



NAJWYŻSZA IZBA KONTROLI

Delegatura we Wrocławiu

LWR.410.14.3.2025

**Pan
Zbigniew Tur
Wójt Gminy Kłodzko

Urząd Gminy Kłodzko
ul. Stefana Okrzei 8A
57-300 Kłodzko**

WYSTĄPIENIE POKONTROLNE

P/25/003–„Realizacja projektu Cyberbezpieczny Samorząd”

III. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy Kłodzko ¹ , ul. Stefana Okrzei 8A, 57-300 Kłodzko.
Kierownik jednostki kontrolowanej	Zbigniew Tur, Wójt Gminy Kłodzko ² , od 21 listopada 2018 r.
Zakres przedmiotowy kontroli	Realizacja przez gminy i powiaty działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych w 2025 r. ³
Podstawa prawna podjęcia kontroli	Artykuł 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli ⁴ .
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura we Wrocławiu
Kontrolerzy	Waldemar Zimoch, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/92/2025 z dnia 7 maja 2025 r. Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/131/2025 z dnia 19 maja 2025 r.

(akta kontroli: tom I, str. 1-10)

¹ Dalej: Urząd.

² Dalej: Wójt.

³ Czynności kontrolne zakończono 18 sierpnia 2025 r.

⁴ Dz. U. z 2022 r. poz. 623; dalej: ustawa o NIK.

I. Ocena ogólna⁵ kontrolowanej działalności

OCENA OGÓLNA

Gmina Kłodzko⁶, w okresie objętym kontrolą, zwiększyła poziom cyberbezpieczeństwa, w tym w ramach realizacji projektu Cyberbezpieczny Samorząd⁷, w ramach Urzędu oraz Ośrodka Pomocy Społecznej Gminy Kłodzko⁸. Na podkreślenie przy tym zasługuje szybka i sprawna realizacja Projektu, która trwała niespełna dziewięć miesięcy.

W Urzędzie rozpoznano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa oraz zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu. Przyjęto także i osiągnięto adekwatne mierniki wskaźników produktu w tym Projekcie. Wypełniono *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego*⁹ i przekazano je do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego¹⁰ z zachowaniem terminu i formy, określonych w umowie o powierzenie grantu. W ramach tej umowy Gmina otrzymała dofinansowanie na realizację Projektu w kwocie 850 000,00 zł i poniosła wydatki z tego tytułu w wysokości 846 615,24 zł. Dotyczyły one nabycia wraz z wdrożeniem sprzętu informatycznego i oprogramowania, zakupu i montażu agregatu prądotwórczego, przeprowadzenia wstępnych i końcowych audytów bezpieczeństwa, szkoleń dla kadry informatycznej oraz innych pracowników, a także opracowania i aktualizacji dokumentacji SZBI. Wydatki te zostały zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków.

Urząd zaktualizował także SZBI, który spełnił wymogi § 19 ust. 1 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 teleinformatycznych¹¹. Przeprowadzono także wymagane okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji.

Jednakże Urząd nie zabezpieczył właściwie swoich interesów w jednym z prowadzonych postępowań, nie formułując wymogu posiadania przez wykonawców/oferentów dwuletniego doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących oraz wzmacniających świadomość cyberzagrożeń, tj. wymogu dla uznania wydatków za kwalifikowalne wynikającego z § 4 pkt 7 ppkt d Regulaminu Konkursu Grantowego pn. "Cyberbezpieczny Samorząd"¹², co było działaniem nierzetelnym.

Stwierdzono także brak adekwatnych zabezpieczeń pomieszczenia serwerowni Urzędu, co było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI oraz nieprawidłowe ustawienie monitorów w Biurze Obsługi Mieszkańców, co

⁵ Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

⁶ Dalej: Gmina.

⁷ Dalej: Projekt.

⁸ Dalej: OPS.

⁹ Dalej: Ankiety.

¹⁰ Dalej: NASK.

¹¹ Dz. U. poz. 773; dalej rozporządzenie KRI.

¹² Dalej: Regulamin Projektu.

naruszało § 19 ust. 2 pkt 7 rozporządzenia KRI. Obie te nieprawidłowości zostały usunięte w toku prowadzonej kontroli.

II. Opis ustalonego stanu faktycznego kontrolowanej działalności

OBSZAR Realizacja przez gminy i powiaty działań w celu zwiększenia poziomu cyberbezpieczeństwa

Opis stanu
faktycznego

1. W okresie objętym kontrolą brak było dokumentów o charakterze strategicznym i planistycznym Gminy, jak i Urzędu, w których zostały wprost uwzględnione zagadnienia dotyczące zwiększenia poziomu cyberbezpieczeństwa.

