



NAJWYŻSZA IZBA KONTROLI

Delegatura we Wrocławiu

LWR.410.14.4.2025

**Pani
Renata Surma
Burmistrz Bystrzycy Kłodzkiej
Urząd Miasta i Gminy
Bystrzyca Kłodzka
Plac Wolności 1
57-500 Bystrzyca Kłodzka**

WYSTĄPIENIE POKONTROLNE

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

III. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta i Gminy w Bystrzycy Kłodzkiej ¹ , Plac Wolności 1, 57-500 Bystrzyca Kłodzka.
Kierownik jednostki kontrolowanej	Renata Surma, Burmistrz Bystrzycy Kłodzkiej ² , od 4 grudnia 2006 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	1. Waldemar Zimoch, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/91/2025 z dnia 7 maja 2025 r. 2. Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/130/2025 z dnia 19 maja 2025 r.

(akta kontroli: tom I, str. 1-5)

¹ Dalej: Urząd.

² Dalej: Burmistrz.

³ Czynności kontrolne zakończono 12 sierpnia 2025 r.

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

I. Ocena ogólna⁵ kontrolowanej działalności

OCENA OGÓLNA

Gmina Bystrzyca Kłodzka⁶ w okresie objętym kontrolą podejmowała działania w celu zwiększenia poziomu cyberbezpieczeństwa, w tym w ramach realizacji projektu Cyberbezpieczny Samorząd⁷.

W Urzędzie zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu. Dla Urzędu oraz siedmiu podległych mu jednostek, biorących udział w tym Projekcie, ustalono adekwatne wskaźniki produktu i rezultatu. Wypełniono *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego*⁸ i przekazano je do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego z zachowaniem terminu i formy, określonych w umowie o powierzenie grantu. W ramach tej umowy Gmina otrzymała dofinansowanie na realizację Projektu w kwocie 849 991,00 zł. Wydatki poniesione przez grantobiorcę w ramach Projektu, w okresie objętym kontrolą, wyniosły 50 061,00 zł i dotyczyły przeprowadzenia wstępnych audytów bezpieczeństwa oraz szkoleń dla kadry informatycznej. Wydatki te zrealizowano zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o przyznanie grantu.

Urząd posiadał także ustanowiony System Zarządzania Bezpieczeństwem Informacji⁹ spełniający 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 teleinformatycznych¹⁰. Jednakże w 2023 r. nie przeprowadzono w Urzędzie okresowego audytu z zakresu bezpieczeństwa informacji, co naruszało z § 19 ust. 2 pkt 14 rozporządzenia KRI.

II. Opis ustalonego stanu faktycznego

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 Gminy, jak i Urzędu, w których zostały wprost uwzględnione zagadnienia dotyczące zwiększenia poziomu cyberbezpieczeństwa. Według wyjaśnień Burmistrz w kilku punktach Strategii rozwoju dla Gminy Bystrzyca Kłodzka na lata 2021-2030¹¹ znajdują się zagadnienia dotyczące rozwoju technologii informacyjno-komunikacyjnych, których elementem jest cyberbezpieczeństwo.

Ponadto w planie działalności Urzędu na 2022 r. ujęto zadanie „wdrożenie zasad cyberbezpieczeństwa w Urzędzie” polegające na dostosowaniu

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: Ankiety.

⁹ Dalej: SZBI.

¹⁰ Dz. U poz. 773; dalej rozporządzenie KRI.

¹¹ Przyjętej Uchwałą Rady Miejskiej Bystrzycy Kłodzkiej Nr LI/423/2021 z dnia 29 grudnia 2021 r.

działalności Urzędu do wymogów ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa¹², a w planach na 2024 r. i 2025 r. realizację Projektu.

(akta kontroli: tom I, str. 9-151; tom II, str. 156-163)

2. Określenie potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa nastąpiło na podstawie audytów bezpieczeństwa informatycznego przeprowadzonych w Urzędzie przez firmę zewnętrzną w 2022 r. oraz formułowanych na ich podstawie raportów zbiorczych dla najwyższego kierownictwa. Według wyjaśnień Burmistrza, z racji zadań przypisanych w regulaminie organizacyjnym Urzędu i zakresach czynności, najbardziej zaangażowane w te zadania były: Wydział Organizacyjno-Prawny oraz Inspektor Ochrony Danych¹³.

