NAJWYŻSZA IZBA KONTROLI

Delegatura w Katowicach

LKA.410.12.2.2025

Tomasz Pieczka
Wójt Gminy Świerklany

Urząd Gminy Świerklany
ul. Kościelna 85
44-266 Świerklany

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 Świerklany[1], ul. Kościelna 85, 44-266 Świerklany, REGON 000551326
Kierownik jednostki kontrolowanej	Tomasz Pieczka, Wójt Gminy Świerklany[2] od 22 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 kontroli w 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Katowicach
Kontroler	Artur Stekla, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKA/78/2025 z 25 kwietnia 2025 r.

(akta kontroli str. 1-6)

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

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia negatywnie działalność Urzędu w kontrolowanym obszarze.

Uzasadnienie oceny ogólnej

W okresie objętym kontrolą (od 18 kwietnia 2024 r.) Gmina Świerklany[5] rozpoczęła okres realizacji przedsięwzięcia[6] w projekcie grantowym „Cyberbezpieczny Samorząd" w ramach Priorytetu II *Zaawansowane usługi cyfrowe*, Działania 2.2. *Wzmocnienie krajowego systemu cyberbezpieczeństwa*[7] Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027[8]. Wartość wydatków Projektu przewidziano na 849 700 zł, wraz z dofinasowaniem ze środków budżetu państwa i UE w wysokości 781 724,01 zł. Pomimo upływu 15 z 24 miesięcznego okresu realizacji umowy o powierzenie grantu[9], do dnia 23 lipca 2025 r. Urząd wykonał jedynie część z przewidzianych działań wykorzystując kwotę 307 838,50 zł tj. 36,3 % łącznego budżetu Projektu. Podniesiony został poziom ogólnej wiedzy z zakresu bezpieczeństwa informacji kierownictwa, kadry urzędniczej Urzędu oraz podległych jednostek, podwyższono poziom ochrony antywirusowej 100 urządzeń końcowych, zakupiono cztery systemy teleinformatyczne, w tym dwa wraz z dedykowanymi im urządzeniami informatycznymi (serwer poczty z funkcjami ochrony przed spamem i złośliwym oprogramowaniem, urządzenie klasy Unified Threat Management[10]). Dotychczas nie zakupiono lub nie oddano w pełni do użytku wszystkich zaplanowanych z punktu widzenia zarządzania ryzykiem cyberbezpieczeństwa rozwiązań informatycznych, środków technicznych (serwerów[11], przełączników sieciowych, zasilaczy awaryjnych, rozwiązań sprzętowo-systemowych do wykonywania kopii zapasowych danych Urzędu i podległych jednostek) i nie wykonano całości koniecznych usług konfiguracyjnych i wdrożeniowych na sieci. Nie udało się przeszkolić pracowników IT Urzędu, kluczowych z punktu widzenia systemu zarządzania bezpieczeństwem informacji[12] oraz wdrażanych rozwiązań technicznych i informatycznych, przeprowadzić edukacji phishingowej pracowników Urzędu i wdrożyć rozwiązania do weryfikacji dwuetapowej. W Urzędzie nie doprowadzono do zmiany lub aktualizacji wadliwej Polityki Bezpieczeństwa Teleinformacyjnego. W toku kontroli stwierdzono, iż nie zachowano ciągłości realizacji zamówień, w konsekwencji powodującej technologiczną zamianę kolejności instalacji urządzeń i sprzętu informatycznego. NIK zauważa ryzyko

---

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

[5] Dalej: *Gmina*.

[6] Dalej: *Projekt*.

[7] Rozumianego jako dziedzina wiedzy zajmująca się zapewnieniem odporności: systemów informacyjnych na działania naruszające poufność, dostępność i autentyczność i przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

[8] Dalej: *FERC.*

[9] Nr FERC.02.02-CS.01-001/23/0296/ FERC.02.02-CS.01-001/23/2024 podpisana kwalifikowanym podpisem elektronicznym w dniach 16 i 17 kwietnia 2024 r. przez Wójta i Skarbnika Gminy oraz 18 kwietnia 2024 r. przez upoważnionego pracownika Centrum Projektów Polska Cyfrowa. Dalej: *umowa grantowa* lub *umowa*.

