NAJWYŻSZA IZBA KONTROLI

Departament Administracji Publicznej

KAP.410.2.4.2025

Pan Roman Smogorzewski
Starosta Legionowski

Starostwo Powiatowe
w Legionowie
ul. gen. Władysława Sikorskiego 11
05-119 Legionowo

WYSTĄPIENIE POKONTROLNE

P/25/003 Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej
ul. Filtrowa 57, 02-056 Warszawa
tel. 48224445308, kap@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Legionowie[1], ul. gen Władysława Sikorskiego 11, 05-119 Legionowo
Kierownik jednostki kontrolowanej	Roman Smogorzewski, Starosta Legionowski, od 6 maja 2024 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Sylwester Sokolnicki, Starosta Legionowski, od 27 kwietnia 2020 r. do 5 maja 2024 r.
Zakres przedmiotowy kontroli	Realizacja przez Powiat Legionowski działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych, tj. 4 lipca 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Łukasz Hertel, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/56/2025 z 7 maja 2025 r.

(akta kontroli str. 1-6)

[1] Dalej: Urząd, Starostwo, Grantobiorca.
[2] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Powiat Legionowski w latach 2023 – 2025 podejmował działania na rzecz zwiększenia poziomu cyberbezpieczeństwa realizując projekt pn. *Cyberbezpieczny samorząd w Powiecie Legionowskim* (dalej: Projekt) na potrzeby Starostwa oraz jednostek podległych. W ramach Projektu m.in. przeprowadzono postępowania przetargowe oraz dokonano zakupu urządzeń i oprogramowania zwiększających odporność na cyberataki, a także prowadzono audyty z zakresu diagnozy cyberbezpieczeństwa. Ponadto, informowano opinię publiczną o otrzymaniu dofinansowania na realizację Projektu. Stwierdzone w trakcie kontroli nieprawidłowości nie miały istotnego wpływu na realizację Projektu. Grantobiorca zrealizował wszystkie zadania dotyczące Projektu i osiągnął założone wskaźniki produktu.

Uzasadnienie oceny ogólnej

W okresie objętym kontrolą w Starostwie rozpoznawano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa oraz wdrożono w tym zakresie rozwiązania organizacyjne i techniczne. W Starostwie w 2021 r. ustanowiono System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), który podlegał regularnym przeglądom. W latach 2023-2024 przeprowadzono okresowy audyt z zakresu bezpieczeństwa informacji oraz wdrażano rekomendacje w nim zawarte. W związku z przystąpieniem do Projektu wypełniono *Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego* (dalej: Ankieta) i przekazano ją do Operatora[4] z zachowaniem terminu i form określonych w umowie o powierzenie grantu[5] (dalej: umowa grantowa) zawartej 17 kwietnia 2024 r. z Centrum Projektów Polska Cyfrowa (dalej: CPPC lub Grantodawca). W ramach tej umowy przyznano Starostwu dofinansowanie na realizację Projektu w kwocie 842 399,77 zł[6] z czego ostatecznie wykorzystano 823 422,02 zł, (tj. 97,7%). Poniesione przez Grantobiorcę wydatki w zakresie zakupu przełączników sieciowych, urządzeń UTM oraz wdrożenia systemów zostały zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o powierzenie grantu.

W toku kontroli stwierdzono nieprawidłowości polegające na:

- nieterminowym przekazaniu Operatorowi informacji o postępie rzeczowym realizacji Projektu, co było niezgodne z § 7 ust. 2 umowy grantowej;
- przeprowadzeniu w Urzędzie zadania audytowego pn.: *Audyt wewnętrzny bezpieczeństwa informacji i ochrony danych osobowych w oparciu o wymagania PN ISO/IEC 27001 i RODO*[7], a także audytów SZBI oraz audytów zgodności z wymaganiami prawnymi – Diagnoza cyberbezpieczeństwa w Urzędzie oraz trzech jednostkach podległych przez osobę, która pełniła jednocześnie funkcję Inspektora Ochrony Danych (dalej: IOD) w tych jednostkach, i tym samym wystąpił konflikt interesów co naruszało art. 38 ust. 6 rozporządzenia Parlamentu

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

[4] Tj. do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

[5] Umowa nr FERC.02.02-CS.01-001/23/0923/ FERC.02.02-CS.01- 001/23/2024.

