NAJWYŻSZA IZBA KONTROLI

DEPARTAMENT ADMINISTRACJI PUBLICZNEJ

KAP.410.2.1.2025

Pan
Stefan Prusik
Wójt Gminy Lelis
Urząd Gminy Lelis
ul. Szkolna 39
07-402 Lelis

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	Urząd Gminy Lelis, ul. Szkolna 39, 07-402 Lelis, dalej: Urząd
Kierownik jednostki kontrolowanej	Stefan Prusik, Wójt, od 18 listopada 2014 r., dalej: Wójt
Zakres przedmiotowy kontroli	Realizacja przez Gminę Lelis działań w celu zwiększenia poziomu cyberbezpieczeństwa
Okres objęty kontrolą	Od 1 stycznia 2023 r. do zakończenia czynności kontrolnych w 2025 r., tj. 27 czerwca 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Marcin Grochal, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/41/2025 z 30 kwietnia 2025 r.

(akta kontroli str.: 1-7)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Gmina Lelis w latach 2023 – 2025 podejmowała działania w celu zwiększenia poziomu cyberbezpieczeństwa, w tym w ramach realizacji projektu pn. *Dostosowanie struktury informatycznej Gminy Lelis w zakresie cyberbezpieczeństwa* (dalej: Projekt) m.in. przeprowadzono postępowanie przetargowe oraz zawarto umowy na dostawę, instalację i konfigurację sprzętu i oprogramowania. Ponadto, uruchomiono usługi SaaS multiportalu Gminy wraz z ochroną AntyDDos. Stwierdzone w trakcie kontroli nieprawidłowości nie miały zasadniczego wpływu na realizację Projektu.

Uzasadnienie oceny ogólnej

W okresie objętym kontrolą w Urzędzie rozpoznano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, m.in. poprzez przeprowadzenie wśród pracowników Urzędu testu cyberbezpieczeństwa i opracowanie koncepcji realizacji Projektu. Przeprowadzono okresowy audyt z zakresu bezpieczeństwa informacji, a także ustalono adekwatne wskaźniki produktu i rezultatu. Wypełniono *Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego* (dalej: Ankieta Dojrzałości) i przekazano do Operatora[3] z zachowaniem terminu i formy określonych w umowie o powierzenie grantu[4] (dalej: umowa grantowa), zawartej 24 czerwca 2024 r. z Centrum Projektów Polska Cyfrowa (dalej: CPPC lub Grantodawca). W ramach tej umowy przyznano dofinansowanie na realizację Projektu w kwocie 807 004,00 zł[5]. Wydatki poniesione przez Grantobiorcę w ramach Projektu w okresie objętym kontrolą wyniosły 34 322,95 zł[6] i dotyczyły w szczególności usług doradczych w zakresie przygotowania wniosku o dofinansowanie i postępowania na zakup sprzętu i oprogramowania, a także zakupu usług SaaS w bezpiecznej chmurze z ochroną AntyDDoS. Zostały one zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we Wniosku o przyznanie grantu[7].

Stwierdzone nieprawidłowości dotyczyły:

- niewdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 19 ust. 1 w związku z ust. 3 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 minimalnych wymagań dla systemów teleinformatycznych[8];
- niewypełnienia niektórych obowiązków z zakresu informacji i promocji Projektu określonych na podstawie § 11 ust. 3 umowy grantowej, w zakresie oznaczenia dokumentów znakami Funduszy Europejskich i Unii Europejskiej oraz barwami Rzeczypospolitej Polskiej, a także nie zawarcia

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Tj. do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.
[4] Umowa nr FERC.02.02-CS.01-001/23/0895/ FERC.02.02-CS.01-001/23/2024.
[5] Z tego z budżetu państwa - 145 260,00 zł, budżet środków Unii Europejskiej – 661 744,00 zł.
[6] Według stanu na 18 czerwca 2025 r.
[7] Wniosek o przyznanie grantu nr 1c608aa1-6511-47ed-9973-b2d048444845 (dalej: Wniosek).
[8] Dz. U. poz. 773, dalej: rozporządzenie KRI.

wymaganych informacji dotyczących opisu Projektu na stronie internetowej i mediach społecznościowych Urzędu;
– nierzetelnego sporządzenia Ankiety Dojrzałości.

