NAJWYŻSZA IZBA KONTROLI

Delegatura w Katowicach

LKA.410.12.3.2025

Joanna Sokolińska
Wójt Gminy

Urząd Gminy
Pl. Kościuszki 31
42-265 Dąbrowa Zielona

WYSTĄPIENIE POKONTROLNE

P/25/003 – Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
ul. Powstańców 29, 40-039 Katowice
tel. 48327844200, lka@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy Dąbrowa Zielona[1], Pl. Kościuszki 31, 42-265 Dąbrowa Zielona, REGON: 151397902
Kierownik jednostki kontrolowanej	Joanna Sokolińska, Wójt Gminy, od 6 maja 2024 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Maria Włodarczyk , Wójt Gminy, od 19 listopada 2018 r. do 6 maja 2024 r.
Zakres przedmiotowy kontroli	Realizacja przez gminy i powiaty działań w celu zwiększania poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych w 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 Delegatura w Katowicach
Kontroler	Piotr Jużków, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LKA/79/2025 z 25 kwietnia 2025 r.

(akta kontroli str. 1)

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

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Uzasadnienie oceny ogólnej

W okresie objętym kontrolą[4] Gmina Dąbrowa Zielona[5] na podstawie umowy o powierzenie grantu zawartej z Centrum Projektów Polska Cyfrowa[6] 22 kwietnia 2024 r.[7] zrealizowała projekt pod nazwą *Wzmocnienie odporności na zagrożenia płynące z* Cyberbezpieczeństwa[8]. Środki finansowe zostały przez Gminę wykorzystane zgodnie z przeznaczeniem, wszystkie wydatki spełniały warunki kwalifikowalności, a niewykorzystaną kwotę grantu zwrócono w przewidzianym umową terminie. CPPC oraz Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy[9] także uznały poniesione przez Gminę wydatki za kwalifikowalne, prawidłowo udokumentowane i poniesione terminowo co potwierdziła przyjmując i zatwierdzając wniosek rozliczeniowy. W ramach projektu zmodernizowano infrastrukturę informatyczną, stworzono system zasilania awaryjnego oraz wprowadzono System Zarządzania Bezpieczeństwem Informacji[10] Urzędu. Audyt zgodności z wymaganiami 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*[11] oraz ustawy z dnia 5 lipca 2018 r. *o Krajowym Systemie Cyberbezpieczeństwa*[12] zakończył się wynikiem pozytywnym. Jako nieprawidłowe, NIK oceniła, że w trakcie realizacji Projektu Urząd nie informował na bieżąco i w sposób ciągły o uzyskanym jego dofinasowaniu ze środków Unii Europejskiej i budżetu państwa oraz niezrealizowanie prac zabezpieczających dostęp do pomieszczenia serwerowni Urzędu.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[13] kontrolowanej działalności

OBSZAR

Realizacja przez gminy i powiaty działań w celu zwiększenia poziomu cyberbezpieczeństwa

Opis stanu faktycznego

1.1 Gmina nie ujęła zagadnień dotyczących cyberbezpieczeństwa ani działań służących jego podnoszeniu w żadnym dokumencie strategicznym. Wójt Gminy wyjaśniła, że Strategia Rozwoju Gminy na lata 2023–2030 została opracowana na przełomie lat 2022 i 2023 i nie zawierała bezpośrednich odniesień do kwestii

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[4] Do 6 czerwca 2025 r.
[5] Dalej: Gmina.
[6] Dalej: CPPC lub grantodawca.
[7] Nr FERC.02.02-CS.01-001/23/0234/FERC.02.02-CS01-001/23/2024 podpisana elektronicznie przez Wójta i Skarbnika Gminy w dniu 11 marca 2024 r. oraz przez upoważnionego pracownika Centrum Projektów Polska Cyfrowa w dniu 22 kwietnia 2024 r. Dalej: umowa grantowa lub umowa.
[8] Dalej: Projekt.
[9] Dalej: NASK.
[10] Dalej: SZBI.
[11] Dz. U. z 2024 r. poz. 773, dalej: rozporządzenie KRI.
[12] Dz. U. z 2024 r. poz. 1777 ze zm. Dalej: ustawa KSC.
[13] 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.