[6] Tj. w kwocie wskazanej we Wniosku o przyznanie grantu nr a2ce3a40-4f32-4e05-8502-85e7a6c31149 (dalej: Wniosek), z tego Budżet Państwa (dalej: BP) - 84 239,98 zł, Budżet środków europejskich (dalej: BŚE) – 758 159,79 zł.

[7] W latach 2023-2024.

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)[8];

- nieprzestrzeganiu niektórych obowiązków informacyjnych i promocyjnych określonych w § 11 ust. 3 umowy grantowej w zakresie stosowania oznaczania znakiem Unii Europejskiej i Funduszy Europejskich i barw Rzeczypospolitej Polskiej w publikowanych informacjach na stronie internetowej oraz oficjalnym profilu mediów społecznościowych, a także części dokumentacji projektowej.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

1. Realizacja przez Powiat Legionowski działań w celu zwiększenia poziomu cyberbezpieczeństwa.

Opis stanu faktycznego

1. *Strategia Rozwoju Powiatu Legionowskiego na lata 2016-2025*[10] (dalej: Strategia) była obowiązującym dokumentem określającym obszary działań, cele oraz kierunki interwencji polityki rozwoju prowadzonej na obszarze Powiatu Legionowskiego. W dokumencie tym wskazano cele strategiczne, operacyjne m.in. *Poprawa sprawności administracji i lepsze dostosowanie do potrzeb mieszkańców i przedsiębiorców, kompleksowa cyfryzacja urzędu i jednostek podległych wraz z wprowadzeniem elektronicznej obsługi dokumentów*, natomiast nie zawarto zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa. Sekretarz Powiatu wyjaśnił[11], że Strategia *opracowywana była w 2015 r. Na podstawie analizy ówczesnych uwarunkowań społeczno-gospodarczych, a także sytuacji geopolitycznej naszego kraju wywnioskowano, iż w tamtym czasie należało położyć szczególny nacisk na poprawę dostępności cyfrowej administracji dla klientów urzędu, w tym jednostek organizacyjnych powiatu. (...) Cyberbezpieczeństwo przed wybuchem pandemii i wojny na Ukrainie, uznane zostało w urzędzie jako wystarczające, dopiero sytuacja po roku 2020 zmieniła ten sposób rozumienia zagadnienia. (...) w ramach tworzonego aktualnie, nowego dokumentu strategicznego dla powiatu, zostaną opracowane cele strategiczne i operacyjne, dotyczące szerszego zakresu cyberbezpieczeństwa*.

(akta kontroli str. 7-108, 123-127, 134-151)

2. W identyfikacji potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa uczestniczyli m.in. Zespół ds. Informatyki, IOD oraz przedstawiciele kierownictwa Urzędu. Określono działalność Starostwa w celu zapewnienia bezpieczeństwa informacji zarówno wewnątrz Urzędu, jak

---

[8] Dz. Urz. UE.L 119 z 04.05.2016, str. 1, ze zm. dalej: RODO.

[9] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

[10] Przyjęta Uchwałą nr 98/XV/16 Rady Powiatu w Legionowie z dnia 26 lutego 2016 r. W dniu 9 kwietnia 2020 r. Uchwałą Nr 134/XVI/2020 dokonano aktualizacji Strategii. W następnych latach dokument nie był aktualizowany.

[11] Na podstawie Upoważnienia (znak: WAK.077.66.2025) z dnia 21 maja 2025 r. udzielonego przez Starostę Legionowskiego.

i w kontaktach z innymi instytucjami i otoczeniem. Ponadto Sekretarz Powiatu wskazał że rozpoznawanie potrzeb dotyczących cyberbezpieczeństwa odbywa się m.in. poprzez: *Coroczne wykonywanie Audytów bezpieczeństwa wraz z przeprowadzaniem testów penetracyjnych (...), analizę potrzeb w zakresie inwestycji i zakupów (...), ciągłe monitorowanie infrastruktury teleinformatycznej (...)*.

(akta kontroli str. 134-151)

3. Zgodnie z § 4 ust. 1 pkt 4 umowy grantowej w terminie 30 dni od dnia jej zawarcia, Starostwo przekazało do Operatora za pośrednictwem skrzynki ePUAP Ankietę.