Według wyjaśnień Wójta kwestie cyberbezpieczeństwa stanowią aspekt organizacyjny funkcjonowania samorządu terytorialnego, który nie jest przedmiotem opracowań strategicznych. Wskazał przy tym, że w kilku punktach Strategii rozwoju Gminy Kłodzko na lata 2022-2030¹³ znajdują się jednak zagadnienia dotyczące rozwoju technologii informacyjno-komunikacyjnych, których elementem jest cyberbezpieczeństwo.

(akta kontroli: tom I, str. 11-152, 232-233)

2. Określenie potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa nastąpiło na podstawie audytów bezpieczeństwa informatycznego przeprowadzonych corocznie w Urzędzie. Na ich podstawie zdiagnozowano m.in. potrzeby podniesienia i wzmocnienia kompetencji kadr w zakresie bezpieczeństwa zasobów cyfrowych oraz podniesienia jakości i ilości technicznych zabezpieczeń. Według wyjaśnień Wójta, podstawą do zaplanowania wydatków na zwiększenie poziomu bezpieczeństwa cyfrowego ujętych we wniosku o przyznanie grantu był audyt przeprowadzony w 2022 r. Udział w opracowaniu tych potrzeb i wniosku mieli: Sekretarz Gminy Kłodzko, Referat Organizacyjny (Informatyk) i Referat Rozwoju Lokalnego.

(akta kontroli: tom I, str. 234-397)

3. Urząd w dniu 7 maja 2024 r.¹⁴ przekazał do NASK wypełnione Ankiety dotyczące Urzędu oraz OPS. Dokumenty te przesłano za pośrednictwem wskazanej w umowie o powierzenie grantu skrytki ePUAP należącej do NASK.

(akta kontroli: tom I, str. 199-231; tom III, str. 10-11)

4. W dniu 25 marca 2024 r. Gmina podpisała z Centrum Projektów Polska Cyfrowa¹⁵ umowę o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0245/FERC.02.02-CS.01-001/23/2024¹⁶. Przedmiotem umowy było dofinansowanie na realizację Projektu w wysokości 850 000,00 zł, z czego 83% pochodziło ze środków Unii Europejskiej, a 17% ze środków budżetu państwa¹⁷. Całkowitą kwotę dofinansowania Gmina otrzymała jednorazowo 17 maja 2024 r., kierując do CPPC w dniu 12 kwietnia 2024 r. wniosek o jednorazową

¹³ Przyjętej Uchwałą Rady Gminy Kłodzko Nr 432/VIII/2022 z dnia 29 września 2022 r.

¹⁴ Ankieta przesyłana na początek realizacji projektu Cyberbezpieczny Samorząd.

¹⁵ Dalej: CPPC.

¹⁶ Dalej: umowa o powierzeniu grantu.

¹⁷ Bez udziału własnego Gminy. Podatek VAT był kosztem niekwalifikowalnym, ponoszonym przez Gminę.

wypłatę dofinansowania¹⁸. Jako uzasadnienie tego wniosku wskazano na chęć optymalizacji wykorzystania środków finansowych i kompleksowej realizacji zadań Projektu. Okres kwalifikowalności wydatków w ramach Projektu rozpoczął się 1 czerwca 2023 r. i zakończy się 30 czerwca 2026 r. Przewidziano także utrzymanie środków trwałych i usług nabytych w ramach Projektu przez okres minimum dwóch lat od jego zakończenia.

Środki pozyskane w ramach tego grantu według wniosku o jego przyznanie miały zostać przeznaczone na realizację zadań w następujących obszarach:

- organizacyjnym, na który przeznaczono 47 000,00 zł na przeprowadzenie audytu zgodności z rozporządzeniem KRI i ustawą z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa¹⁹ w Urzędzie i w OPS oraz na aktualizację dokumentacji SZBI w Urzędzie i wykonanie takiej dokumentacji w OPS,
- kompetencyjnym, na który przeznaczono 22 000,00 zł na przeprowadzenie szkoleń specjalistycznych dla pracowników oraz kadry informatycznej,
- technicznym, na który przeznaczono 781 000,00 zł na zakup i wdrożenie: urządzeń UTM²⁰, przełączników sieciowych, serwerów wirtualizacyjnych²¹, serwerów backup, systemów do zarządzania aktualizacjami aplikacji na komputerach PC, macierzy NAS²², oprogramowania bazodanowego, serwerowego systemu operacyjnego, przełączników i kontrolerów FC²³, system do monitorowania infrastruktury informatycznej oraz zakup i montaż agregatu prądotwórczego.