związanych z cyberbezpieczeństwem. Pomimo braku ujęcia tych zagadnień w ww. dokumentach, Gmina podejmowała działania mające na celu zwiększenie poziomu cyberbezpieczeństwa – zarówno ze środków własnych, jak i poprzez pozyskiwanie funduszy zewnętrznych. Środki te wykorzystywano m.in. na podnoszenie kompetencji cyfrowych pracowników oraz poprawę zabezpieczeń przed zagrożeniami w sferze cyfrowej.

(akta kontroli str. 230)

1.2 Działania Urzędu w zakresie zapewnienia cyberbezpieczeństwa zostały przewidziane w § 12 ust. 3 pkt 10 Regulaminu Organizacyjnego z dnia 28 czerwca 2024 r.[14] Na mocy tego postanowienia, Referat Organizacyjny był zobowiązany do zapewnienia funkcjonowania oraz przestrzegania zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych, zapewnienia zgodności ich działania ze szczególnymi wymaganiami w zakresie bezpieczeństwa, a także do sprawowania kontroli nad przestrzeganiem zasad bezpiecznej eksploatacji systemów informatycznych. Podobne zapisy znajdowały się w Regulaminie Organizacyjnym Urzędu obowiązującym do 30 czerwca 2024 r.[15]

Ponadto, Zarządzeniem nr 0050.43.2021 Wójta Gminy z 16 czerwca 2021 r. powołano osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

(akta kontroli str. 243, 269-274)

1.3 Gmina, w terminie zgodnym z § 4 pkt 4 lit. a umowy grantowej tj. 22 maja 2024 r., przekazała do NASK *Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego*.

W ankiecie przeprowadzono analizę wdrożonych rozwiązań w zakresie cyberbezpieczeństwa na dzień realizacji grantu oraz określono planowany stan tych rozwiązań po jego zakończeniu. W szczególności zaplanowano działania w obszarach takich jak: zarządzanie cyberbezpieczeństwem, wdrożenie SZBI, ochrona zasobów, monitorowanie zdarzeń, reagowanie na incydenty oraz rozwój infrastruktury technicznej.

(akta kontroli str. 41-48,66-67)

1.4 Urząd na realizację projektu uzyskał dofinansowanie w ramach programu *Fundusze Europejskie Na Rozwój Cyfrowy 2021-2027* w kwocie 300 150 zł[16]. Zgodnie z umową grantową i wnioskiem o udzielenie grantu z 16 listopada 2023 r. środki te zostały wydatkowane przez Gminę na: modernizację infrastruktury informatycznej Urzędu[17], zakup agregatu prądotwórczego (z montażem i uruchomieniem) oraz opracowanie audytu zerowego

[14] Zarządzenie 0050.73.2024 Wójta Gminy z 28 czerwca 2024 r. w sprawie nadania Regulaminu Organizacyjnego.
[15] Zarządzenie 0050.144.2016 Wójta Gminy z dnia 30 czerwca 2016 r. w sprawie nadania Regulaminu Organizacyjnego.
[16] W tym 246 106,88 zł ze środków UE oraz 54 022,32 zł ze środków z budżetu państwa, co stanowiło 100% całkowitej wartości projektu.
[17] Wniosek o udzielenie grantu przewidywał dostawę: serwera (z konfiguracją i wdrożeniem), urządzenia UTM (z konfiguracją), programu VPN z dwuetapową autentyfikacją (z wdrożeniem) oraz oprogramowania antywirusowego EDR lub XDR.

i końcowego z wdrożeniem SZBI zgodnego z rozporządzeniem KRI oraz ustawą KSC.