(akta kontroli: tom II, str. 154-158, 232-333, 344-377)

3. Urząd w dniu 13 sierpnia 2024 r. przekazał do NASK wypełnione Ankiety. Dokumenty te przesłano za pośrednictwem wskazanej w umowie udostępnienia grantu skrytki ePUAP należącej do NASK. Przedmiotowa wysyłka obejmowała ankiety dotyczące Urzędu oraz siedmiu jednostek podległych uczestniczących w Projekcie¹⁴.

(akta kontroli: tom II, str. 334-343)

4. W dniu 18 lipca 2024 r. Gmina podpisała z Centrum Projektów Polska Cyfrowa¹⁵ umowę o powierzeniu grantu o numerze FERC.02.02-CS.01-001/23/0768/FERC.02.02-CS.01-001/23/2024¹⁶. Przedmiotem umowy było dofinansowanie na realizację Projektu w wysokości 849 991,00 zł, z czego 82% pochodziło ze środków Unii Europejskiej, a 18% ze środków budżetu państwa¹⁷. Całkowitą kwotę dofinansowania pozyskano jednorazowo 27 sierpnia 2024 r., kierując do CPPC w dniu 24 lipca 2024 r. wniosek o jednorazową 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 mają zostać przeznaczone na realizację zadań w następujących obszarach:

- organizacyjnym, na który przeznaczono 36 285,00 zł na przeprowadzenie audytu KRI wstępnego oraz końcowego dla Urzędu oraz siedmiu jednostek podległych uczestniczących w Projekcie,

¹² Dz. U z 2024 r. poz. 1077, ze zm.

¹³ Dalej: IOD.

¹⁴ T.J. Zespół Szkół Ogólnokształcących w Bystrzycy Kłodzkiej, Szkoła Podstawowa nr 2 w Bystrzycy Kłodzkiej, Szkoła Podstawowa w Wilkanowie, Centrum Integracji Społecznej w Bystrzycy Kłodzkiej, Przedszkole nr 2 w Bystrzycy Kłodzkiej, Ośrodek Pomocy Społecznej w Bystrzycy Kłodzkiej oraz Środowiskowy Dom Samopomocy w Bystrzycy Kłodzkiej.

¹⁵ Dalej: CPPC.

¹⁶ Dalej: umowa o powierzeniu grantu.

¹⁷ Bez udziału własnego Gminy. Według informacji przekazanych przez Burmistrza Gmina nie ma możliwości odliczenia VAT, podatek ten więc jest kosztem kwalifikowalnym.

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

- kompetencyjnym, na który przeznaczono 36 803,00 zł na przeprowadzenie szkoleń specjalistycznych dla kadry informatycznej (administratorów),
- technicznym, na który przeznaczono 776 903,00 zł na zakup i wdrożenie: serwera do wykonywania kopii zapasowej z biblioteką taśmową, urządzeń UTM¹⁹, oprogramowania do monitorowania infrastruktury informatycznej, serwerów rack²⁰, serwerów NAS²¹, macierzy dyskowej do replikacji oraz zakup zasilaczy UPS²².

(akta kontroli: tom II, str. 2-57, 190-193)

Realizowane według stanu na 12 sierpnia 2025 r. działania w ramach przyznanego grantu polegały na:

- przeprowadzeniu wstępnego audytu wewnętrznego z zakresu bezpieczeństwa informacji w Urzędzie i siedmiu jednostkach podległych uczestniczących w Projekcie. Wykonawca został wybrany w ramach postępowania >>Wstępny audyt bezpieczeństwa informacji, którego kryterium jest Rozporządzenie 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 (zwanym dalej „Rozporządzeniem KRI”) dla Urzędu Miasta i Gminy Bystrzyca Kłodzka i siedmiu jednostek podległych<<. Postępowanie przeprowadzono zgodnie z regulacjami wewnętrznymi o wartości poniżej 130 000,00 zł. Zostało ono wszczęte w dniu 24 lipca 2024 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 11 000,00 zł netto²³ w dniu 5 sierpnia 2024 r.
- przeszkoleniu dwóch administratorów/informatyków Urzędu z zakresu przełączników sieciowych, UTM, zarządzania infrastrukturą IT oraz zarządzania serwerowym systemem operacyjnym. Wykonawca został wyłoniony w ramach postępowania „Dostawa voucherów na certyfikowane szkolenia w języku polskim dla dwóch administratorów”. Postępowanie przeprowadzono zgodnie z regulacjami wewnętrznymi o wartości poniżej 130 000,00 zł. Zostało ono wszczęte w dniu 27 listopada 2024 r., a zakończyło się podpisaniem umowy z wykonawcą o wartości 29 700,00 zł netto²⁴ w dniu 9 grudnia 2024 r.
- przygotowywaniu i prowadzeniu postępowania o zamówienie publiczne w trybie art. 275 ust. 1 ustawy z 11 września 2019 r. – Prawo zamówień publicznych²⁵ na zakup sprzętu informatycznego w ramach zadania „Zakup i wdrożenie sprzętu informatycznego poprawiającego cyberbezpieczeństwo