[10] Dalej: *UTM* (pol.: wielofunkcyjna zapora sieciowa). System bezpieczeństwa wyposażony w zaporę sieciową, ochronę przed atakami, filtrowanie treści www, wirtualną sieć prywatną, kontrolę aplikacji i optymalizację pasma.

[11] Urząd poinformował, że planuje wprowadzić zmianę w Projekcie i odstąpić od zakupu serwerów przewidzianych we wniosku o przyznanie grantu.

[12] Dalej: *SZBI*.

niepowodzenia realizacji celu Projektu jakim jest kompleksowe zwiększenie poziomu bezpieczeństwa informacji jednostki samorządu terytorialnego. Ponadto zidentyfikowano nieprawidłowości, takie jak:

- nieprzekazanie do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego[13] Ankiety Dojrzałości Cyberbezpieczeństwa dotyczącej jednej z gminnych jednostek przewidzianych jako korzystające z grantu oraz przekazane jednej z ankiet zawierającej nierzetelne informacje o liczbie pracowników jednostki;
- nieuzasadnione opóźnienie odbioru I etapu przedmiotu umowy z 15 grudnia 2023 r. na wykonanie usługi doradczej w ramach Projektu;
- udzielenie w dniu 31 grudnia 2024 r. zamówienia publicznego na dostawę urządzeń i oprogramowania o wartości 254 548,50 zł brutto bez zastosowania przepisów ustawy z dnia 11 września 2019 r. *Prawo zamówień publicznych*[14] oraz nierzetelna realizacja i odbiór przedmiotu tego zamówienia;
- naruszenie postanowień *Wytycznych dotyczących kwalifikowalności wydatków na lata 2021-2027* Ministra Funduszy i Polityki Regionalnej z 18 listopada 2022 r.[15] i obowiązującego w Urzędzie *Regulaminu udzielania zamówień publicznych o wartości szacunkowej nieprzekraczającej kwoty 130 000 zł*[16] podczas ustalania wartości szacunkowej zamówienia publicznego na przeprowadzenie szkolenia pracowników Urzędu i jednostek podległych w zakresie bezpieczeństwa informacji oraz w trakcie prowadzenia tego postępowania;
- wdrożenie w dniu 24 lipca 2023 r. *Polityki Bezpieczeństwa Teleinformatycznego w Urzędzie*, która zawierała postanowienia niezgodne z przepisami rozporządzenia 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*[17] oraz nierzetelne postanowienia i zapisy;
- niezapewnienie przeprowadzenia w 2024 r. w Urzędzie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji do czego zobowiązywały przepisy rozporządzenia KRI z 2012 r. oraz 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*[18];
- nierzetelną, niezgodną z postanowieniami §11 umowy grantowej realizację obowiązków w zakresie informowania i promowania dofinansowania uzyskanego na realizację Projektu.

[13] Dalej: *NASK*.
[14] Dz.U. z 2024, poz. 1320, ze zm. Dalej: *ustawa PZP*.
[15] M.P., poz. 1119 z 25 listopada 2022 r., https://www.funduszeeuropejskie.gov.pl/media/112343/Wytyczne_dotyczace_kwalifikowalnosci_2021_2027.pdf (wersja obowiązująca od 25.11.2022 do 24.03.2025, dostęp 7.06.2025 r.). Dalej: *Wytyczne kwalifikowalności*.
[16] Wprowadzonego zarządzeniem nr W.0050.235.2020 Wójta Gminy z dnia 28 grudnia 2020 r.
[17] Dz.U. z 2017 r., poz. 2247. Dalej: *rozporządzenie KRI z 2012 r.*
[18] Dz.U., poz. 773. Dalej: *rozporządzenia KRI z 2024 r*.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[19] kontrolowanej działalności[20]