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

OBSZAR

1. Realizacja przez Gminę Lelis działań w celu zwiększenia poziomu cyberbezpieczeństwa

Opis stanu faktycznego

1. Obowiązującym w Urzędzie dokumentem wskazującym kierunki rozwoju gminy na najbliższe lata była Strategia rozwoju Gminy Lelis na lata 2014-2030, uchwalona przez Radę Gminy Lelis w 2014 r.[10], która nie była aktualizowana. W dokumencie nie zawarto zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa.

Wójt poinformował, że *w roku 2014 roku pojęcie cyberbezpieczeństwa nie było tak rozpowszechnione jak obecnie i nie stanowiło to tak istotnego elementu strategii rozwoju.* Dodał także, że 28 kwietnia 2025 r. Rada Gminy Lelis, podjęła uchwałę dotyczącą opracowania Strategii Gminy Lelis na lata 2026 – 2035[11].

(akta kontroli str.: 8-86, 288-291)

2. W zakresie działań podejmowanych w Urzędzie w celu rozpoznania potrzeb zwiększenia poziomu cyberbezpieczeństwa Wójt wyjaśnił, że w 2023 r. i 2024 r. we współpracy z firmą zewnętrzną opracowano koncepcję realizacji projektu w ramach konkursu Cyberbezpieczny Samorząd, stanowiącą podstawę do określenia potrzeb oraz zakresu Projektu. Ponadto, w 2024 r. przeprowadzono test cyberbezpieczeństwa, którego celem było zidentyfikowanie potencjalnych luk w zabezpieczeniach systemów informatycznych Urzędu oraz ocena zachowania pracowników.

(akta kontroli str.: 288-352, 441-472)

3. W Urzędzie opracowano Ankietę Dojrzałości, która została przekazana do Operatora za pośrednictwem skrzynki ePUAP w terminie 30 dni od zawarcia umowy o powierzenie grantu, zgodnie z § 4 ust. 1 pkt 4 umowy grantowej.

Ankieta Dojrzałości została opracowana nierzetelnie, co opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.: 87-90; CD pliki: 028-038)

4. Projekt *Dostosowanie struktury informatycznej Gminy Lelis w zakresie cyberbezpieczeństwa* był realizowany w ramach programu Fundusze Europejskie na Rozwój Cyfrowy, Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2.

[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] Uchwała nr XXX/229/2014 Rady Gminy Lelis z dnia 28 kwietnia 2014 r., dalej: Strategia.
[11] Uchwała XIII/97/2025 w sprawie przystąpienia do opracowania projektu Strategii Rozwoju Gminy Lelis na lata 2026-2035 oraz określenia szczegółowego trybu i harmonogramu opracowania projektu Strategii Rozwoju Gminy Lelis na lata 2026-2035, w tym trybu konsultacji.

Wzmocnienie krajowego systemu cyberbezpieczeństwa. Powierzenie grantu nastąpiło na podstawie umowy grantowej zawartej na okres 24 miesięcy, tj. do 24 czerwca 2026 r.

Grant przyznano w kwocie 807 004 zł, stanowiącej 100% kwoty wnioskowanej, z tego 661 744,00 zł (82,00%) ze środków Unii Europejskiej i 145 260,00 zł (18,00%) ze środków budżetu państwa. Zakres przedmiotowy grantu wskazany we wniosku obejmował realizację zadań w dwóch obszarach określonych w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd”[12] – organizacyjnym i technicznym.

W obszarze organizacyjnym wniosek obejmował realizację zadań związanych z przeglądem, aktualizacją dokumentacji i audytem Systemu Zarządzania Bezpieczeństwem Informacji oraz przygotowaniem Ankiety Dojrzałości. Ich wartość oszacowano na 43 050,00 zł, co stanowiło 5,3% wnioskowanej kwoty grantu. W obszarze technicznym wniosek obejmował w szczególności zakup sprzętu, oprogramowania oraz usług doradczych i SaaS[13] o łącznej wartości 763 954,00 zł, stanowiących 94,7% wnioskowanej kwoty grantu. W wniosku nie wskazano zadań w obszarze kompetencyjnym.