W umowie określono, że środki z grantu zostaną wypłacone w trzech transzach, w wysokości 30%, 30% i 40%, umowa dopuszczała zmianę sposobu wypłaty po uprzednim złożeniu wniosku. Pierwsza transza w kwocie 73 837,20 zł (30%) wpłynęła 11 czerwca 2024 r. a pozostała część w kwocie 172 286,74 zł w dniu 17 grudnia 2024 r.

W ramach grantu Gmina zgodnie umową i harmonogramem wydatkowała łącznie 300 129 zł, w tym 43 050 zł (15%) w obszarze organizacyjnym[18] i 257 100 zł (85%) w technicznym[19], a nie wykorzystaną część środków grantu w kwocie 20,80 zł zwróciła przelewem 14 lutego 2025 r. W trakcie realizacji grantu nie wystąpiły żadne opóźnienia a wniosek rozliczający Gminy został zatwierdzony przez NASK w dniu 2 czerwca 2025 r.

(akta kontroli str. 2-39, 92-97)

Na podstawie analizy ewidencji księgowej projektu zweryfikowano 100% wydatków Gminy na realizację Projektu. Badanie prawidłowości wydatkowania środków w ramach umowy wykazało, że poniesione wydatki były kwalifikowalne, poniesione w terminie i udokumentowane za pomocą dowodów księgowych, spełniających wymagania określone dla dowodu księgowego wg ustawy z 29 września 1994 r. o rachunkowości[20].

(akta kontroli str. 71-91,166-219, 276)

1.5 W ramach grantu nie przewidziano udziału jednostek Urzędu w jego realizacji. Wójt wyjaśniła, że grant był planowany w Urzędzie ze względu na prowadzenie pełnej obsługi księgowej i kadrowej podległych jednostek.

(akta kontroli str. 230)

Wójt wyjaśniła, że po analizie poziomu cyberbezpieczeństwa w podległych jednostkach, Gmina podjęła działania zmierzające do pozyskania środków na podniesienie kompetencji cyfrowych oraz cyberbezpieczeństwa m.in. poprzez udział w naborze wniosków w innym konkursie[21].

(akta kontroli str. 230)

1.6 W okresie objętym kontrolą nie odnotowano problemów w realizacji projektu wynikających z fluktuacji kadr. Wójt Gminy wskazała jako osobę odpowiedzialną za przygotowanie wniosków oraz realizację grantu głównego specjalistę

---

[18] Audyt zerowy zgodności z *rozporządzeniem KRI* za kwotę 2 460 zł (faktura FV 105/2024) oraz wdrożenie SZBI i przeprowadzenie audytu końcowego za kwotę 5 495 zł (faktura 171/2024).

[19] Zakupy: serwera z konfiguracją i wdrożeniem; urządzenia UTP z licencją, wdrożeniem i szkoleniem; programu VPN z wdrożeniem; programu antywirusowego EDR (38 licencji); trzech routerów zarządzalnych za łączną kwotę 150 785 zł (faktura FS 0035/11/2024); agregatu prądotwórczego z montażem za 125 952 zł (faktura FV/326/2024); tzw. serwera plików NAC z dyskami i urządzenia UPS za łączną kwotę 15 436,50 zł (faktura FS/145/12/2024). Z tego zakup routerów zarządzalnych, serwera plików NAS z dyskami i urządzenia UPS, łącznie za kwotę 37576,50 zł nie był przewidziany we wniosku o udzielenie grantu, jednakże zdaniem NIK urządzenia te miały związek z poprawą poziomu cyberbezpieczeństwa Urzędu i z tego powodu spełniały warunek kwalifikowalności.

[20] Dz. U. z 2023 r. poz. 120 ze zm.