(akta kontroli: tom I, str. 153-198, 668-669, 730-738)

Gmina zakończyła realizację Projektu w 2024 r., wydając łącznie na ten cel 1 039 979,75 zł, z czego koszty kwalifikowalne wyniosły 846 615,24 zł²⁴. Niewykorzystaną kwotę grantu w wysokości 3 384,76 zł zwrócono na konto NASK w dniu 30 grudnia 2024 r.²⁵ Udział wydatków poniesionych na urządzenia oraz oprogramowanie wyniósł 93,81% ogółu kwalifikowalnych wydatków Projektu²⁶.

Urząd w dniu 10 lutego 2025 r. przekazał do NASK „Wniosek rozliczający zaliczkę w ramach Programu Cyberbezpieczny Samorząd”, wypełniając wymóg wynikający z § 5 ust. 2 i 3 umowy o powierzenie grantu. Natomiast w dniu 16 kwietnia 2025 r. wpłynęła do Urzędu informacja z NASK o akceptacji przedłożonego wniosku rozliczającego.

¹⁸ Zgodnie z możliwością wynikającą z § 2 ust. 8 umowy o powierzeniu grantu.

¹⁹ Dz. U z 2024 r. poz. 1077, ze zm.

²⁰UTM (Unified Threat Management) - zintegrowane rozwiązanie do zarządzania zagrożeniami, które umożliwia ochronę sieci.

²¹ Serwer wirtualizacyjny to fizyczny serwer, który za pomocą oprogramowania (hiperwizora) jest podzielony na kilka wirtualnych maszyn. Każda z tych maszyn działa jak niezależny serwer, z własnym systemem operacyjnym i aplikacjami, mimo że współdzieli zasoby jednego fizycznego komputera.

²² NAS (Network Attached Storage) – serwer umożliwiający użytkownikom w łatwy sposób przechowywanie, udostępnianie i zarządzanie danymi z dowolnego miejsca w sieci lokalnej lub zdalnej.

²³ Urządzenia i oprogramowanie, które służy do budowania i zarządzania siecią, pozwalając na szybkie i niezawodne połączenie serwerów z urządzeniami pamięci masowej.

²⁴ Koszty niekwalifikowalne w całości stanowił podatek VAT.

²⁵ Na rachunek, z którego Gmina otrzymała kwotę grantu.

²⁶ 794 211,99 zł z 846 615,24 zł ogółem.

Realizowane działania w ramach przyznanego grantu polegały na:

- przeprowadzeniu audytu wstępnego bezpieczeństwa informacji w Urzędzie i OPS. Wykonawca został wybrany w ramach postępowania „Wykonanie w Urzędzie Gminy Kłodzko i Ośrodku Pomocy Społecznej Gminy Kłodzko audytu cyberbezpieczeństwa, bezpieczeństwa informacji i danych osobowych”. Postępowanie zostało przeprowadzone zgodnie z regulacjami wewnętrznymi o wartości poniżej 130 000,00 zł. Zostało ono wszczęte 19 października 2023 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 8 900,00 zł netto²⁷ w dniu 26 października 2023 r.
- aktualizacji istniejącej dokumentacji SZBI w Urzędzie, opracowaniu dokumentacji SZBI dla OPS oraz przeprowadzeniu szkoleń dla pracowników tych jednostek, w tym informatyków. Wykonawca został wybrany w ramach postępowania >>Wykonanie dla Urzędu Gminy Kłodzko aktualizacji istniejącej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Ośrodka Pomocy Społecznej Gminy Kłodzko oraz zorganizowanie i przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach realizacji zadania współfinansowanego z programu „Cyberbezpieczny Samorząd” pod nazwą „Cyberbezpieczna Gmina Kłodzko”<<. Postępowanie przeprowadzono zgodnie z regulacjami wewnętrznymi o wartości poniżej 130 000 zł. Zostało ono wszczęte w dniu 28 czerwca 2024 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 34 103,25 zł netto²⁸ w dniu 10 lipca 2024 r.²⁹.