¹⁹UTM (Unified Threat Management) - zintegrowane rozwiązanie do zarządzania zagrożeniami, które umożliwia ochronę sieci.

²⁰ Serwery przeznaczone do montażu w szafie serwerowej.

²¹ NAS (Network Attached Storage) – serwer umożliwiający użytkownikom w łatwy sposób przechowywanie, udostępnianie i zarządzanie danymi z dowolnego miejsca w sieci lokalnej lub zdalnej.

²² zasilacz UPS (uninterruptible power supply) – urządzenie lub system, którego funkcją jest utrzymanie zasilania innych urządzeń elektrycznych lub elektronicznych w przypadku zaniku lub nieprawidłowych parametrów zasilania sieciowego.

²³ 13 530,00 zł brutto.

²⁴ 36 531,00 zł brutto.

²⁵ Dz.U z 2024 r. poz.1320, ze zm.

w Urzędzie Miasta i Gminy Bystrzyca Kłodzka oraz w siedmiu jednostkach podległych". W zadaniu tym, w dniu 7 sierpnia 2025 r. dokonano otwarcia ofert²⁶, a okres związania ofertą trwa do 5 września 2025 r.

Zgodnie z § 7 umowy o powierzeniu grantu, w dniu 12 sierpnia 2025 r. Urząd przekazał do CPPC, za pośrednictwem udostępnionego systemu teleinformatycznego, informację o postępie rzeczowym realizacji Projektu.

Do dnia 12 sierpnia 2025 r. wykorzystano jedynie 5,89%²⁷ otrzymanego grantu na Projekt, mimo wpłynięcia jednorazowej transzy grantu na konto Urzędu w dniu 27 sierpnia 2024 r. Ponadto przez prawie rok od otrzymania pełnej kwoty środków finansowych nie rozstrzygnięto jeszcze postępowania o zamówienie publiczne obejmującego zakupu sprzętu przewidzianego we wniosku o przyznaniu grantu.

Burmistrz wyjaśniła, że realizacja zadań Projektu, a w szczególności przetarg na sprzęt informatyczny został przesunięty na późniejszy termin ze względu na zaplanowane zmiany organizacyjno-techniczne w Urzędzie. Wskazała również, że rozliczenie umowy o powierzenie grantu przez Urząd planowane jest do końca 2025 r.

(akta kontroli: tom II, str. 58-151, 195, 378-396)

5. W realizacji Projektu przewidziano udział siedmiu podległych Urzędowi jednostek, tj.: Zespołu Szkół Ogólnokształcących w Bystrzycy Kłodzkiej²⁸, Szkoły Podstawowej nr 2 w Bystrzycy Kłodzkiej²⁹, Szkoły Podstawowej w Wilkanowie³⁰, Centrum Integracji Społecznej w Bystrzycy Kłodzkiej³¹, Przedszkola nr 2 w Bystrzycy Kłodzkiej³², Ośrodka Pomocy Społecznej w Bystrzycy Kłodzkiej³³ oraz Środowiskowego Domu Samopomocy w Bystrzycy Kłodzkiej³⁴. Podstawowym kryterium dołączenia tych jednostek do Projektu była chęć zwiększenia ich cyberbezpieczeństwa. Jednostki te spełniały wymogi formalne oraz zostały także objęte audytem zewnętrznym w 2022 r. w zakresie bezpieczeństwa informacji na podstawie którego sformułowano potrzeby.

W ramach Projektu we wskazanych wyżej siedmiu jednostkach, do dnia 12 sierpnia 2025 r. przeprowadzono audyty wstępne z zakresu bezpieczeństwa informacji.