[21] FESL.01.04-IŻ.01-135/24 w ramach naboru z działania 1.4. Cyfryzacja administracji publicznej bezpośrednio przez jednostki podległe

ds. obsługi informatycznej, zarządzania kryzysowego i obrony cywilnej w Referacie Organizacyjnym Urzędu. Pracownik ten był odpowiedzialny za zapewnienie ciągłości działania systemów informatycznych Urzędu oraz jednostek organizacyjnych mu podległych. Od 16 czerwca 2021 r. był on osobą wyznaczoną przez Wójta Gminy do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, w zakresie zadań publicznych zależnych od funkcjonowania systemów informatycznych, realizowanych przez Urząd i jednostki organizacyjne Gminy a od 19 października 2023 pełnił on także funkcję Administratora Systemu Teleinformatycznego[22].

(akta kontroli str. 231, 240-243, 247)

1.7. W związku ze zmianą na stanowisku Wójta, w maju 2024 r. Gmina poinformowała o tym fakcie grantodawcę.

(akta kontroli str. 229, 231,281)

1.8. W toku realizacji projektu Gmina, we wniosku rozliczeniowym z dnia 7 maja 2025 r. wykazała realizację wskaźników wynikających z Załącznika nr 9 do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd"[23], Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa określając także ich wartość bazową. Według wniosku rozliczeniowego, osiągnięto planowane wartości wskaźników: liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji - 1, liczba użytkowników nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych - 2, liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach jednostek samorządu terytorialnego (JST) - 1, liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym (kobiety) - 1. Wniosek rozliczeniowy został zaakceptowany przez NASK bez uwag 2 czerwca 2025 r.

NIK zwraca uwagę, że sposób zdefiniowania wskaźników projektu przez grantodawcę nie zapewniał właściwego ich wykazywania przez Gminę. Zgodnie z Załącznikiem nr 9 każdy zakupiony program komputerowy (aplikacja), urządzenie z oprogramowaniem systemowym czy agregat prądotwórczy, służące zapewnieniu ciągłości cyberbezpieczeństwa w Urzędzie powinno się traktować jako odrębny system (służący zwiększeniu poziomu bezpieczeństwa informacji) i wykazać we wniosku rozliczającym (w osiągniętych wskaźnikach). Jednocześnie w Załączniku tym znajdował się inny zapis zobowiązujący Gminę do niezaliczania różnych aplikacji wchodzących w skład jednego systemu. Opis wskaźników dopuszczał zatem różną ich interpretację. Należy też zauważyć, że grantobiorca przyjął wniosek sprawozdawczy, nie wzywał Gminy do korekty wskaźników i zatwierdził je bez uwag.

(akta kontroli str. 73, 83, 92, 96-97, 232)

1.9 W ramach zrealizowanego Projektu Gmina zakupiła dwa rodzaje oprogramowania komputerowego, cztery rodzaje urządzeń sieciowych oraz

[22] Dalej zwany: Administrator S.T.
[23] Dalej zwany: Załącznik nr 9

agregat prądotwórczy i urządzenie UPS mające na celu zapewnienie ciągłości zasilania w przypadku utraty energii elektrycznej z sieci energetycznej.

Zainstalowany agregat prądotwórczy został zgłoszony do odbioru. W dniu 10 grudnia 2024 r. komisja odbiorowa sporządziła protokół odbioru i przekazania tego urządzenia do eksploatacji, w którym stwierdzono, że dostawa oraz prace towarzyszące zostały wykonane bez wad i zostały przyjęte od wykonawcy. Działanie tego urządzenia potwierdziły przeprowadzone testy przeprowadzone w ramach oględzin NIK. Za właściwe utrzymanie stanu technicznego agregatu odpowiadał główny specjalista ds. obsługi informatycznej, któremu obowiązki te zostały przekazane ustnie.