Zgodnie z § 2 ust. 7 umowy grantowej wypłata dofinansowanie na realizację Projektu miała nastąpić w trzech transzach stanowiących 30%, 30% i 40% kwoty wydatków kwalifikowanych. Pierwszą transzę grantu w kwocie 242 101,20 zł (30,0%) Gmina Lelis otrzymała 7 sierpnia 2024 r. W dniu 20 listopada 2024 r. Wójt wystąpił do Operatora z wnioskiem o wypłatę pozostałej kwoty. W uzasadnieniu wniosku wskazano na konieczność zabezpieczenia pełnej kwoty postępowania przetargowego na dostawę sprzętu IT oraz oprogramowania, oszacowanej na 683 337,26 zł. Wniosek został zaakceptowany i pozostała kwota dofinansowania 564 902,80 zł (70,0%) została przekazana Gminie 6 grudnia 2024 r.

(akta kontroli str.: 860-885; CD pliki: 003-027, 045-086, 096-104)

Gmina Lelis zawarła w ramach Projektu sześć umów obejmujących w szczególności: zakup sprzętu, oprogramowania oraz usługi SaaS w bezpiecznej chmurze z ochroną Anty DDoS i usługi doradcze, na łączną kwotę 754 519,50 zł. Wartość sprzętu teleinformatycznego objętego umowami, w tym serwera aplikacyjnego, serwera backupu, pięciu dysków do macierzy, ośmiu dysków do NAS i dwóch przełączników sieciowych, wyniosła 529 662,60 zł, co stanowiło 70,2% łącznej wartości zawartych umów.

Według stanu na dzień 18 czerwca 2025 r. wydatki poniesione przez Urząd w ramach Projektu wyniosły 34 322,95 zł, z tego 17 629,00 zł na opracowanie koncepcji realizacji Projektu i usługi doradcze wspomagające realizację Projektu i 16 693,95 zł w ramach usług SaaS multiportalu Gminy Lelis w bezpiecznej chmurze wraz z ochroną AntyDDos, SSL, kopią bezpieczeństwa, monitorowaniem zdarzeń i reagowaniem, ciągłą aktualizacją i hostingiem za okres od grudnia 2024 r. do maja 2025 r. Poniesione w okresie objętym kontrolą

[12] https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad
[13] Software as a Service (oprogramowanie jako usługa).

wydatki stanowiły 4,55% wartości zawartych umów i 4,25% łącznej kwoty przyznanego dofinansowania.

(akta kontroli str.: 473-484, 598-828, 860-885; CD pliki: 007, 045-067, 092-095)

5. We wniosku o przyznanie grantu wskazano Urząd Gminy Lelis jako jedyny podmiot korzystającym z wnioskowanych rozwiązań. W ramach realizowanego Projektu nie przewidziano udziału innych, poza Urzędem Gminy, jednostek organizacyjnych gminy. Wójt poinformował, że wynikało to z ograniczonych możliwości finansowych budżetu Gminy. Dodał także, że *w przypadku pojawienia się możliwości uczestnictwa w kolejnych projektach dedykowanych dla cyberbezpieczeństwa urząd gminy uwzględni poszczególne jednostki organizacyjne*.

(akta kontroli str.: 94-317, 861-885; CD pliki: 003-027)

6. W realizację Projektu zaangażowanych było pięciu pracowników Urzędu, z tego jeden informatyk koordynujący Projekt i uczestniczący w komisji przetargowej powołanej zarządzeniem Wójta Gminy Lelis[14], trzy osoby z Referatu Inwestycji i Rozwoju uczestniczące w postępowaniach zakupowych w ramach Projektu, w tym w komisji przetargowej oraz jedna osoba z Referatu Finansowego w zakresie rozliczenia finansowego Projektu. Pracownicy posiadali kwalifikacje i doświadczenie.