Ponadto przewidywany jest zakup sprzętu informatycznego z przeznaczeniem dla tych jednostek w postaci:

- urządzeń UTM i serwerów NAS dla wszystkich siedmiu jednostek podległych Urzędowi, biorących udział w Projekcie,

²⁶ Według „Informacji z otwarcia ofert” wpłynęła jedna oferta w ramach tego postępowania. Postępowanie to ze względu na fakt, że nie zostało zakończone w trakcie trwania kontroli NIK, nie podlegało sprawdzeniu w jej ramach.

²⁷ 50 061,00 zł z 849 991,00 zł.

²⁸ Planowana wartość projektu – 117 225,00 zł.

²⁹ Planowana wartość projektu – 58 305,00 zł.

³⁰ Planowana wartość projektu – 54 369,00 zł.

³¹ Planowana wartość projektu – 24 480,00 zł.

³² Planowana wartość projektu – 21 774,00 zł.

³³ Planowana wartość projektu – 25 828,00 zł.

³⁴ Planowana wartość projektu – 21 774,00 zł.

- serwerów typu rack, zasilaczy UPS i oprogramowania do monitorowania infrastruktury informatycznej dla Zespołu Szkół Ogólnokształcących w Bystrzycy Kłodzkiej, Szkoły Podstawowej nr 2 w Bystrzycy Kłodzkiej oraz Szkoły Podstawowej w Wilkanowie,
- zasilacza UPS dla Centrum Integracji Społecznej w Bystrzycy Kłodzkiej.

Na zakończenie Projektu przewidziano wykonanie audytu końcowego w każdej z biorących udział w Projekcie jednostek podległych Urzędowi.

(akta kontroli: tom II, str. 1-57, 152, 166-167)

6. Do realizacji zadań związanych z realizacją Projektu w Urzędzie wyznaczony został Kierownik Wydziału Organizacyjno-Prawnego, Informatyk w tym Wydziale oraz IOD. Wynikało to z wewnętrznych ustaleń i miało odzwierciedlenie w aktualnym zakresie ich czynności oraz kompetencjach.

(akta kontroli: tom II, str. 154, 203-206, 270-333)

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

(akta kontroli: tom II, str. 154, 203-206, 270-333)

8. We wniosku o przyznanie grantu Gmina sformułowała następujące wskaźniki produktu i rezultaty Projektu:

- dwóch administratorów przeszkolonych z zakresu konfiguracji i zarządzania przełącznikami sieciowymi, konfiguracji i zarządzania urządzeniami UTM, konfiguracji i zarządzania serwerowymi systemami operacyjnymi oraz zarządzania oprogramowaniem do monitorowania infrastruktury informatycznej,
- osiem systemów w zakresie zwiększenia bezpieczeństwa informacji Urzędu i siedmiu jednostek podległych, biorących udział w Projekcie.

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 NIK wskaźniki osiągnięto w zakresie przeszkolenia dwóch administratorów, pozostałe nie zostały jeszcze w pełni zrealizowane ze względu na nierozstrzygnięcie postępowania w zakresie zakupu sprzętu informatycznego.

(akta kontroli: tom II, str. 1-167, 270-333, 378-396)

9. Według stanu na 12 sierpnia 2025 r. w ramach Projektu wykonano wstępny audyt bezpieczeństwa informacji, a dwóch administratorów/informatyków Urzędu przeszło cztery szkolenia specjalistyczne z zakresu konfiguracji i zarządzania przełącznikami sieciowymi, konfiguracji i zarządzania urządzeniami UTM, konfiguracji i zarządzania serwerowymi systemami operacyjnymi oraz zarządzania oprogramowaniem do monitorowania infrastruktury informatycznej.

Do dnia zakończenia czynności kontrolnych NIK, nie rozstrzygnięto natomiast postępowania o zamówienie publiczne na zakup sprzętu informatycznego oraz nie ogłoszono postępowań na wykonanie audytów końcowych z zakresu bezpieczeństwa informacji.

(akta kontroli: tom II, str. 1-167, 270-233, 378-396)

Według wyjaśnień złożonych przez Burmistrza w ramach Projektu nie będzie instalowane żadne oprogramowanie dziedzinowe, a planowane do zakupu serwery mają służyć do wykonywania kopii zapasowych.