(akta kontroli str. 109-127, DVD-1 pliki: 010-018)

4. Projekt *Cyberbezpieczny samorząd w Powiecie Legionowskim* był realizowany w ramach programu Fundusze Europejskie na Rozwój Cyfrowy (dalej: FERC), Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa. Powierzenie grantu nastąpiło na podstawie umowy grantowej, której przedmiotem było przyznanie Grantobiorcy dofinansowania na realizację Projektu w kwocie 842 399,77 zł. Ostatecznie wykorzystano 823 422,02 zł, tj. 97,7%, w związku z oszczędnościami wynikającymi z różnic pomiędzy szacowaniem wartości zamówienia a ostatecznym kosztem zrealizowanego zamówienia. W dniu 27 grudnia 2024 r. Starostwo dokonało zwrotu niewykorzystanych środków w kwocie: BP – 1897,77 zł, BŚE – 17 079,98 zł. Sekretarz Powiatu wskazał, że *Obecnie trwa etap kompleksowego przygotowania dokumentacji niezbędnej do złożenia wniosku rozliczającego grant. Równolegle prowadzona jest szczegółowa weryfikacja kompletności i poprawności dokumentacji merytorycznej oraz finansowej dotyczącej zrealizowanych zadań projektowych. (...)* Zgodnie z postanowieniami § 3 ust. 1 umowy grantowej termin na złożenie Wniosku o rozliczenie grantu przypada na 17 kwietnia 2026 r.

(akta kontroli str. 123-127, 134-151, 164-173, DVD-1 pliki: 010-018)

Głównym celem Projektu, jak wskazano we Wniosku o dofinansowanie, było zabezpieczenie integralności, dostępności i niezaprzeczalności przetwarzanych danych w systemach teleinformatycznych Starostwa oraz czterech jednostek podległych[12] na poziomie odpowiadającym współczesnym potrzebom i zagrożeniom oraz wymaganiom prawnym. Realizacja projektu została podzielona na trzy zadania, tj.:

- Zadanie 1 – polegało na: wymianie przełączników sieciowych na urządzenia najnowszej generacji, posiadające wsparcie producenta na odpowiednim poziomie funkcjonalności, gwarancji oraz kompatybilności z innymi systemami, wdrożeniu systemu NAC[13], wymianie urządzeń służących do analizy ruchu na styku sieci LAN/WAN;

[12] Tj. Liceum Ogólnokształcącego im. Marii Konopnickiej w Legionowie, Liceum Ogólnokształcącego im. Stanisława Lema w Stanisławowie Pierwszym, Domu Pomocy Społecznej Kombatant w Legionowie, Poradni Psychologiczno-Pedagogicznej w Legionowie.

[13] System NAC (Network Access Control) to rozwiązanie bezpieczeństwa, które kontroluje dostęp do sieci, zapewniając, że tylko autoryzowani użytkownicy i urządzenia mogą się do niej dostać.

- Zadanie 2 – polegało na zakupie urządzeń UTM[14] do czterech jednostek organizacyjnych Powiatu;
- Zadanie 3 – polegało na przeprowadzeniu audytu z zakresu diagnozy cyberbezpieczeństwa w pięciu jednostkach (Starostwie i w czterech jednostkach, dla których przewidziano zakup urządzeń UTM).

(akta kontroli: DVD-1 pliki: 010-018)

W dniu 31 lipca 2024 r. Starosta Powiatu Legionowskiego zwrócił się do CPPC z wnioskiem o wyrażenie zgody na przekazanie środków w ramach Projektu w jednej transzy w wysokości 100% grantu, argumentując m.in. *że otrzymanie pełnej kwoty grantu w jednej transzy pozwoli na sprawne i terminowe wdrożenie zaplanowanych działań, a realizacja projektu będzie mogła odbywać się w sposób płynny*. W dniu 14 sierpnia CPPC przekazało informację o pozytywnym rozpatrzeniu wniosku i 5 września 2024 r. przekazano środki.
Starostwo w dniu 19 sierpnia 2024 r. wszczęło postępowanie[15] na *Dostawę urządzeń i oprogramowania zwiększających odporność na cyberataki wraz z wdrożeniem w ramach realizacji projektu grantowego Cyberbezpieczny samorząd w Powiecie Legionowskim,* w wyniku którego 19 września 2024 r. zawarto Umowę na podstawie której dokonano zakupów[16] na potrzeby:

- Starostwa – dwa przełączniki sieciowe typ I, 14 przełączników sieciowych typ II, jeden System NAC, jeden System SIEM[17], jeden system analizy ruchu sieci Fortianalyzer[18], łącznie na kwotę: BŚE – 639 576,78 zł, BP – 71 064,08 zł, wkład własny – 166 693,54 zł;
- Jednostek podległych objętych Projektem – cztery urządzenia UTM na kwotę: BŚE – 87 156,32 zł, BP – 9684,04 zł, Wkład własny – 22 715,64 zł.