W postępowaniu tym w umowie i specyfikacji warunków zamówienia dla zapytania ofertowego nie zawarto wymogu spełniania kryterium dwuletniego doświadczenia w przeprowadzaniu przez wykonawcę/oferentów szkoleń z zakresu cyberbezpieczeństwa, co opisano w sekcji *Stwierdzone nieprawidłowości*,

- zakupie agregatu prądotwórczego dla Urzędu. Wykonawca został wybrany w ramach postępowania „Zakup agregatu prądotwórczego wraz z dostawą i montażem w ramach projektu Cyberbezpieczna Gmina Kłodzko. Postępowanie przeprowadzono zgodnie z regulacjami wewnętrznymi o wartości poniżej 130 000 zł. Zostało ono wszczęte w dniu 19 lipca 2024 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 125 250,00 zł netto³⁰ w dniu 23 sierpnia 2024 r.³¹,
- zakupie sprzętu informatycznego i oprogramowania dla Urzędu i OPS³². Wykonawca został wybrany w ramach postępowania >>Zakup sprzętu i oprogramowania wraz z wdrożeniem w ramach realizacji zadania współfinansowanego z programu „Cyberbezpieczny Samorząd” pod nazwą

²⁷ 10 947,00 zł brutto.

²⁸ 40 590,00 zł brutto.

²⁹ W dniu 26 września 2024 r. zawarto aneks wydłużający czas realizacji umowy do czterech miesięcy od zawarcia umowy (z trzech miesięcy), bez zmiany pozostałych warunków.

³⁰ 154 057,50 zł brutto.

³¹ W dniu 30 października 2024 r. zawarto aneks wydłużający termin realizacji umowy do 30 listopada 2024 r. (z 30 października 2024 r.), bez zmiany pozostałych warunków.

³² W postaci: dwóch UTM (dla Urzędu i OPS), przełącznika sieciowego dla Urzędu, serwera wirtualizacyjnego do Urzędu, serwera backup dla Urzędu, serwera dla OPS, systemu do zarządzania aktualizacjami aplikacji na komputerach PC dla Urzędu, macierzy NAS dla Urzędu, dwóch oprogramowań bazodanowych dla Urzędu, dwóch przełączników FC dla Urzędu, dwóch kontrolerów FC dla Urzędu, systemu do monitorowania infrastruktury informatycznej.

„Cyberbezpieczna Gmina Kłodzko”<<. Postępowanie to zostało przeprowadzone w trybie art. 175 ust. 1 ustawy z 11 września 2019 r. – Prawo zamówień publicznych³³, zgodnie z obowiązującymi przepisami PZP. Postępowanie to wszczęto 23 maja 2024 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 639 800,00 zł netto³⁴ w dniu 17 czerwca 2024 r.

- przeprowadzeniu audytu końcowego bezpieczeństwa informacji w Urzędzie i OPS. Wykonawca został wybrany w ramach postępowania „Wykonanie w Urzędzie Gminy Kłodzko i Ośrodku Pomocy Społecznej Gminy Kłodzko audytu cyberbezpieczeństwa, bezpieczeństwa informacji i danych osobowych”. Postępowanie zostało przeprowadzone zgodnie z regulacjami wewnętrznymi o wartości poniżej 130 000,00 zł. Zostało ono wszczęte 31 października 2024 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 9 400,00 zł netto³⁵ w dniu 12 listopada 2024 r.
- zakupie dwóch UPS oraz macierzy dyskowej NAS dla OPS. Wykonawca został wybrany w ramach postępowania >>Dostawa sprzętu wraz z konfiguracją dla Ośrodka Pomocy Społecznej Gminy Kłodzko w ramach realizacji zadania współfinansowanego z programu „Cyberbezpieczny Samorząd” pod nazwą „Cyberbezpieczna Gmina Kłodzko”<<. Postępowanie zostało przeprowadzone zgodnie z regulacjami wewnętrznymi o wartości poniżej 130 000,00 zł. Zostało ono wszczęte 8 listopada 2024 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 20 000,00 zł³⁶ w dniu 22 listopada 2024 r.,
- zakupie dla OPS przełącznika sieciowego o wartości 7 817,99 zł netto³⁷ oraz oprogramowania antywirusowego o wartości 1 344,00 zł netto³⁸ w dniu 20 grudnia 2024 r.

(akta kontroli: tom I, str. 153, 198, 671-675, 734-738; tom II, str. 1-760; tom III, str. 12-34)

5. W realizacji Projektu przewidziano także udział OPS. Podstawowym kryterium udziału tej jednostki w Projekcie było przetwarzanie przez nią danych wrażliwych, które wymagają szczególnej ochrony. W związku z tym, zdaniem Wójta, niezbędnym było podjęcie działań wpływających na podniesienie bezpieczeństwa infrastruktury informatycznej OPS, w tym serwerów, a także wdrożenie odpowiednich procedur i środków organizacyjnych. Potrzeby w tym zakresie zostały oszacowane przez sporządzający wniosek o przyznanie grantu Urząd w uzgodnieniu z OPS.