(akta kontroli str. 62-64, 237, 195, 238)

Oględziny sprzętu komputerowego potwierdziły wykorzystywanie 38 subskrypcji[24] licencji oprogramowania antywirusowego. W zakresie oprogramowania VPN, serwera, urządzenia UTP i routerów Gmina odebrała te przedmioty i usługi protokołem z 12 listopada 2024 r. nie wnosząc do niego żadnych uwag. Wszystkie zakupione systemy i urządzenia zostały zainstalowane i prawidłowo wdrożone co zwiększyło poziom bezpieczeństwa jednostki.

(akta kontroli str. 54-55, 60, 180-183, 235, 237,278-279)

1.10 Wójt Gminy, zarządzeniem Nr 0050.148.2024 z 31 grudnia 2024 r., wprowadziła „Procedurę monitorowania utrzymania efektów Projektu", dotyczącą środków trwałych i usług nabytych w ramach projektu Funduszy Europejskich na Rozwój Cyfrowy 2021–2027 (FERC).

W procedurze określono jej cel i zakres, tj. systematyczne gromadzenie informacji dotyczących utrzymania środków trwałych oraz usług nabytych w ramach projektu przez okres co najmniej dwóch lat od jego zakończenia, a także zapewnienia trwałości projektu w tym samym okresie. Dokument wskazywał, że procedura obowiązywała wszystkich pracowników Urzędu, natomiast odpowiedzialność za jej prawidłowe wdrożenie i stosowanie ponosiła Wójt Gminy.

W ramach procedury monitoringiem objęto elementy z trzech obszarów: organizacyjnego, kompetencyjnego oraz technicznego[25].

(akta kontroli str. 221-224)

---

[24] 34 licencje na stanowiska komputerowe oraz 4 na serwery

[25] Dane i informacje na potrzeby monitoringu będą zbierane cyklicznie raz do roku począwszy od 2026 roku; Monitoring będzie prowadzony z wykorzystaniem metody ilościowej i wartościowej określonej dla wykazanych we wniosku wskaźników/liczby jednostek; Dane do monitoringu będą przekazywane pracownikowi upoważnionemu do kontaktu z grantodawcą (Główny Specjalista) przez pracownika odpowiedzialnego za utrzymanie efektów projektu przez okres 2 lat od zakończenia projektu oraz utrzymania trwałości projektu; Interpretacja danych zgromadzonych w systemie monitoringu następuje na podstawie karty stanowiącej zał. Nr 1 do Procedury monitorowania utrzymania efektów; Osoby wyznaczone w umowie zawartej z Wykonawcą monitorują sprawność i czasookres zakupionych usług i /lub dostaw przez cały okres realizacji projektu z zachowaniem terminów utrzymania efektów i trwałości; Pracownik upoważniony do kontaktu z grantodawcą przedkłada na żądanie grantodawcy lub Instytucji Zarządzającej (FERC), Instytucji Pośredniczącej lub Komisji Europejskiej raporty z monitoringu utrzymania efektów projektu tj. utrzymania środków trwałych i usług nabytych; W sprawach nieuregulowanych procedurą stosuje się odpowiednie przepisy prawa, akty wewnętrzne oraz regulamin organizacyjny

Jak wskazała Wójt po zakończeniu realizacji grantu Gmina planuje utrzymywać licencje na oprogramowanie, sprzęt oraz pakiety wsparcia technicznego ze środków własnych.

Wyjaśniła ponadto, że w ramach Krajowego Funduszu Szkoleń, główny specjalista ds. obsługi informatycznej, zarządzania kryzysowego i obrony cywilnej Urzędu weźmie udział w szkoleniu pn. „Audytor wiodący systemu zarządzania bezpieczeństwem informacji wg PN-EN ISO/IEC 27001:2023", zaplanowanym na lipiec 2025 r. Według niej ukończenie szkolenia umożliwi tej osobie samodzielne weryfikowanie zgodności procedur z wymaganiami rozporządzenia KRI oraz ustawy KSC. Tym samym Gmina planuje ograniczyć koszty związane z audytami zewnętrznymi, przeznaczając środki na inne działania w obszarze cyberbezpieczeństwa.