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

Opis stanu faktycznego

1. Na realizację Projektu Gmina zawarła z Centrum Projektów Polska Cyfrowa[21] umowę grantową, której integralną częścią są załączniki, w tym wniosek Gminy o przyznanie grantu złożony w dniu 20 listopada 2023 r., podpisany w dniu 18 stycznia 2024 r.[22] Termin realizacji umowy w zakresie rzeczowym, stosownie do § 3 ust. 1 ww. umowy, upływa w dniu 18 kwietnia 2026 r. Wniosek ten w pkt *6. Montaż finansowy* zawierał informacje o: przewidzianych wydatkach ogółem i kwalifikowalnych projektu (kwota 849 700 zł), kwocie przewidzianego dofinansowania (781 724,01 zł tj. 92 % wydatków kwalifikowalnych), wkładzie finansowym ze środków UE (656 648,19 zł, tj. 77,3 % wydatków kwalifikowalnych), wkładzie finansowym ze środków budżetu Państwa (125 075,85 zł, tj. 14,7 % wydatków kwalifikowalnych) i wysokości wkładu własnego Gminy (67 975,99 zł, tj. 8 % wydatków kwalifikowalnych). W okresie od dnia 12 lipca 2024 r.[23] do 23 lipca 2025 r. ze środków grantu i środków Gminy Urząd wykorzystał na realizację Projektu łącznie kwotę 307 838,50 zł, tj. 36,3 % wartości Projektu. W tym samym czasie od niewykorzystanych środków finansowych grantu ulokowanych na rachunku bankowym Projektu zaksięgowano odsetki bankowe w łącznej kwocie 5 308,56 zł, które są dochodem Gminy.

(akta kontroli str. 13-45, 50-61, 1030-1031)

W obowiązującej Strategii Rozwoju Gminy na lata 2015-2023 oraz innych dokumentach strategicznych zamieszczonych na jej stronie internetowej nie były uwzględnione zagadnienia dotyczące potrzeby zwiększenia poziomu cyberbezpieczeństwa. W związku z tym nie określano też terminów wdrożenia działań w tym zakresie.

(akta kontroli str. 9-13)

Sekretarz Gminy nadzorująca Pion informatyczny Urzędu poinformowała m.in., że w projekcie budowy nowej siedziby Urzędu przewidziano potrzebę wydzielenia osobnego pomieszczenia przeznaczonego na urządzenia i systemy teleinformatyczne[24]. W ramach budowy zostało także przewidziane zabezpieczenie w postaci głównego zasilacza UPS zintegrowanego z agregatem

---

[19] 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.

[20] W treści wystąpienia pokontrolnego NIK wyłączyła jawność informacji ustawowo chronionych na podstawie art. 5 ust. 2 ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz. U z 2022 r. poz. 902) i art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji* (Dz. U. z 2022 r. poz. 1233) w interesie podmiotów, których dotyczą zawarte w wystąpieniu pokontrolnym informacje, poprzez ich anonimizację i zastąpienie oznaczeniem „[...]".

[21] Dalej: *CPPC*.

[22] Kwalifikowanym podpisem elektronicznym przez Wójta Gminy.

[23] Data uzyskania pierwszych zaliczek ze środków budżetu państwa i UE w łącznej kwocie 234 517,18 zł.

[24] Między innymi serwery, przełączniki sieciowe, systemy alarmowe i monitoring.

prądotwórczym w celu zapewnienia ciągłości działania Urzędu na wypadek braku zasilania z sieci energetycznej. Przewidziano także zabezpieczenie pomieszczenia serwerowni . Zarządzeniem[25] Wójta z dnia 24 lipca 2023 r. wprowadzono Politykę Bezpieczeństwa Teleinformatycznego w Urzędzie.