Wartość Projektu dla tej jednostki wyniosła 171 925,10 zł, z czego 139 776,50 zł stanowiły koszty kwalifikowalne³⁹. W ramach tego Projektu w OPS przeprowadzono audyty wstępny i końcowy z zakresu bezpieczeństwa informacji, opracowano dokumentację SZBI oraz przeszkolono pracowników tej jednostki z zakresu cyberbezpieczeństwa.

³³ Dz. U. z 2024 r. poz. 1320, ze zm.; dalej: PZP.

³⁴ 786 954,00 zł brutto.

³⁵ 11 562,00 zł brutto.

³⁶ 24 600,00 zł brutto.

³⁷ 9 616,13 zł brutto.

³⁸ 1 653,12 zł brutto.

³⁹ Pozostałe koszty stanowił podatek VAT.

Ponadto zakupiono i wdrożono następujący sprzęt oraz oprogramowanie:

- urządzenie UTM,
- przełącznik sieciowy,
- serwer,
- serwer NAS,
- urządzenie UPS,
- dwa urządzenia UPS,
- oprogramowanie antywirusowe.

Realizacja Projektu w OPS wpłynęła na podniesienie bezpieczeństwa informatycznego poprzez doposażenie sprzętowe, zwiększenie świadomości pracowników w tym zakresie oraz opracowanie i przyjęcie procedur w tym zakresie w postaci SZBI.

(akta kontroli: tom I, str. 153-199; tom II, str. 1-760; tom III, str. 17-34)

6. Do realizacji zadań związanych z realizacją Projektu w Urzędzie wyznaczeni zostali Sekretarz Gminy Kłodzko, Informatyk i Kierownik Referatu Rozwoju Lokalnego. Wynikało to z wewnętrznych ustaleń i miało odzwierciedlenie w aktualnych zakresach ich czynności oraz w posiadanych kompetencjach.

(akta kontroli: tom I, str. 334-397)

7. W trakcie przygotowania i realizacji Projektu w Urzędzie nie doszło do fluktuacji kadr zajmujących się tymi zagadnieniami.

(akta kontroli: tom I, str. 334-397)

8. We wniosku o przyznanie grantu Gmina określiła następujące wskaźniki produktu i rezultatu Projektu:

- dwóch pracowników IT objętych wsparciem szkoleniowym,
- 90 pracowników⁴⁰ Urzędu i OPS objętych wsparciem szkoleniowym,
- dwa systemy w zakresie zwiększenia bezpieczeństwa informacji Urzędu i OPS.

Przyjęte wskaźniki były adekwatne do planowanych działań zapisanych we wniosku o przyznanie grantu oraz są zgodne z załącznikiem nr 9 do Regulaminu Konkursu Grantowego - Opis wskaźników projektu Cyberbezpieczny Samorząd.

Na dzień zakończenia czynności kontrolnych wszystkie te wskaźniki zostały w pełni zrealizowane.

(akta kontroli: tom I, str. 188, 671-675, 714-729; tom III, str. 17-34)

9. W ramach realizacji Projektu w Urzędzie wykonano wstępny i końcowy audyt bezpieczeństwa informacji, dokonano aktualizacji dokumentacji SZBI, dwóch informatyków Urzędu przeszło szkolenia specjalistyczne dla IT, a pracownicy Urzędu szkolenie z zakresu cyberbezpieczeństwa.

Ponadto dokonano zakupu i wdrożenia następujących urządzeń oraz oprogramowania, zwiększających poziom bezpieczeństwa informatycznego, w postaci:

- urządzenia UTM,

⁴⁰W tym 70 kobiet i 20 mężczyzn.

- przełącznika sieciowego,
- serwera wirtualizacyjnego wraz z systemem operacyjnym,
- serwera backupu,
- systemu do zarządzania aktualizacjami aplikacji na komputerach PC,
- macierzy NAS,
- oprogramowania bazodanowego,
- agregatu prądotwórczego,
- serwerowego oprogramowania operacyjnego,
- dwóch przełączników i kontrolerów FC,
- systemu monitorowania infrastruktury informatycznej.

Łączna wartość Projektu dla Urzędu wyniosła 868 054,65 zł, z czego koszty kwalifikowalne wyniosły 706 838,74 zł⁴¹.