NIK zauważa, że audyt to niezależna, systematyczna ocena procesu, produktu, systemu lub organizacji pod kątem zgodności z określonymi standardami, przepisami lub celami a zatem nie może on być prowadzony przez tą samą osobę, która odpowiada za audytowany obszar.

(akta kontroli str. 232)

1.11 W Urzędzie, od 31 grudnia 2024 r., Zarządzeniem Nr 0050.147.2024 Wójta z 31 grudnia 2024 r., wprowadzono SZBI. Wszyscy pracownicy Urzędu zostali zapoznani z dokumentacją SZBI, co potwierdzili podpisem pod stosownym oświadczeniem.

Zgodnie z § 4 ww. zarządzenia, odpowiedzialność za wdrożenie oraz utrzymanie dokumentacji SZBI powierzono Administratorowi S.T, natomiast w zakresie dokumentacji dotyczącej ochrony danych osobowych – Inspektorowi Ochrony Danych Osobowych.

(akta kontroli str. 127-165, 229, 275,277-279)

W ramach analizy ryzyka przeprowadzonej w Urzędzie na potrzeby opracowania i wdrożenia SZBI stwierdzono istnienie ryzyka nieuprawnionego dostępu urządzeń serwerowni i zalecono wprowadzenie zabezpieczeń obniżających ich wystąpienie. Zgodnie z przyjętym planem postępowania powyższe ryzyka miały zostać usunięte do końca II kwartału 2025 r. czego nie zrealizowano, co opisano w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 46-48, 138-139, 228, 268)

1.12 Po wprowadzeniu w dniu 31 grudnia 2024 r. Polityki Bezpieczeństwa Informacji stanowiącej element SZBI, do dnia zakończenia kontroli w Urzędzie nie przeprowadzono aktualizacji wewnętrznych regulacji w zakresie bezpieczeństwa informacji, wynikającej z § 19 ust. 2 pkt 1 rozporządzenia KRI. Zgodnie z tym przepisem, jednostka zobowiązana jest do zapewnienia aktualizacji regulacji wewnętrznych w odpowiedzi na zmieniające się otoczenie (organizacyjne, technologiczne i prawne). Wójt Gminy wyjaśniła, że w okresie objętym kontrolą nie wystąpiły przypadki naruszenia polityk bezpieczeństwa, a więc taka potrzeba nie wystąpiła zaś audyt zostanie przeprowadzony do końca 2025 roku.

(akta kontroli str. 154-157, 275)

1.13 W Urzędzie, w dniu 6 grudnia 2024 r. na potrzeby przyjęcia SZBI zakończono przeprowadzenie audytu bezpieczeństwa informacji, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI w zakresie zgodności z tym rozporządzeniem oraz ustawą KSC, który zakończył się wynikiem pozytywnym.

(akta kontroli str. 98-126)

W 2022 r. podobny audyt prowadzony był przez podmiot zewnętrzny. Wójt wyjaśniła, że w tymże roku nastąpiła wymiana sprzętu komputerowego w Gminie. W 2023 r. weryfikację zgodności bezpieczeństwa informacji Urzędu z rozporządzeniem 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*[26] przeprowadził główny specjalista ds. obsługi informatycznej, zarządzania kryzysowego i obrony cywilnej Urzędu. NIK zwraca uwagę, iż audyt wykonany przez nieuprawnioną osobę, odpowiadającą jednocześnie za audytowany obszar nie może zostać uznany jako przeprowadzony w sposób niezależny i w związku tym może być on kwestionowany.