(akta kontroli: tom II, str. 378-396)

10. Na dzień zakończenia czynności kontrolnych NIK realizacja Projektu w Urzędzie była na etapie rozstrzygania postępowania na zakupu urządzeń. W związku z powyższym przyjęcie i wdrożenie procedur monitorowania utrzymania efektów Projektu, o których mowa w § 13 umowy o powierzenie grantu, nastąpi po wykonaniu wszystkich umów dotyczących dostaw i usług w ramach Projektu.

(akta kontroli: tom II, str. 378-396)

11. Urząd posiadał SZBI spełniający wymagania § 19 ust. 1 rozporządzenia KRI. Podstawowym dokumentem w tym zakresie była Księga SZBI, przyjęta 25 listopada 2022 r., która wykazywała zgodności systemu z wymaganiami normy ISO/IEC 27001³⁵. Właścicielem tego dokumentu ustanowiono Burmistrza, którego w zakresie wdrożenia, oceny, przeglądu i aktualizacji dokumentacji wspomagał Pełnomocnik ds. SZBI oraz Zespół ds. SZBI. Księga ta zawierała m.in. zapisy dotyczące kontekstu organizacji, przywództwa, planowania, wsparcia oraz zabezpieczeń³⁶, oceny wyników oraz doskonalenia. Została ona zatwierdzona przez Burmistrza³⁷ i przedstawiona do zapoznania się oraz stosowania wszystkim pracownikom.

Ponadto na SZBI składały się:

- plan komunikacji w zakresie SZBI,
- polityka klasyfikacji informacji,
- polityka haseł,
- polityka zarządzania systemami informatycznymi³⁸;
- polityka ochrony obiektu,
- polityka korzystania z Internetu,
- wykaz przepisów prawnych i regulacyjnych dotyczących bezpieczeństwa informacji,
- polityka bezpieczeństwa informacji,
- polityka bezpieczeństwa ochrony danych osobowych,
- procedura nadzoru nad udokumentowanymi informacjami,
- procedura zarządzania ryzykiem w obszarze bezpieczeństwa informacji,

³⁵ Norma ISO/IEC 27001 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania; dalej: norma ISO/IEC 27001.

³⁶ Odnosi się do wymagań określonych w Załączniku A do normy ISO/IEC-27001.

³⁷ Zarządzenie nr 0050.345.2022 Burmistrza Bystrzycy Kłodzkiej z dnia 25 listopada 2022 r. w sprawie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy Bystrzyca Kłodzka.

³⁸ Regulująca zagadnienia: techniczne środki ochrony; dostęp do zasobów informatycznych; nadawanie uprawnień do systemów teleinformatycznych; wykorzystywanie programów narzędziowych umożliwiających obejście zabezpieczeń systemów i aplikacji; środki i metody uwierzytelniania użytkowników; rozpoczynanie, zawieszanie i kończenie pracy w systemie; tworzenie kopii zapasowych; zarządzanie nośnikami informacji; złośliwe oprogramowanie; zarządzanie bezpieczeństwem pracy w sieci Internet; naruszenie bezpieczeństwa informacji w sieci; zabezpieczenia kryptograficzne; przeglądy, konserwacje i naprawy oraz czynności kontrolne.

- procedura zarządzania zmianą, zarządzanie projektami,
- procedura inwentaryzacji sprzętu i oprogramowania,
- procedura niszczenia nośników danych cyfrowych,
- procedura niszczenia nośników tradycyjnych,
- procedura dostępu i zdalnego przetwarzania mobilnego,
- procedura zarządzania uprawnieniami do systemów informatycznych,
- procedura realizacji zastępstw,
- procedura dostępu do sieci,
- procedura przechowywania haseł administracyjnych,
- procedura szyfrowania informacji przesyłanych pocztą email i zabezpieczania kluczy odzyskiwania,
- procedura dostępu do serwerowni,
- procedura rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych,
- procedura postępowania z kluczami oraz zabezpieczania pomieszczeń,
- procedura wykonywania przeglądów i konserwacji systemów i nośników,
- procedura zabezpieczania przed szkodliwym oprogramowaniem,
- procedura tworzenia kopii zapasowych,
- procedura korzystania z poczty e-mail,
- procedura monitorowania i reagowania na zdarzenia, incydenty i naruszenia,
- procedura – plan ciągłości działania systemów informatycznych,
- procedura realizacji oceny skutków dla ochrony danych osobowych,
- procedura audytu wewnętrznego i działań korygujących,
- procedura przeglądu zarządzania,
- procedura nadawania i odbierania upoważnień do przetwarzania danych osobowych,
- procedura udostępniania danych w zakresie wniosków Policji i innych instytucji,
- procedura wynoszenia dokumentacji poza obszar organizacji,
- procedura realizacji praw osób, których dane dotyczą,
- procedura współpracy z organem nadzorczym,
- procedura kontaktu z IOD.