(akta kontroli: tom I, str. 153-199; tom II, str. 1-760; tom III, str. 17-34)

Według wyjaśnień złożonych przez Wójta, na zakupionych w ramach Projektu serwerach i macierzach nie zainstalowano i nie jest przewidywane do zainstalowania żadne oprogramowanie dziedzinowe. Wyjaśnił także, że poprzez zakup oprogramowania bazodanowego zapewniono mechanizmy bezpieczeństwa dla baz danych w kontekście prewencji detekcji i reagowania. Zakupione oprogramowanie obsługuje bowiem mechanizmy kryptograficzne i inne mechanizmy podnoszące poziom bezpieczeństwa przetwarzania danych w bazach.

(akta kontroli: tom III, str. 17-18)

10. Realizacja Projektu w Urzędzie poprawiła poziom bezpieczeństwa informatycznego poprzez aktualizację procedur wchodzących w skład dokumentacji SZBI, zwiększenie świadomości pracowników w zakresie cyberbezpieczeństwa oraz doposażenie w urządzenia i oprogramowanie pozwalające zwiększyć poziom odporności jednostki na zagrożenia związane z cyberbezpieczeństwem.

W celu realizacji obowiązku wynikającego z § 13 umowy o powierzenie grantu, przyjęto procedury monitorowania utrzymania efektów Projektu⁴². Polegały one na cyklicznym gromadzeniu informacji w zakresie utrzymania środków trwałych i usług nabytych w ramach Projektu przez okres minimum dwóch lat od jego zakończenia, począwszy od I kwartału 2026 r. Systemowi monitorowania podlegać będą także elementy z obszaru organizacyjnego, kompetencyjnego oraz technicznego, dla których we wniosku o przyznanie grantu określono wskaźniki.

(akta kontroli: tom II, str. 89; tom III, str. 17-39)

11. Urząd posiadał SZBI spełniający wymagania § 19 ust. 1 rozporządzenia KRI. Dokumentacja ta powstała poprzez aktualizację dotychczas obowiązującej⁴³, jako produkt Projektu wykonany przez firmę zewnętrzną.

⁴¹ Pozostałe koszty (niekwalifikowalne) stanowił podatek VAT.

⁴² Zarządzenie Nr 264/2025 Wójta Gminy Kłodzko z dnia 25 marca 2025 r. w sprawie wprowadzenia Procedury monitorowania utrzymania efektów Projektu pn. Cyberbezpieczna Gmina Kłodzko.

⁴³ Instrukcja Zarządzania Systemem Informatycznym, wprowadzona zarządzeniem 604/2020 Wójta Gminy Kłodzko z dnia 8 listopada 2020 r., zmieniona zarządzeniem nr 1112/2022 Wójta Gminy

SZBI wprowadzono Zarządzeniem 206/2025 Wójta Gminy Kłodzko z dnia 3 stycznia 2025 r., a wchodziły w jego skład następujące elementy:

- Polityka Bezpieczeństwa Informacji⁴⁴,
- Polityka Ochrony Danych Osobowych⁴⁵,
- Instrukcja Zarządzania Systemem Informatycznym,
- Polityka kluczy;
- Procedura zarządzania zmianą, ryzykiem i oceną skutków.

PBI została ustanowiona nadrzędnym dokumentem SZBI i zawierała zasady bezpieczeństwa informacji obowiązujące w Urzędzie oraz odwołania do innych dokumentów wewnętrznych uszczegóławiających. Za wdrożenie i zapewnienie przestrzegania PBI odpowiadał Wójt, a wyznaczony przez niego Administrator Bezpieczeństwa Systemów Informatycznych odpowiadał za zapewnienie, że procedury i systemy informatyczne stosowane w Urzędzie spełniają wymagania obowiązujących przepisów prawa oraz zapewniają bezpieczeństwo przetwarzanych danych osobowych. PBI została zatwierdzona i przedstawiona do zapoznania się i stosowania wszystkim pracownikom.

PODO natomiast regulowała organizację ochrony danych, postępowanie z upoważnieniami do przetwarzania danych osobowych, zakres prowadzenia analizy ryzyka w ochronie danych osobowych, środki organizacyjne i techniczne zabezpieczające dane osobowe, postępowanie w przypadku naruszeń ochrony danych osobowych, rolę i status inspektora danych osobowych, audyty ochrony danych osobowych, przywracanie dostępności danych osobowych, postępowanie dyscyplinarne w przypadku naruszenia ochrony danych osobowych, zakres szkoleń z ochrony danych osobowych oraz procedury szczegółowe dotyczące obszaru ochrony danych osobowych.