Łączna wartość zakupionych urządzeń w ramach dofinansowania stanowiła 98,06% wartości grantu (z BŚE wydatkowano 726 733,1 zł, z BP – 80 748,12 zł). Zgodnie z końcowym protokołem odbioru zamówienie zostało zrealizowane w dniu 18 listopada 2024 r.

(akta kontroli str. 201-213, 238-415)

Ponadto, w dniu 6 grudnia 2024 r. Starostwo udzieliło zamówienia na przeprowadzenie *Audytów SZBI, audytów zgodności z wymaganiami KRI/uoKSC – Diagnoza cyberbezpieczeństwa zgodnie z wytycznymi w ramach realizacji projektu grantowego Cyberbezpieczny samorząd w Powiecie Legionowskim*[19] na potrzeby Starostwa oraz jednostek podległych objętych Projektem (BŚE – 14 346,7 zł, BP – 1594,1 zł, wkład własny – 3769,2 zł).
Łączna wartość zamówionych audytów stanowiła 1,94% grantu.

[14] Unified Threat Management - to zintegrowany system ochrony sieci komputerowej, który łączy w sobie kilka funkcjonalności, takich jak zapory sieciowe, systemy wykrywania i zapobiegania atakom, serwery poczty elektronicznej, VPN, antywirusy i filtry treści internetowych.
[15] Oznaczenie sprawy ZPU.272.30.2024.
[16] Na łączną kwotę 996 890,40 zł.
[17] System SIEM (Security Information and Event Management) to rozwiązanie, które pomaga organizacjom w zarządzaniu bezpieczeństwem poprzez zbieranie, analizowanie i korelowanie danych z różnych źródeł w czasie rzeczywistym.
[18] FortiAnalyzer to zaawansowane narzędzie do analizy i zarządzania danymi bezpieczeństwa.
[19] W łącznej kwocie 19 680 zł.

Ustalono, że Audyty te przeprowadzała osoba wyznaczona na IOD w Starostwie oraz w trzech jednostkach podległych[20] (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 123-127, 134-151, 214-237, 416-484, 524-596, 600-764, 783-907)

Zgodnie z § 7 ust. 2 umowy grantowej Starostwo zobowiązane było do przekazania za pomocą systemu służącego do rozliczania wniosków, informacji o postępie rzeczowym realizacji Projektu. Ustalono, że wniosek sprawozdawczy został przekazany do Operatora w dniu 2 czerwca 2025 r. tj. 16 dni po upływie terminu określonego w umowie grantowej (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 174-178, 188-198, DVD-1 pliki: 010-018)

5. W realizacji Projektu poza Starostwem Powiatowym uczestniczyły cztery jednostki organizacyjne Powiatu, tj. Liceum Ogólnokształcące im. Marii Konopnickiej w Legionowie, Liceum Ogólnokształcące im. Stanisława Lema w Stanisławowie Pierwszym, Dom Pomocy Społecznej Kombatant w Legionowie, Poradnia Psychologiczno-Pedagogiczna w Legionowie. Dla podległych jednostek dokonano zakupu urządzeń UTM oraz przeprowadzono audyty z zakresu diagnozy cyberbezpieczeństwa.

(akta kontroli str. 123-127)

6. W ramach struktury organizacyjnej Wydziału obsługi Starostwa funkcjonował Zespół do spraw Informatyki, w zakresie zadań którego były m.in. działania związane z wdrażaniem nowych technologii i koordynacji prac związanych z projektami o charakterze informatycznym. Sekretarz Powiatu wskazał, że *realizacja zadań w ramach projektu wykonywana była zgodnie zakresem obowiązków służbowych oraz poleceń przełożonych.* W realizację Projektu od strony organizacyjnej, technicznej i merytorycznej zaangażowanych było 13 osób.

(akta kontroli str. 123-152)

7. Według stanu na dzień 4 lipca 2025 r. nie wystąpiła fluktuacja kadr utrudniająca sprawną realizację grantu[21].

(akta kontroli str. 128-133)

8. W ramach realizacji Projektu ustalono następujące wskaźniki produktu:
   - liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji – jeden system;
   - liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST – trzy podmioty;
   - liczba JST wspartych w zakresie cyberbezpieczeństwa – jedna JST;

[20] Tj. w Liceum Ogólnokształcącym im. Marii Konopnickiej w Legionowie, Liceum Ogólnokształcącym im. Stanisława Lema w Stanisławowie Pierwszym, Poradni Psychologiczno-Pedagogicznej w Legionowie.