(akta kontroli str.: 473-484)

7. W okresie objętym kontrolą nie wystąpiła w Urzędzie fluktuacja kadr mogąca wpłynąć na realizację Projektu.

(akta kontroli str.: 473-484)

8. We wniosku o przyznanie grantu Gmina Lelis wskazała pięć planowanych do osiągnięcia wskaźników wyrażających cele Projektu:

- Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji – 2 szt.;
- Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST – 1 szt.;
- Liczba JST wspartych w zakresie cyberbezpieczeństwa – 1 szt.;
- Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa – 1 szt.;
- Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych – 1 szt.

Były one zgodne ze wskaźnikami zdefiniowanymi dla całego konkursu grantowego określonymi w załączniku nr 9 do Regulaminu Konkursu Grantowego i były adekwatne do zakresu działań w ramach grantu.

[14] Zarządzenie nr 120.8.2022 Wójta Gminy Lelis z dnia 10 maja 2022 r. w sprawie powołania komisji przetargowej.

Do zakończenia czynności kontrolnych, tj. 27 czerwca 2025 r. realizacja Projektu nie została zakończona i docelowe wartości wskaźników nie zostały osiągnięte.

(akta kontroli str.: 861-885; CD pliki: 003-027)

9. W ramach Projektu, w okresie objętym kontrolą wykonano usługi doradcze w zakresie przygotowania koncepcji realizacji Projektu i przygotowania wniosku o przyznanie grantu oraz przygotowania Opisu Przedmiotu Zamówienia w postępowaniu przetargowym na dostawę, instalację i konfigurację sprzętu i oprogramowania. Ponadto, uruchomiono w ramach Projektu świadczenie usługi SaaS multiportalu Gminy Lelis w bezpiecznej chmurze wraz z ochroną AntyDDos, SSL, kopią bezpieczeństwa, monitorowaniem zdarzeń i reagowaniem, ciągłą aktualizacją i hostingiem. Do zakończenia czynności kontrolnych, tj. do 27 czerwca 2025 r. sprzęt oraz oprogramowanie nie zostały uruchomione, gdyż zgodnie z zawartymi w ramach Projektu umowami, termin dostawy, konfiguracji i uruchomienia urządzeń i oprogramowania ustalony został w drugim półroczu 2025 r.

(akta kontroli str.: 598-885; CD pliki: 045-055)

10. Zgodnie z § 13 ust. 1 Umowy grantowej, Urząd 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. 27 czerwca 2025 r. Projekt był w trakcie realizacji i na tym etapie nie przewidziano jeszcze działań w celu utrzymania poziomu cyberbezpieczeństwa po zakończeniu realizacji grantu. Projekt miał być realizowany w okresie maksymalnie 24 miesięcy od dnia wejścia w życie Umowy grantowej, tj. do 24 czerwca 2026 r.

(akta kontroli str.: 861-885; CD pliki: 001-027)

11. W Urzędzie nie został opracowany, ustanowiony i wdrożony System Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI, co opisano w sekcji *Stwierdzone nieprawidłowości.*

W okresie objętym kontrolą w zakresie bezpieczeństwa informacji w Urzędzie obowiązywała jedynie *Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji*[15] wprowadzona w 2022 r. Wprowadzone w 2021 r. *Polityka Ochrony Danych Osobowych w Urzędzie Gminy Lelis*[16], *Instrukcja Zarządzania Systemem Informatycznym w Urzędzie Gminy Lelis*[17] dotyczyły bezpieczeństwa danych osobowych.

(akta kontroli str.: 94-95, 148-287, 571-583)

---

[15] Zarządzenie nr 120.15.2022 Wójta Gminy Lelis z dnia 31 sierpnia 2022 r. w sprawie wprowadzenia w Urzędzie Gminy Lelis procedury zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji.

[16] Zarządzenie nr 120.3.2021 Wójta Gminy Lelis z dnia 19 marca 2021 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy Lelis.

