionego:

- sporządzenie kopii zapasowej, jeżeli jest to niezbędne do korzystania z programu komputerowego. Jeżeli umowa nie stanowi inaczej, kopia ta nie może być używana równocześnie z programem komputerowym;
- obserwowanie, badanie i testowanie funkcjonowania programu komputerowego w celu poznania jego idei i zasad przez osobę posiadającą prawo korzystania z egzemplarza programu komputerowego, jeżeli, będąc do tych czynności upoważniona, dokonuje ona tego w trakcie wprowadzania, wyświetlania, stosowania, przekazywania lub przechowywania programu komputerowego;
- zwielokrotnianie kodu lub tłumaczenie jego formy, jeżeli jest to niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego z innymi programami komputerowymi, o ile zostaną spełnione następujące warunki:
    - czynności te dokonywane są przez licencjobiorcę lub inną osobę uprawnioną do korzystania z egzemplarza programu komputerowego bądź przez inną osobę działającą na ich rzecz,

- informacje niezbędne do osiągnięcia współdziałania nie były uprzednio łatwo dostępne dla licencjobiorcy lub innej osoby uprawnionej do korzystania z egzemplarza programu komputerowego bądź innej osoby działającej na ich rzecz,
- czynności te odnoszą się do tych części oryginalnego programu komputerowego, które są niezbędne do osiągnięcia współdziałania (art. 75 ust. 1–2).

Informacje, dotyczące zwielokrotniania kodu lub tłumaczenia jego formy, nie mogą być:

- wykorzystane do innych celów niż osiągnięcie współdziałania niezależnie stworzonego programu komputerowego;
- przekazane innym osobom, chyba że jest to niezbędne do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego;
- wykorzystane do rozwijania, wytwarzania lub wprowadzania do obrotu programu komputerowego o istotnie podobnej formie wyrażenia lub do innych czynności naruszających prawa autorskie (art. 75 ust. 3).

Postanowienia umów sprzeczne z ww. warunkami są nieważne (art. 76).

Uprawniony może domagać się od użytkownika programu komputerowego zniszczenia posiadanych przez niego środków technicznych (w tym programów komputerowych), których jedynym przeznaczeniem jest ułatwianie niedozwolonego usuwania lub obchodzenia technicznych zabezpieczeń programu (art. 77^1). Ochrona przyznana bazom danych spełniającym cechy utworu nie obejmuje programów komputerowych używanych do sporządzenia lub obsługi baz danych dostępnych przy pomocy środków elektronicznych (art. 77^2).

Twórca, którego autorskie prawa osobiste zostały zagrożone cudzym działaniem, może żądać zaniechania tego działania. W razie dokonanego naruszenia może także żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności aby złożyła publiczne oświadczenie o odpowiedniej treści i formie. Jeżeli naruszenie było zawinione, sąd może przyznać twórcy odpowiednią sumę pieniężną tytułem zadośćuczynienia za doznaną krzywdę lub – na żądanie twórcy – zobowiązać sprawcę, aby uiścił odpowiednią sumę pieniężną na wskazany przez twórcę cel społeczny art. 78 ust. 1).

Uprawniony, którego autorskie prawa majątkowe zostały naruszone, może żądać od osoby, która naruszyła te prawa:

- zaniechania naruszania;
- usunięcia skutków naruszenia;
- naprawienia wyrządzonej szkody:
- na zasadach ogólnych albo poprzez zapłatę sumy pieniężnej w wysokości odpowiadającej dwukrotności, a w przypadku gdy naruszenie jest zawinione – trzykrotności stosownego wynagrodzenia, które w chwili jego dochodzenia byłoby należne tytułem udzielenia przez uprawnionego zgody na korzystanie z utworu;
- wydania uzyskanych korzyści (art. 79 ust. 1).

Niezależnie od ww. roszczeń, uprawniony może się domagać jednokrotnego albo wielokrotnego ogłoszenia w prasie oświadczenia o odpowiedniej treści i formie lub podania do publicznej wiadomości części albo całości orzeczenia sądu wydanego w rozpatrywanej sprawie, w sposób i w zakresie określonym przez sąd. Sąd może nakazać osobie, która naruszyła autorskie prawa majątkowe, na jej wniosek i za zgodą uprawnionego, w przypadku gdy naruszenie jest niezawinione, zapłatę stosownej sumy pieniężnej na rzecz uprawnionego, jeżeli zaniechanie naruszania lub usunięcie skutków naruszenia byłoby dla osoby naruszającej niewspółmiernie dotkliwe. Sąd, rozstrzygając o naruszeniu prawa, może orzec na wniosek uprawnionego o bezprawnie wytworzonych przedmiotach oraz środkach i materiałach użytych do ich wytworzenia, w szczególności może orzec o ich wycofaniu z obrotu, przyznaniu uprawnionemu na poczet należnego odszkodowania lub zniszczeniu. Orzekając, sąd uwzględnia wagę naruszenia oraz interesy osób trzecich art. 79 ust. 2–4).

Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3 art. 115 ust. 1). Kto w celu osiągnięcia korzyści majątkowej w inny sposób niż ww. określony narusza cudze prawa autorskie lub prawa pokrewne podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 115 ust. 3).

Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 116 ust. 1). Jeżeli sprawca dopuszcza się ww. czynu w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3 (art. 116 ust. 2). Jeżeli sprawca czynu działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 116 ust. 4).

Kto bez uprawnienia albo wbrew jego warunkom w celu rozpowszechnienia utrwala lub zwielokrotnia cudzy utwór w wersji oryginalnej lub w postaci opracowania podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 117 ust. 1).

Odpowiedzialność karna za korzystanie z cudzego programu

Kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (art. 279 § 2 ustawy z 6 czerwca 1997 r. Kodeks karny[77]). W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 279 § 3 kk).

Ewidencja wartości niematerialnych i prawnych

Na mocy art. 3 ust. 1 pkt 14 ustawy z 29 września 1994 o rachunkowości[78] przez wartości niematerialne i prawne rozumie się nabyte przez jednostkę, zaliczane do aktywów trwałych, prawa majątkowe nadające się do gospodarczego wykorzystania, o przewidywanym okresie ekonomicznej użyteczności dłuższym niż rok, przeznaczone do używania na potrzeby jednostki. Należą do nich m.in.: licencje, koncesje, autorskie prawa majątkowe.

[77] Dz. U. z 2022 r. poz. 1138, ze zm., dalej: kodeks karny, kk.

[78] Dz. U. z 2023 r. poz. 120, dalej: ustawa o rachunkowości, uor.

Jeśli zakupiona licencja spełnia definicję wartości niematerialnej i prawnej, to od jej wartości początkowej dokonuje się odpisów amortyzacyjnych lub umorzeniowych. W myśl art. 33 ust. 1 ustawy o rachunkowości do wyceny wartości niematerialnych i prawnych oraz sposobów dokonywania od nich odpisów amortyzacyjnych lub umorzeniowych stosuje się odpowiednio przepisy art. 31 ust. 2 i art. 32 ust. 1–4 i ust. 6 ww. ustawy. Jeżeli, w ocenie jednostki, zakupiona licencja ma nieistotną wartość, to, na podstawie art. 32 ust. 6 ustawy, można dokonać jednorazowego odpisu amortyzacyjnego od jej wartości początkowej.

Szczególne zasady wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej: budżet i finanse publiczne

Ustawa z 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne określa zasady wykonywania niektórych projektów informatycznych o publicznym zastosowaniu w celu zapewnienia ministrowi właściwemu do spraw budżetu i finansów publicznych, zwanemu dalej *ministrem właściwym do spraw finansów publicznych*, oraz innym organom Krajowej Administracji Skarbowej, systemów i rozwiązań teleinformatycznych, wspierających wykrywanie naruszenia przepisów prawa podatkowego oraz wyższą efektywność poboru podatków, niepodatkowych należności budżetowych oraz opłat w oparciu o dane uzyskiwane z systemów teleinformatycznych ministra właściwego do spraw finansów publicznych oraz organów Krajowej Administracji Skarbowej oraz systemów teleinformatycznych służących do obsługi budżetu państwa, jak również obsługę procesów pomocniczych dla realizacji tych zadań (art. 1).

Ww. projekty informatyczne powierza się spółce z ograniczoną odpowiedzialnością utworzonej w tym celu przez Skarb Państwa, zwanej dalej *spółką celową*. W ramach realizacji projektów informatycznych, spółka celowa wykonuje na rzecz Skarbu Państwa reprezentowanego przez ministra właściwego do spraw finansów publicznych zadania publiczne w zakresie: budowy systemów lub rozwiązań teleinformatycznych, rozbudowy lub unowocześnienia istniejących systemów lub rozwiązań teleinformatycznych, utrzymania systemów lub rozwiązań teleinformatycznych (art. 2 ust. 1 i 2). W celu budowy, rozbudowy, unowocześnienia lub utrzymania systemów lub rozwiązań teleinformatycznych spółka celowa nabywa urządzenia informatyczne i oprogramowanie na własny rachunek (art. 2 ust. 4).