[21] W okresie objętym kontrolą nastąpiła zmiana na stanowisku Starosty Legionowskiego – Projekt został rozpoczęty przez poprzedniego Starostę, a obecny Starosta kontynuuje jego realizację.

- liczba podmiotów wspartych w zakresie cyberbezpieczeństwa – dwa podmioty.

Sekretarz Powiatu wskazał, że *Pomiar wysokości wskaźników oparto na danych z realizacji poszczególnych zadań, projektowych, dokumentacji wdrożeniowej oraz zestawieniach przygotowywanych na potrzeby rozliczenia końcowego. Wszystkie przypisane projektowi wskaźniki zostały osiągnięte z założeniami. Wniosek rozliczający projekt nie został jeszcze złożony – działanie planowane jest w 2025 roku. Osiągnięcie wszystkich wskaźników zostanie w nim wykazane.*

(akta kontroli str. 134-151)

9. W toku kontroli dokonano oględzin zakupionego sprzętu, oprogramowania i ustalono, że sprzęt został uruchomiony, działa prawidłowo a systemy NAC, SIEM, Fortinite zostały skonfigurowane, m.in. monitorują i kontrolują dostęp do sieci, analizują dane w celu wykrywania zagrożeń, zarządzają ruchem sieciowym. Zlecone Audyty zostały wykonane i sformułowano w nich wnioski/rekomendacje, z których część została wdrożona a część została zaplanowana do realizacji.

(akta kontroli str. 152-163, 188-198, 415)

10. Zgodnie z § 13 ust. 1 umowy grantowej, Grantobiorca zobowiązany był do utrzymania efektów Projektu, w tym do opracowania oraz wdrożenia procedury monitorowania utrzymania efektów Projektu przez okres minimum dwóch lat od jego zakończenia. Na dzień zakończenia czynności kontrolnych, tj. 4 lipca 2025 r. Projekt był w trakcie realizacji[22], Sekretarz Powiatu wskazał, że *wszystkie elementy zarówno sprzęt, oprogramowanie jak i całe systemy wdrożone w ramach projektu, jako rozwiązania kluczowe dla bezpieczeństwa w ramach Starostwa jak i jednostek podległych, będą podlegały ciągłemu nadzorowi oraz bieżącej aktualizacji. Planowane jest zapewnienie ciągłego utrzymania oraz finansowania zarówno wsparcia, gwarancji jak i aktualizacji zakupionych rozwiązań (...) zapewnienie dokonywania przeglądów SZBI oraz odpowiednich szkoleń dla pracowników z zakresu wdrażanych rozwiązań. (...) W przypadku Starostwa planowane jest również zatrudnienie dodatkowego pracownika w ramach zespołu ds. Informatyki (...)*. Projekt miał być realizowany w okresie maksymalnie 24 miesięcy od dnia wejścia w życie umowy grantowej, tj. do 17 kwietnia 2026 r.

(akta kontroli str. 164-173)

11. Zarządzeniem nr 25/2021 Starosty Legionowskiego z dnia 10 czerwca 2021 r. wprowadzono do stosowania w Starostwie dokumentację bezpieczeństwa informacji i ochrony danych osobowych[23]. Wdrożona dokumentacja SZBI wypełnia wymogi rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz

[22] Tj. zrealizowano zakres rzeczowy projektu natomiast nie złożono wniosku rozliczającego.

[23] Obejmujące m.in. *Słownik pojęć Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), Politykę Systemu Zarządzania Bezpieczeństwem Informacji, Politykę Bezpieczeństwa Danych Osobowych, Politykę Bezpieczeństwa Fizycznego, Politykę Bezpieczeństwa Teleinformatycznego.*

minimalnych wymagań dla systemów teleinformatycznych[24], a także RODO. Wszyscy pracownicy Starostwa zaangażowani w proces przetwarzania informacji, zostali zapoznani z powyższą dokumentacją i zobowiązani do przestrzegania zasad w niej zawartych. Osobą odpowiedzialną za projektowanie, przegląd oraz aktualizację dokumentu był IOD, natomiast Starosta Legionowski odpowiadał za zatwierdzenie dokumentu.

(akta kontroli str. 123-127, 600-722)

12. Zgodnie z § 19 ust. 2 pkt 1 rozporządzenia KRI w Starostwie corocznie dokonywano przeglądu dokumentacji SZBI i dokonywano w niej zmian w wyniku zaleceń audytowych.