[17] Zarządzenie nr 120.4.2021 Wójta Gminy Lelis z dnia 19 marca 2021 r. w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Lelis.

12. W okresie objętym kontrolą w latach 2023 – 2024 w Urzędzie dwukrotnie przeprowadzono audyt z zakresu bezpieczeństwa informacji, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI[18]. Audyt został przeprowadzony przez podmiot zewnętrzny, którego personel posiadał odpowiednie kwalifikacje oraz doświadczenie w realizacji tego typu zadań, zgodnie z obowiązującymi standardami i przepisami. W wyniku audytu sformułowano trzy zalecenia:

- wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji obejmującego politykę bezpieczeństwa informacji i instrukcję zarządzania systemem informatycznym oraz dokonywanie jego przeglądu i aktualizacji w cyklu przynajmniej 12 miesięcznym;
- przeprowadzenie i powtarzanie w cyklu co najmniej rocznym analizy ryzyka utraty integralności, poufności, dostępności informacji;
- zapewnienie systemowego podejścia do zarządzania podatnościami.

W celu realizacji zaleceń, w styczniu 2025 r. w przeprowadzono ocenę ryzyka systemów informatycznych i ochrony danych w urzędzie. Wójt wyjaśnił, że w zakresie systemowego podejścia do zarządzania podatnościami Gmina posiada wdrożony system znacząco zmniejszający ryzyko wielu zagrożeń cyberataków. Dodał że, w ramach Projektu Cyberbezpieczny Samorząd wdrażane będzie oprogramowanie oraz monitoring usług i systemów IT użytkowanych przez Urząd oraz zostanie opracowany i wdrożony pełny Systemu Zarządzania Bezpieczeństwem Informacji.

(akta kontroli str.: 94-143, 288-352, 861-885; CD pliki: 039-044)

13. Na podstawie § 11 ust. 3 umowy grantowej, w zakresie informacji i promocji Projektu Grantobiorca zobowiązany był do stosowania zasad określonych w *Podręczniku wnioskodawcy i beneficjenta programów polityki spójności na lata 2021 -2027 w zakresie informacji i promocji* (dalej: Podręcznik). Obowiązek obejmował w szczególności:

- oznaczenie miejsca realizacji Projektu poprzez umieszczenie plakatu;
- zamieszczenie znaków Funduszy Europejskich, barw RP i Unii Europejskiej na dokumentach związanych z Projektem, w tym na dokumentacji przetargowej, umowach, stronach internetowych, e-publikacjach;
- umieszczenie opisu Projektu na stronie internetowej oraz w mediach społecznościowych urzędu.

Gmina informowała opinię publiczną o fakcie otrzymania dofinansowania poprzez umieszczenie plakatów m.in. na tablicach informacyjnych w holu głównym oraz przed budynkiem Urzędu. Plakaty zawierały wszystkie wymagane oznaczenia, tj. znaki Funduszy Europejskich oraz Unii Europejskiej, nazwę beneficjenta oraz tytuł Projektu, a także wysokość dofinansowania i adres portalu mapadotacji.gov.pl. Na stronie internetowej Urzędu[19] oraz w mediach społecznościowych umieszczono informacje dotyczące realizacji Projektu oraz jego dofinansowania ze środków Unii Europejskiej. Wypełniono także obowiązek w zakresie dokumentowania realizacji działań informacyjnych i promocyjnych poprzez utworzenie segregatora, w którym przechowywano zrzuty ekranu ze

[18] Audyt przeprowadzono 24 listopada 2023 r. i 18 listopada 2024 r.
[19] https://lelis.pl/cyberbezpieczny-samorzad.html

strony internetowej oraz mediów społecznościowych, a także zdjęcia plakatów informujących o Projekcie, umieszczonych w Urzędzie.