Określenie zadań spółki następuje w umowie zawartej na piśmie między ministrem właściwym do spraw finansów publicznych a spółką celową (art. 9 ust. 1). W umowie o świadczenie usług określa się w szczególności: przedmiot umowy obejmujący zadania, w tym usługi, powierzane do wykonania przez spółkę celową, sposób realizacji przez spółkę celową przedmiotu umowy, obowiązki spółki celowej, w szczególności w zakresie ochrony informacji niejawnych i innych informacji zawierających tajemnice ustawowo chronione, tryb kontroli wykonania przedmiotu umowy przez spółkę celową (art. 9 ust. 2). Spółka celowa może otrzymać dotacje celowe na finansowanie lub dofinansowanie zadań spółki (art. 10 ust. 1). W ww. przypadku określenie zadań spółki następuje w umowie (art. 10 ust. 2). Przychodami spółki celowej są m.in.: przychody z tytułu umowy

o świadczenie usług, dotacje celowe z budżetu państwa, w tym dotacje celowe na finansowanie lub dofinansowanie kosztów inwestycji, dotacje podmiotowe na dofinansowanie działalności bieżącej spółki celowej (art. 12 ust. 1).

System lub rozwiązanie teleinformatyczne zbudowane, rozbudowane lub unowocześnione w wykonaniu umowy o świadczenie usług lub umowy o dotację spółka celowa przekazuje nieodpłatnie na rzecz Skarbu Państwa reprezentowanego przez ministra właściwego do spraw finansów publicznych (art. 13 ust. 1). Szczegółowy sposób i tryb przekazania systemu lub rozwiązania teleinformatycznego, o których mowa wyżej, określa umowa zawarta na piśmie między spółką celową a Skarbem Państwa reprezentowanym przez ministra właściwego do spraw finansów publicznych art. 13 ust. 2).

Przetwarzanie danych osobowych

Dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f RODO).

Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą (ar. 28 ust.1). Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora (art. 28 ust. 3). Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym (art. 28 ust. 4).

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego (art. 29).

Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający m.in. informacje: imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot

przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych (art. 30 ust. 2 lit. a). Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (art. 32 ust. 1).

6.4. Wykaz aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57, ze zm.).
2. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509).
3. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2022 r. poz. 1138, ze zm.).
4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, ze zm.).
5. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r. poz. 1634, ze zm.).
6. Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, ze zm.).
7. Ustawa z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne (Dz. U. z 2021 r. poz. 186).
8. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L z 2016 r. Nr 1, poz. 119, ze zm.).
9. Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF z 2009 r. Nr 84, poz. 15).
10. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728).
11. Zarządzenie Ministra Finansów z dnia 28 grudnia 2018 r. w sprawie zarządzania portfelem programów i projektów w działach administracji rządowej: budżet, finanse publiczne, instytucje finansowe (Dz. Urz. MFFiPR z 2020 r. poz. 25, ze zm.).

6.5. Wykaz podmiotów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Przewodniczący Sejmowej Komisji do Spraw Kontroli Państwowej
8. Przewodniczący Sejmowej Komisji Administracji i Spraw Wewnętrznych
9. Przewodniczący Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
10. Przewodniczący Sejmowej Komisji Samorządu Terytorialnego i Polityki Regionalnej
11. Przewodniczący Senackiej Komisji Gospodarki Narodowej i Innowacyjności
12. Przewodniczący Senackiej Komisji Samorządu Terytorialnego i Administracji Państwowej
13. Minister Cyfryzacji
14. Minister Finansów
15. Prezes Urzędu Zamówień Publicznych

WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI

ul. Filtrowa 57, 02-056 Warszawa
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

P/22/082 LPO.430.1.2023

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57
02-056 Warszawa

WARSZAWA 1
30082023
OG

OPŁATA POBRANA
TAXE PERÇUE - POLOGNE
Umowa nr ID 484453/W
z Pocztą Polską S.A.

RP MINISTERSTWO FINANSÓW KASA GŁÓWNA
Wpł. 2023 -08- 04
Dep. ..... Zał. .....

list polecony + ZPO

RKW/5959/2023

Ministerstwo Finansów
ul. Świętokrzyska 12
00-916 Warszawa

Za zwrotnym potwierdzeniem odbioru

R (00)359007734519329322

2023

Poczta Polska
Opłata pobrana ____ zł ____ gr

30/