Instrukcja zarządzania systemem informatycznym, określała procedury dotyczące zasad pracy i zachowania bezpieczeństwa w systemach informatycznych wykorzystywanych w Urzędzie, dotyczyły one:

- zarządzania uprawnieniami,
- rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu informatycznego,
- zabezpieczenia systemów informatycznych,
- aktualizacji oprogramowania,
- zabezpieczania przed działaniem złośliwego oprogramowania,
- kopii bezpieczeństwa,
- zasad przechowywania i niszczenia cyfrowych nośników informacji zawierających dane chronione,
- zabezpieczenia komputerów przenośnych i zewnętrznych nośników danych, pracy poza obszarem przetwarzania danych Urzędu oraz pracy zdalnej,

Kłodzko z dnia 24 sierpnia 2022 r., zarządzeniem nr 1268/2023 Wójta Gminy Kłodzko z dnia 18 stycznia 2023 r., zarządzeniem nr 1467/2023 z 14 listopada 2023 r. oraz Polityka Ochrony Danych Osobowych Urzędu Gminy Kłodzko, przyjęta zarządzeniem nr 603/2020 Wójta Gminy Kłodzko z dnia 8 listopada 2020 r., zmieniona zarządzeniem nr 955/2022 Wójta Gminy Kłodzko z 1 marca 2022 r.,

⁴⁴ Dalej: PBI.

⁴⁵ Dalej: PODO.

- określenia zasad zabezpieczania oraz wykonywania przeglądów, konserwacji i napraw sprzętu i systemów służących do przetwarzania danych,
- postępowania w zakresie komunikacji sieciowej,
- pracy w godzinach nadliczbowych,
- obsługi incydentów,
- zintegrowanego zarządzania systemem teleinformatycznym,
- zarządzania hasłami, w tym administracyjnymi,
- kontroli dostępu oraz dostępu zdalnego i przetwarzania mobilnego,
- planu ciągłości działania.

Dokumenty składające się na SZBI zostały zatwierdzone i zakomunikowane pracownikom Urzędu odpowiedzialnym za realizację zadań, określonych tymi dokumentami.

(akta kontroli: tom I, str. 398-665)

Serwerownia Urzędu zlokalizowana była w odrębnym i klimatyzowanym pomieszczeniu, do którego dostęp mieli informatycy. Niemniej, pomieszczenie to nie posiadało należytych zabezpieczeń, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: tom I, str. 670; tom III, str. 1-9)

Ustawienie monitorów w Biurze Obsługi Mieszkańców umożliwiała nieuprawniony dostęp do informacji, co opisano w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: tom III, str. 1-9)

12. Dokumentacja składająca się na SZBI była na bieżąco aktualizowana i w razie potrzeby doskonalona. Była ona poddawana okresowym przeglądom, głównie na podstawie wyników okresowych audytów wewnętrznych oraz zachodzących zmian. Dotyczyło to szczególnie dokumentacji obowiązującej przed aktualizacją SZBI, która miała miejsce w styczniu 2025 r.

W wyniku przeprowadzonych audytów zidentyfikowano także potrzebę kompleksowej aktualizacji obowiązującej dokumentacji SZBI, którą wykonała, w ramach Projektu, zewnętrzna firma.

(akta kontroli: tom I, str. 233-235, 398-518)

13. W okresie objętym kontrolą w Urzędzie przeprowadzono dwa audyty wewnętrzne w zakresie bezpieczeństwa informacji⁴⁶, co wypełniało wymogi wynikające z § 19 ust. 2 pkt 14 rozporządzenia KRI.

Audyt wewnętrzny z zakresu bezpieczeństwa informacji za 2024 r., mający charakter końcowego w realizowanym Projekcie, wykonywała firma zewnętrzna posiadająca niezbędne kompetencje w tym zakresie. Badanie audytowe obejmowało ocenę spełnienia wymagań § 19 rozporządzenia KRI. W zakresie dotyczącym SZBI nie formułowano w nim rekomendacji, podkreślając zauważalny wzrost poziomu spełniania wymogów przez Urząd.

(akta kontroli: tom I, str. 236-343)

⁴⁶ Przeprowadzone 2-3 listopada 2023 r. oraz 13 listopada 2024 r.

14. Do dnia zakończenia czynności kontrolnych prowadzone działania informacyjne i promocyjne, w związku z realizacją Projektu przez Urząd i OPS polegały na:

- oznaczeniu znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich plakatów w budynkach oraz informacji na stronie internetowej i w mediach społecznościowych, a także dokumentów związanych z realizacją Projektu, w tym dotyczących postępowań o zamówienia publiczne oraz oznaczeń na zakupionym sprzęcie;
- umieszczeniu plakatów w formacie A3 w siedzibie Urzędu oraz OPS;
- umieszczeniu opis Projektu na stronie internetowej oraz mediach społecznościowych Urzędu i OPS;
- oznakowaniu zakupionych urządzeń.
- bieżącym dokumentowaniu działań informacyjnych i promocyjnych prowadzonych w ramach Projektu.