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

(akta kontroli: tom I, str. 157-699; tom II, str. 231)

12. Dokumentacja składająca się na SZBI była na bieżąco aktualizowana i w razie potrzeby doskonalona. Była ona poddawana okresowym przeglądom, głównie pod kątem zmian przepisów prawa, zmian personalnych i organizacyjnych, które wymagały wprowadzenia uaktualnień w dokumentacji systemu. Podstawowym dokumentem w tym zakresie były protokoły ze spotkań zespołu ds. SZBI, na których m.in. dokonywano przeglądu aktualności Księgi SZBI oraz przygotowywano projekt planów szkoleń i audytów. W wyniku

tak prowadzonych przeglądów w ostatnich dwóch latach dokonano czterech zmian w Księdze SZBI³⁹.

(akta kontroli: tom I, str. 152-699; tom II, str. 164)

13. W okresie objętym kontrolą w Urzędzie przeprowadzono jeden audyt wewnętrzny w zakresie bezpieczeństwa informacji za 2024 r.⁴⁰, nie przeprowadzono natomiast audytu za 2023 r., co opisano w sekcji *Stwierdzone nieprawidłowości*.

Audyt wewnętrzny z zakresu bezpieczeństwa informacji za 2024 r. wykonywała firma zewnętrzna posiadająca niezbędne kompetencje w tym zakresie. Badanie audytowe obejmowało ocenę spełnienia wymagań wynikających z § 19 rozporządzenia KRI.

W zakresie dotyczącym SZBI w ostatnim audycie sformułowano 17 „spostrzeżeń” i nie formułowano rekomendacji, podkreślając przy tym wysoki poziom wyszkolenia personelu oraz zaangażowanie kierownictwa.

(akta kontroli: tom II, str. 165, 344-365)

14. Do dnia zakończenia czynności kontrolnych NIK prowadzone działania informacyjne i promocyjne, w związku z realizacją przez Urząd i jednostki podległe, biorące udział w Projekcie, polegały na:

- oznaczeniu znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich plakatów w budynkach oraz informacji na stronie internetowej, a także dokumentów związanych z realizacją Projektu, dotyczących postępowań o zamówienia publiczne;
- umieszczeniu plakatów w formacie A3 w siedzibie Urzędu oraz siedmiu jednostkach podległych, biorących udział w Projekcie;
- umieszczeniu opisu Projektu na stronie internetowej Urzędu;
- bieżącym dokumentowaniu działań informacyjnych i promocyjnych, prowadzonych w ramach Projektu.

(akta kontroli: tom II, str. 168-178)

Stwierdzone
nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

W Urzędzie nie przeprowadzono w 2023 r. audytu wewnętrznego z zakresu bezpieczeństwa informacji, co było niezgodne z § 19 ust. 2 pkt 14 rozporządzenia KRI.

Burmistrz przyznała, że taki stan miał miejsce, wyjaśniając, że audyt taki był zaplanowany w grudniu 2023 r. w ramach realizacji Projektu, ale w związku ze znacznym opóźnieniem w podpisaniu umowy, doszedł on do skutku w 2024 r.

NIK wskazuje, że rozporządzenie KRI wprowadziło wymóg dokonywania tego typu audytów nie rzadziej niż raz na rok.

(akta kontroli: tom II, str. 165)

³⁹ W dniach: 28 maja 2024 r.; 1 sierpnia 2024 r.; 4 marca 2025 r. oraz 29 kwietnia 2025 r.

⁴⁰ Przeprowadzony 12 sierpnia 2024 r.

IV. Uwagi i wnioski

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

Uwagi	Najwyższa Izba Kontroli nie formułuje uwag.
Wnioski	Zapewnienie przeprowadzania audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz w roku.

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 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.
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 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosku pokontrolnego oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań. W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Wrocław, 19 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/