Nie wszystkie dokumenty posiadały wymagane oznaczenia w postaci znaków Funduszy Europejskich, barw RP i Unii Europejskiej. Ponadto ustalono, że termin oraz zakres informacji publikowanych na stronie internetowej oraz w mediach społecznościowych, a także oznaczenie części dokumentów w postępowaniu przetargowym w ramach Projektu nie były zgodne z wymaganiami określonymi w *Podręczniku wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji*. Szczegółowy opis nieprawidłowości w punkcie drugim w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.: 353-369, 861-885; CD pliki: 003-027)

Stwierdzone nieprawidłowości

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

1. W Urzędzie Gminy Lelis nie został opracowany, ustanowiony i wdrożony Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), co było niezgodne z § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI. Stosownie do ww. przepisów Urząd Gminy zobowiązany był m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i doskonalenia SZBI, zapewniającym poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak rozliczalność, autentyczność, niezaprzeczalność i niezawodność.

Wójt wyjaśnił, że Polityka Bezpieczeństwa Informacji (w myśl rozporządzenia KRI) oraz inne dokumenty stanowiące System Zarządzania Bezpieczeństwem Informacji nie zostały wcześniej opracowane, ponieważ uznano, że obowiązujące w Urzędzie dokumenty, są wystarczające w zakresie bezpieczeństwa informacji. Dodał także, że (...) *w ramach przystąpienia do projektu „Cyberbezpieczny Samorząd" zaplanowano przegląd, opracowanie i wdrożenie nowej dokumentacji w zakresie Polityki Bezpieczeństwa Informacji (w myśl rozporządzenia KRI)*.

(akta kontroli str.: 94-287, 571-583, 861-885; CD pliki: 039-044)

2. Niepełna realizacja obowiązków w zakresie informacji i promocji.

Zgodnie z pkt 3 Podręcznika obowiązek w zakresie informacji i promocji powstał od momentu podpisania umowy grantowej. Informacje o realizacji Projektu zostały umieszczone na stronie internetowej 8 sierpnia 2024 r., a w mediach społecznościowych 14 maja 2025 r. tj. odpowiednio 45 i 324 dni po powstaniu obowiązku, tj. po podpisaniu umowy grantowej. Ustalono, że informacje na stronie internetowej Urzędu (www.lelis.pl) oraz na oficjalnym profilu Urzędu w mediach społecznościowych (Facebook.com/GminaLelis) nie zawierały niektórych wymaganych informacji dotyczących opisu Projektu, wskazanych w punkcie 11 Podręcznika. Nie wskazano tam m.in. zadań i działań, które będą

realizowane w Projekcie, grup docelowych, efektów, rezultatów Projektu. Nie umieszczono także hashtagów #FunduszeUE lub #FunduszeEuropejskie.

Wójt wyjaśnił, że *na etapie początkowym realizacji projektu (...) Gmina Lelis koncentrowała się przede wszystkim na przygotowaniu infrastruktury technicznej organizacyjnej niezbędnej do wdrożenia zadań projektowych (...). W związku z tym, zadania promocyjne i informacyjne nie były jeszcze realizowane (...) działania promocyjne zostały podjęte w momencie przekazania pierwszej transzy środków.* Dodał także, że w momencie podpisania umowy w natłoku zadań przeoczono umieszczenie informacji w mediach społecznościowych.

Ponadto ustalono, że część dokumentów dotyczących postępowania przetargowego przeprowadzonego w ramach Projektu[20] nie posiadała oznaczeń wskazanych w punkcie 7 Podręcznika, tj. znaku Unii Europejskiej, barw Rzeczypospolitej Polskiej i znaku Funduszy Europejskich. W trakcie kontroli dokonano uzupełnienia brakujących danych na stronie internetowej oraz na profilu w mediach społecznościowych.

Wójt wyjaśnił, że pominięcie oznaczeń było przeoczeniem wynikającym z intensywnego harmonogramu prac w celu zapewnienia zgodności formalnej i merytorycznej postępowania przetargowego.