(akta kontroli str. 152-173)

13. W okresie objętym kontrolą zadania IOD zostały powierzone osobie nie będącej pracownikiem Starostwa na podstawie trzech następujących po sobie umów zawartych z firmą zewnętrzną.

(akta kontroli str. 134-151, 524-596)

Zgodnie z § 19 ust. 2 pkt 14 rozporządzenia KRI w Starostwie przeprowadzano okresowe audyty wewnętrzne z zakresu bezpieczeństwa informacji. W wyniku przeprowadzonych audytów przedstawiono rekomendacje, z czego większość została wdrożona.
Ustalono, że ww. audyty[25] przeprowadzała osoba wyznaczona na IOD w Starostwie (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 164-173, 600-782)

14. Obowiązki w zakresie informacji i promocji zostały określone w § 11 umowy grantowej. Starostwo Powiatowe w Legionowie, realizując postanowienia zawartej umowy, opublikowało informację o przyznaniu dofinansowania m.in.:
    - na oficjalnej witrynie internetowej Powiatu Legionowskiego – w aktualności z dnia 5 lutego 2024 r., dostępnej pod adresem: https://powiat-legionowski.pl/aktualnosci/cyberbezpieczny-samorzad-w-powiecie-legionowskim;
    - w mediach społecznościowych – na oficjalnym profilu Powiatu Legionowskiego w serwisie Facebook;

Ustalono, że zakres publikowanych informacji nie był zgodny z postanowieniami § 11 ust. 3 umowy grantowej (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).
Zgodnie z § 11 ust. 4 pkt 2 umowy grantowej, zamieszczono plakaty informacyjne i promocyjne w formacie A3 oraz plakaty reklamowe Programu Cyberbezpieczny Samorząd - w Starostwie Powiatowym w Legionowie oraz w jednostkach biorących udział w Projekcie. Plakaty zawierały wszystkie wymagane oznaczenia, tj. znak Funduszy Europejskich oraz Unii Europejskiej,

[24] Dalej: rozporządzenie KRI (Dz.U. poz. 773). Poprzednio w okresie objętym kontrolą obowiązywało także 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).

[25] Zadania pn. *Audyt wewnętrzny bezpieczeństwa informacji i ochrony danych osobowych w oparciu o wymagania PN ISO/IEC 27001 i RODO (w latach 2023-2024).*

nazwę beneficjenta oraz tytuł projektu, a także wysokość dofinansowania i adres portalu mapadotacji.gov.pl.

(akta kontroli str. 164-173, 179-198, DVD-1 pliki: 010-018)

Stwierdzone nieprawidłowości

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

1. Opóźnienie w realizacji obowiązków sprawozdawczych, co stanowiło naruszenie § 7 ust. 2 umowy grantowej.
   W myśl postanowienia umowy grantowej, Grantobiorca zobowiązuje się do przekazania za pomocą systemu służącego do rozliczania wniosków, dostępnego na stronie internetowej konkursu pn. „Cyberbezpieczny Samorząd" informacji o postępie rzeczowym realizacji Projektu w formie wskazanej przez Operatora w terminie 30 dni następujących po upływie 12 miesięcy od podpisania Umowy przy wykorzystaniu transzy pierwszej, oraz w terminie 30 dni następujących po upływie 18 miesięcy od dnia podpisania Umowy przy wykorzystaniu transzy drugiej. Ustalono, że wniosek sprawozdawczy został przekazany do Operatora w dniu 2 czerwca 2025 r., tj. 16 dni po upływie terminu określonego w umowie grantowej.
   Sekretarz Powiatu wyjaśnił, że m.in. *Opóźnienie w złożeniu informacji o postępie rzeczowym realizacji Projektu wynikało z przyjętej przez Grantobiorcę interpretacji postanowień § 7 ust. 2 umowy grantowej, opartej na sposobie wypłaty środków. Powiat Legionowski wystąpił do Operatora z wnioskiem o wypłatę całkowitej kwoty dofinansowania w formie jednorazowej zaliczki. W konsekwencji obie transze zostały przekazane jednocześnie. Grantobiorca uznał, że w takiej sytuacji zastosowanie znajduje termin określony w zdaniu drugim § 7 ust. 2 umowy grantowej – tj. 30 dni po upływie 18 miesięcy od podpisania Umowy. W ocenie Grantobiorcy wcześniejszy, 12 – miesięczny termin odnosił się wyłącznie do przypadków, gdy transze wypłacane są rozdzielnie, zgodnie z domyślnym harmonogramem. (...) Podkreślamy, że zaistniałe opóźnienie miało charakter interpretacyjny, incydentalny (...) złożenie wniosku sprawozdawczego nastąpiło niezwłocznie po otrzymaniu wezwania, z zachowaniem należytej staranności i w duchu pełnej współpracy z Operatorem.*