(akta kontroli: tom I str. 691-713)

Stwierdzone
nieprawidłowości

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

1. Urząd nie zabezpieczył właściwie swoich interesów w prowadzonym postępowaniu o zamówienie publiczne pn. >>Wykonanie dla Urzędu Gminy Kłodzko aktualizacji istniejącej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Ośrodka Pomocy Społecznej Gminy Kłodzko oraz zorganizowanie i przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa w ramach realizacji zadania współfinansowanego z programu „Cyberbezpieczny Samorząd” pod nazwą „Cyberbezpieczna Gmina Kłodzko”<<. W postępowaniu tym nie sformułowano bowiem wymogu posiadania przez wykonawców/oferentów dwuletniego doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących oraz wzmacniających świadomość cyberzagrożeń, tj. wymogu dla uznania wydatków za kwalifikowalne wynikającego z § 4 pkt 7 ppkt d Regulaminu Projektu, co było działaniem nierzetelnym.

Wójt wyjaśnił, że w ramach tego postępowania zamawiający poinformował potencjalnych oferentów o realizacji zadania w ramach Projektu, a załącznikiem do formularza ofertowego było oświadczenie oferenta. W tym oświadczeniu deklarował on posiadanie uprawnień lub kompetencji wynikających z odrębnych przepisów, przez co zdaniem Wójta, należy także rozumieć posiadanie odpowiedniego doświadczenia opisanego w regulaminie tego konkursu grantowego. Do wyjaśnień dołączył także oświadczenie firmy oraz dokumenty potwierdzające spełnianie przez nią wymogów w zakresie doświadczenia.

NIK wskazuje, że zasady kwalifikowalności wydatków Projektu są skierowane do zamawiającego, a nie do wykonawcy. Nie stanowią więc dla niego punktu odniesienia do deklarowania posiadania uprawnień lub kompetencji wynikających z odrębnych przepisów. W przypadku braku wymaganego doświadczenia umowy o zamówienie publiczne mogłyby być wprowadzone wykonane właściwie i z należytą starannością przez wykonawców, lecz ich koszt stanowiłby wydatek niekwalifikowalny Projektu i w całości obciążałby Gminę. Zatem ustanowienie takiego wymogu leżało w interesie Gminy by maksymalnie

wykorzystać środki zewnętrzne otrzymane na realizację Projektu i nie angażować własnych.

(akta kontroli: tom I, str. 669-670, 739-743; tom II, str. 1-90)

2. W pomieszczeniu serwerowni Urzędu brak było adekwatnych zabezpieczeń⁴⁷, co stwarzało potencjalne zagrożenie włamania i narażenia na zniszczenie lub nieuprawniony dostęp do aktywów informacyjnych i było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI.

Wójt przyznał, że serwerownia była nieadekwatnie zabezpieczona, a w czasie kontroli dokonano poprawy i montażu nowych zabezpieczeń, które usunęły stwierdzone nieprawidłowości.

(akta kontroli: tom I, str. 670; tom III, str. 1-9)

3. Ustawienie monitorów w Biurze Obsługi Mieszkańców umożliwiało nieuprawniony dostęp do informacji (w tym danych osobowych), co było niezgodne § 19 ust. 2 pkt 7 rozporządzenia KRI.

Wójt w złożonych wyjaśnieniach przekazał informację o montażu filtrów prywatyzujących na te monitory, przez co wyeliminował stwierdzoną nieprawidłowość.

(akta kontroli: tom III, str. 10-11)

III. Uwagi i wnioski

Uwzględniając podjęte w trakcie kontroli działania oraz zakończenie realizacji Projektu, Najwyższa Izba Kontroli nie formułuje uwag ani wniosków.

⁴⁷ O szczegółach Wójt został powiadomiony i udzielił na nie odpowiedzi pismem z 11 czerwca 2025 r. (pkt 5).

IV. 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 Delegatury NIK we Wrocławiu. 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.

Wrocław, 22 sierpnia 2025 r.

Kontroler

Cezary Mazik

Główny specjalista kontroli
państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Delegatura we Wrocławiu

p.o. Dyrektor

Radosław Kujawiński

/podpisano elektronicznie/