(akta kontroli str.: 353-440, 861-885; CD pliki: 001-27, 101-138)

3. Nierzetelne sporządzenie Ankiety Dojrzałości.
W przekazanej do Operatora Ankiecie Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego, przedstawiono informacje o obecnym i planowanym w ramach Projektu stanie poszczególnych działań wymienionych we wzorze ankiety stanowiącym załącznik nr 6 do Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd".
Ustalono, że w przypadku trzech działań opis stanu obecnego był nierzetelny:

1) W działaniu *Konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji Jednostki* w ramach obszaru *System Zarządzania Bezpieczeństwem Informacji (SZBI)* wskazano jako stan obecny *CZĘŚCIOWO.* Kontrola NIK ustaliła, że w Urzędzie w dokumentach strategicznych nie ujęto kwestii zapewnienia bezpieczeństwa informacji. Wójt wyjaśnił, że *Strategia rozwoju Gminy Lelis określa wykorzystanie nowych technologii w zakresie dostępu mieszkańców do e-usług (np. E-podatki) oraz współpracę z operatorami w zakresie dostępu do szerokopasmowego internetu. Brak formalnej strategii wynika z etapu przygotowań do jej opracowania, planowanego w ramach opracowywania SZBI*.

Zdaniem NIK, zawarte w Strategii rozwoju Gminy Lelis informacje dotyczące usług internetowych nie odnoszą się do zapewnienia bezpieczeństwa informacji.

2) W działaniu *Polityki reagowania na incydenty w Jednostce są aktualizowane* w ramach obszaru *Reagowanie (RE)* wskazano stan obecny jako *TAK*. Wójt wyjaśnił, że Polityka bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznym z 2018 r. zostały zaktualizowane

[20] M.in.: ustalenie wartości zamówienia publicznego, informacja z otwarcia ofert, odpowiedź na wniosek oferenta.

w 2021 r. Dodał także, że *kolejna aktualizacja pełnej dokumentacji i procedur nastąpi w ramach projektu "Cyberbezpieczny Samorząd" w 2025 r. - 2026 r.*

Ustalono, że w okresie objętym kontrolą obowiązująca w Urzędzie od 2022 r. *Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji* nie została zaktualizowana, pomimo, że zmianie uległa podstawa prawna opracowania tej procedury. Jako podstawę prawną dokumentu wskazano bowiem 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[21], które straciło moc 23 maja 2024 r., po wejściu w życie Rozporządzenia KRI.

3) W działaniu *W Jednostce polityki odtwarzania są aktualizowane,* w ramach obszaru *Odtwarzanie (OD),* wskazano stan obecny jako TAK.

Wójt wyjaśnił, że podstawą wskazania TAK w ankiecie było stosowanie w Urzędzie procesu okresowego odtwarzania i weryfikowania baz danych, zgodnie z Procedurą określoną w załączniku do Instrukcji Zarządzania Systemem Informatycznym.

Zdaniem NIK wskazane w ankiecie działanie odnosi się do aktualizacji posiadanych procedur, nie samego faktu dokonywania odtwarzania baz danych systemów informatycznych.

Ponadto w wyjaśnieniach do działań w zakresie obszaru Systemu Zarządzania Bezpieczeństwem Informacji, jako podstawę uzasadniającą stan obecny Wójt wskazał obowiązujące w Urzędzie Politykę ochrony danych osobowych i Instrukcję Zarządzania Systemem Informatycznym. Z ustaleń kontroli wynika, że dokumenty te odnoszą się wyłącznie do danych osobowych i nie stanowią Systemu Zarządzania Bezpieczeństwem Informacji, który nie został wdrożony.

(akta kontroli str.: 473-481, 584-595, 861-885; CD pliki: 028-038, 144)

[21] Dz. U. z 2017 r. poz. 2247.

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. Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.
2. Zapewnienie wypełniania obowiązku w zakresie informacji i promocji zgodnie z wymogami określonymi w Podręczniku.
3. Zapewnienie, przy rozliczeniu Projektu, zgodności informacji zawartych w Ankiecie Dojrzałości ze stanem faktycznym.

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 NIK. 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

Marcin Grochal

Główny specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Departament Administracji Publicznej

p.o. Dyrektor

Bogdan Skwarka

/podpisano elektronicznie/