   (akta kontroli str. 174-178, 188-198, DVD-1 pliki: 010-018)

2. Przeprowadzenie w Urzędzie i trzech jednostkach podległych *Audytów SZBI, audytów zgodności z wymaganiami KRI/uoKSC – Diagnoza cyberbezpieczeństwa zgodnie z wytycznymi w ramach realizacji projektu grantowego Cyberbezpieczny samorząd w Powiecie Legionowskim,* a także przeprowadzenie w Urzędzie *Audytu wewnętrznego bezpieczeństwa informacji i ochrony danych osobowych w oparciu o wymagania PN ISO/IEC 27001 i RODO*[26] przez osobę, która pełniła w tych jednostkach jednocześnie funkcję IOD, co naruszało art. 38 ust. 6 RODO.
   Zgodnie z art. 38 ust. 6 RODO, osoba wyznaczona na IOD może wykonywać inne zadania i obowiązki, jednak administrator danych (tj. Starosta) musi zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. Zgodnie z wytycznymi Normy PN-ISO/IEC 27001:2017 punkt 9.2 *Audyt*

[26] W latach 2023-2024.

wewnętrzny Organizacja powinna: wybierać audytorów i prowadzić audyty w sposób zapewniający obiektywność i bezstronność procesu audytu.

Sekretarz Powiatu wyjaśnił, że *Audyt przeprowadzony przez Inspektora Ochrony Danych nie narusza zasady niezależności, ponieważ: IOD nie odpowiada za wdrażanie środków technicznych i organizacyjnych w zakresie bezpieczeństwa informacji – jego rola ogranicza się do funkcji doradczej i kontrolnej, audyt nie dotyczył obszarów, za które IOD ponosiłby odpowiedzialność operacyjną, działania audytowe były zgodne z zakresem jego zadań określonych w art. 39 RODO. Tym samym nie występuje konflikt interesów, o którym mowa w motywie 97 RODO. Zadania otrzymane w ramach umowy na pełnienie funkcji Inspektora Ochrony Danych w ramach dokumentacji (jako wyciąg z oferty): Opracowanie szczegółowych procedur obsługi żądań oraz wniosków osób, których dane osobowe są przetwarzane, w celu realizacji ich praw wynikających z RODO; Wsparcie w opracowaniu indywidualizowanej dokumentacji ochrony danych osobowych na gruncie prawa krajowego w tym umów powierzenia, klauzul informacyjnych , analizy ryzyka, RCP, DPIA, zasad bezpieczeństwa zgodnie z ISO 27001, ISO 27005, ISO 31000 (...) W związku z powyższym w ramach funkcjonującej umowy na pełnienie funkcji Inspektora Ochrony Danych obowiązki dot. aktualizacji dokumentacji ograniczają się do opiniowania i wsparcia. Jako osoba, która przed podpisem przez Sekretarza lub Starostą zatwierdza wprowadzone zmiany i zgodnie z zarządzeniem 25/2021 z dn. 10 czerwca 2021 r. widnieje jako osoba ostatecznie wprowadzająca zmianę, jednak nie tworzy tych zmian.*

Zdaniem NIK wykonywanie obowiązków IOD w Starostwie, jak i jednostkach podległych, oraz przeprowadzenie ww. audytów, stanowi konflikt interesów i tym samym narusza art. 38 ust. 6 RODO. Powyższe wynika z faktu, iż zadaniem audytora było sprawdzenie przestrzegania zgodności działań Starostwa (jego pracowników) z przepisami prawa (w tym RODO), natomiast jednym z zadań IOD jest decydowanie o stosowaniu przepisów RODO w Starostwie (art. 39 ust. 1 RODO). Pomimo, iż Starosta ostatecznie zatwierdzał zmiany w SZBI, to merytoryczne opracowanie zmian leżało po stronie IOD – osoby, która sama dokonywała przeglądów zgodności, audytowała wdrożone procedury i kontrolowała obszar działań, m.in. postępowania z incydentami naruszenia danych osobowych, które sama współtworzyła i za które odpowiadała, tym samym oceniając poprawność tych działań, oraz przygotowując propozycje zmian. Biorąc pod uwagę fakt, że audyt wewnętrzny SZBI powinien być przeprowadzany przez osoby zapewniające obiektywność i bezstronność procesu audytu, w tym przypadku ocena SZBI przez IOD stwarza ryzyko dla procesu weryfikacji zapewnienia stanu bezpieczeństwa informacji stosowanego w Starostwie.