(akta kontroli str. 252)

1.14 Urząd w okresie od 21 kwietnia 2024 r. do 28 kwietnia 2025 r. nie wywiązywał się z obowiązku informacyjnego określonego w §11 umowy grantowej, co opisano w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 225-230)

Stwierdzone nieprawidłowości

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

1. Po zawarciu w dniu 21 kwietnia 2024 r. umowy grantowej, główny specjalista ds. obsługi informatycznej, zarządzania kryzysowego i obrony cywilnej Urzędu do 28 kwietnia 2025 r.[27] tj. przez 372 dni nie wywiązywał się z obowiązków informacyjnych określonych w §11 umowy: nie wywiesił na terenie budynku Urzędu obowiązkowego plakatu informacyjnego oraz nie zapewnił informowania społeczeństwa w sposób ciągły na stronach internetowych Gminy o fakcie realizacji Projektu. Informacje o fakcie otrzymania dofinasowania na jego realizację ze środków ze środków Funduszy Na Rozwój Cyfrowy 2021-2027 (FERC) należało udostępnić i opublikować po podpisaniu umowy grantowej i rozpoczęciu jej realizacji oraz utrzymywać co najmniej do końca upływu okresu trwałości Projektu (art. 13 ust. 1 umowy). Ww. główny specjalista wyjaśnił, że plakat miał być wywieszony na okres trwałości projektu po jego rozliczeniu. Wójt Gminy wyjaśniła, że *"Pierwsza, informacja o uzyskaniu dofinansowania w ramach Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny samorząd" została zamieszczona na oficjalnej stronie internetowej*

[26] Dz.U. z 2017 r., poz. 2247.
[27] Dzień rozpoczęcia kontroli NIK.

Gminy w dniu 20.03.2024 r. Kolejna informacja informująca o zrealizowaniu wyżej wymienionego grantu została zamieszczona na stronie internetowej w dniu 30.12. 2024 r. Obie informacje zostały zamieszczone w zakładce aktualności, w której niestety informacje są wyświetlane automatycznie przez 30 dni. Po tym czasie informacje przechodzą do archiwum. Podczas trwania kontroli, została wydzielona odrębna zakładka Strona Główna – Dla Mieszkańców – Cyberbezpieczny samorząd, która ułatwi wyszukiwanie informacji na temat Projektu Cyberbezpieczny Samorząd."

W trakcie kontroli NIK, 7 czerwca 2025 r. główny specjalista ds. obsługi informatycznej, zarządzania kryzysowego i obrony cywilnej umieścił na drzwiach wejściowych plakat informacyjny oraz zamieścił opis Projektu na stronach internetowych urzędu. W związku z zamieszczeniem informacji o dofinansowaniu Projektu w Urzędzie i na stronach internetowych Gminy, odstąpiono od sformułowania wniosku pokontrolnego.

(akta kontroli str. 225-230)

2. Do dnia zakończenia kontroli pomieszczenie serwerowni Urzędu nie zostało zabezpieczone zgodnie z wymaganiami określonymi w SZBI co było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI. Wójt Gminy wyjaśniła, że w budżecie Gminy na 2025 r. zostały zabezpieczone środki finansowe na realizację zadania pn. „Modernizacja budynku Urzędu Gminy w Dąbrowie Zielonej", w ramach którego przewidziano wykonanie prac dostosowujących zabezpieczenia pomieszczenia serwerowni do wymagań określonych w SZBI. Zgodnie z oświadczeniem Wójta[28], zakończenie ww. prac dostosowawczych przewidziano na koniec czerwca 2025 r. a Urząd był na etapie przygotowania umowy na wykonanie ww. prac.

(akta kontroli str. 228, 268)

IV. Uwagi i wnioski

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

Wnioski

Niezwłoczne podjęcie i zrealizowanie prac zabezpieczających dostęp do pomieszczenia serwerowni, zgodnie z wymaganiami określonymi w SZBI.

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 w Katowicach. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje

[28] Z 6 czerwca 2025 r.

do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

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.

Katowice, dnia 10 września 2025 r.

Kontroler

Piotr Jużków

St. inspektor kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Delegatura w Katowicach

p.o. Dyrektor

Marcin Wesoły

/podpisano elektronicznie/