(akta kontroli str. 123-127, 134-151, 164-173, 214-237, 416-484, 524-596, 600-907)

3. Nieprzestrzeganie niektórych obowiązków informacyjnych i promocyjnych w zakresie stosowania oznaczania znakiem Unii Europejskiej i Funduszy Europejskich, i barw Rzeczypospolitej Polskiej w publikowanych informacjach na stronie internetowej oraz oficjalnym profilu mediów społecznościowych,

a także części dokumentacji projektowej, co było niezgodne z postanowieniami § 11 ust. 3 umowy grantowej.

Zgodnie z § 11 ust. 3 umowy grantowej, w zakresie informacji i promocji Starostwo ma obowiązek stosować zasady określone w „Podręczniku wnioskodawcy i beneficjenta programów polityki spójności na lata 2021 - 2027 w zakresie informacji i promocji" (dalej: podręcznik). Obowiązki informacyjne i promocyjne muszą być wypełniane od momentu podpisania umowy (punkt 3 podręcznika). W toku kontroli ustalono, że wśród dokumentów dotyczących postępowania przetargowego przeprowadzonego w ramach projektu, część dokumentów[27] nie posiadała oznaczenia, wymaganego umową, tzn. nie zostały oznaczone znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich.

Ponadto, w wyniku przeprowadzonych oględzin ustalono, że Starostwo w dniu 5 lutego 2024 r. zamieściło informację na stronie internetowej Starostwa oraz oficjalnym profilu w mediach społecznościowych (facebook) o otrzymaniu dofinansowania w zakresie Projektu *Cyberbezpieczny Samorząd.* Zamieszczone informacje nie spełniały wymogów określonych w podręczniku, gdyż brak było informacji o otrzymaniu wsparcia finansowego z Unii Europejskiej, czyli: znaku Funduszy Europejskich, znaku barw Rzeczypospolitej Polskiej i znaku Unii Europejskiej; zadaniach, działaniach, które będą realizowane w projekcie (opis, co zostanie zrobione, zakupione etc.); efektach, rezultatach projektu (jeśli opis zadań, działań nie zawiera opisu efektów, rezultatów); hasztagi: #FunduszeUE lub #FunduszeEuropejskie.

Sekretarz Powiatu wyjaśnił, że m.in.: *(...) Uchybienie to miało charakter incydentalny, niezamierzony i zostało zidentyfikowane niezwłocznie po zakończeniu postępowania (...) w odpowiedzi na zidentyfikowane uchybienie, wdrożono działania naprawcze mające na celu zapewnienie pełnej zgodności z wymogami promocyjnymi w dalszym przebiegu projektu oraz w przyszłych działaniach grantowych. (...) W trakcie przeprowadzonych oględzin w dniu 16 czerwca 2025 r. ustalono, że artykuł ten nie zawierał wówczas wymaganych oznaczeń graficznych (logotypów) ani obowiązkowych hasztagów (...) Grantobiorca potwierdza, że był to efekt przeoczenia. Braki zostały uzupełnione przez Grantobiorcę (...).*

W związku z usunięciem stwierdzonej nieprawidłowości, NIK odstępuje od formułowania wniosku pokontrolnego w tym zakresie.

(akta kontroli str. 164-173, 179-198, DVD-1 pliki: 010-018)

[27] M.in.: wyjaśnienie i zmiana treści SWZ, ogłoszenie o zamówieniu, ogłoszenie o zmianie ogłoszenia, opis przedmiotu zamówienia, protokół postępowania w trybie podstawowym.

IV. Wnioski

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

Wnioski

1. Terminowe przekazywanie informacji o postępie rzeczowym realizacji Projektu.
2. Zapewnienie aby zadania zlecane IOD nie powodowały konfliktu interesów.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne sporządzono w postaci elektronicznej z użyciem kwalifikowanych podpisów elektronicznych.

Prawo zgłoszenia zastrzeżeń

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Warszawa, lipca 2025 r.

Kontroler

Łukasz Hertel

Główny specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Departament Administracji Publicznej

p.o. Dyrektor

Bogdan Skwarka

/podpisano elektronicznie/