(akta kontroli str. 8, 167-168, 201-242)

2. Odpowiadając na pytanie czy w Urzędzie rozpoznano faktyczne zagrożenia i potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa oraz czy w Gminie (tj. Urzędzie wraz z podległymi jednostkami) przeprowadzone były działania mające na celu określenie ich potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa Sekretarz Gminy wyjaśniła, że z racji zgłaszanych przez pracowników Urzędu i jednostek częstych problemów z pocztą pod kątem zagrożeń cybernetycznych (złośliwego oprogramowania, zjawiska spamu i wyłudzania informacji) rozpoczęto przeprowadzanie szkolenia z podstaw cyberbezpieczeństwa, ochrony danych osobowych, bezpiecznego korzystania z poczty elektronicznej i Internetu oraz reagowania na incydenty bezpieczeństwa. Według Sekretarz zwrócono uwagę na potrzebę wdrożenia rozwiań zarówno systemowych jak i programowych w celu zmniejszenia zagrożeń wynikających z obsługi poczty elektronicznej. Kontrolującym nie przedstawiono żadnej dokumentacji i badań z zakresu zagrożeń cyberbezpieczeństwa w Urzędzie i mających na celu określenie potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa.

(akta kontroli str. 8, 167-168)

Część z gminnych jednostek przed rozpoczęciem realizacji Projektu korzystała ze wspólnej sieci teleinformatycznej (sieć komputerowa wraz z infrastrukturą serwerowni[26]), z zasobów informatycznych (przestrzeni dysku sieciowego z dedykowanymi folderami przeznaczonymi do wymiany informacji i danych[27]) oraz ze wspólnej licencji stanowiskowej oprogramowania antywirusowego[28].

Odpowiadając na pytanie czy zamierzony rezultat zaplanowanych działań został osiągnięty oraz czy był prowadzony wraz z dokumentowaniem monitoring działań realizowanych przez jednostki organizacyjne urzędu, Wójt podał, że Projekt jest w trakcie realizacji. Na dzień 16 maja 2025 r., według Wójta, rezultat zamierzonych działań został uzyskany dla:
- podstawowego (ogólnego) szkolenia z zakresu cyberbezpieczeństwa. Monitoring tego działania obejmował listę obecności na szkoleniu. Po przeprowadzonym szkoleniu, zdaniem Wójta zauważono zwiększoną świadomość zagrożeń i poprawę umiejętności w zakresie reagowania na incydenty i tworzenia bezpiecznych haseł;

[25] Nr W.0050.155.2023.
[26] Urząd, Gminny Ośrodek Pomocy Społecznej, Gminny Zespół Obsługi Placówek Oświatowych, Gminny Ośrodek Kultury i Rekreacji.
[27] Urząd, Gminny Ośrodek Pomocy Społecznej, Gminny Zespół Obsługi Placówek Oświatowych, Gminny Ośrodek Kultury i Rekreacji, Gminny Zakład Wodociągów i Kanalizacji, Gminna Biblioteka Publiczna.
[28] Urząd, Gminny Ośrodek Pomocy Społecznej, Gminny Zakład Wodociągów i Kanalizacji, Gminny Zespół Obsługi Placówek Oświatowych, Gminny Ośrodek Kultury i Rekreacji.

- dostawy rozwinięcia oprogramowania antywirusowego; urządzenia klasy UTM; oprogramowanie typu Network Access Control[29], których monitoring był prowadzony na podstawie protokołu odbioru.

(akta kontroli str. 292-293, 694-695)

3. Urząd opracował i przekazał w dniu 22 maja 2024 r. do NASK 10 Ankiet Dojrzałości Cyberbezpieczeństwa dotyczących Urzędu i dziewięciu podległych jednostek objętych Projektem[30]. Zostały one przesłane w formie elektronicznej w sposób wskazany w § 4 pkt 4 umowy grantowej tj. na adres skrytki Elektronicznej Platformy Usług Administracji Publicznej NASK. Urząd dotychczas nie przekazał jednej Ankiety dotyczącej gminnego żłobka a ankieta dotycząca Przedszkola w Jankowicach zawierała nierzetelne informacje o liczbie pracowników. Powyższe opisano w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 96-165, 252-256)

4. Zgodnie z zapisami wniosku o przyznanie grantu środki finansowe pozyskane przez Gminę na realizację Projektu w wysokości 781 724,01 zł były przeznaczone na zwiększenie poziomu bezpieczeństwa informacji poprzez wykonanie czterech zadań:

1) usługi doradczej w celu wsparcia Urzędu w realizacji Projektu o łącznej wartości wydatków 5 700 zł, w obszarze organizacyjnym;
2) wykonania audytu bezpieczeństwa informacji w Urzędzie i podległych jednostkach oraz aktualizacja SZBI, przeprowadzenie szkoleń dla pracowników z zakresu bezpieczeństwa informacji oraz specjalistycznych dla administratorów sieci o łącznej wartości wydatków 198 000 zł, w obszarach organizacyjnym i kompetencyjnym;
3) zakupu urządzeń i oprogramowania informatycznego dla Urzędu zwiększającego odporność na cyberataki[31] i wycieki danych wraz z wdrożeniem, o łącznej wartości wydatków 526 000 zł, w obszarze technicznym;
4) zakupu urządzeń i oprogramowania informatycznego dla podległych instytucji zwiększającego odporność na cyberataki i wycieki danych w tych jednostkach z wdrożeniem o łącznej wartości 120 000 zł, w obszarze technicznym.

W opisie merytorycznym realizowanego Projektu nie wskazano, które z przewidzianych gminnych jednostek, poza Urzędem, będą jego odbiorcami lub uczestnikami oraz w jakim zakresie.

W dniu 17 lipca 2025 r. Zastępca Wójta, zwrócił się do NASK wnioskiem[32] o potwierdzenie dopuszczalności zmian w zakresie rzeczowym Projektu polegających na rezygnacji z trzech wydatków przewidzianych we wniosku

---

[29] Dalej: *NAC* (pol.: technologie i polityki, których celem jest ujednolicenie technologii zabezpieczeń punktów końcowych i kontrola dostępu do sieci komputerowej przez urządzenia i użytkowników).

[30] Gminnego Ośrodka Pomocy Społecznej, Gminnego Zespołu Obsługi Placówek Oświatowych, Gminnego Zakładu Wodociągów i Kanalizacji, Szkół Podstawowej nr 1 i 2 w Świerklanach, Szkoły Podstawowej w Jankowicach, Przedszkoli nr 1 i 2 w Świerklanach i Przedszkola w Jankowicach.

[31] Rodzaj ofensywnego działania w Internecie osób lub organizacji, którego celem mogą być systemy informatyczne, sieci komputerowe, komputery lub inne urządzenia osobiste.

[32] Uzupełnionym w dniu 21 sierpnia 2025 r.

o przyznanie grantu (w ramach zadania 3): „Zarządzanie zasobami IT", „Edukacja phishingowa" i „Weryfikacja dwuetapowa" o łącznej wartości 31 000 zł. Jednocześnie Gmina zaplanowała przeznaczenie powstałych w wyniku ww. zmian oszczędności *na dodatkowe rozwiązania techniczne z obszaru cyberbezpieczeństwa* (wdrożenie rozwiązań backupu o wyższym poziomie bezpieczeństwa i większej wydajności, w tym macierzy i serwera backup wraz z konfiguracją, dodatkowego switcha zarządzalnego i serwerów NAS dla sześciu jednostek podległych wraz dyskami i konfiguracją) i na wymagane dodatkowe audyty końcowe z zakresu cyberbezpieczeństwa. Według Zastępcy zmiany te nie wpłyną na wartość żadnego z przyjętych w Projekcie wskaźników a konieczność ich modyfikacji wyniknęła z identyfikacji nowych potrzeb wdrożeniowych, których nie można było przewidzieć na etapie przygotowywania założeń projektowych w 2023 r. oraz z niedoszacowania wartości audytów dla wszystkich jednostek objętych grantem.
Ponadto, w dniu 24 lipca 2025 r., Kierownik Referatu Rozwoju i Promocji Gminy oraz Inspektor ds. informatyki i bezpieczeństwa systemów informatycznych poinformowali, że Gmina planuje odstąpić od zakupu serwerów przewidzianych we wniosku o przyznanie grantu (w zadaniu 3 i 4) na kwoty 99 000 zł i 50 000 zł a jednocześnie zamierza przeznaczyć ww. kwoty na zakup *systemów dedykowanych do backupu i archiwizacji danych* (serwerów NAS i macierzy dyskowej). Według ww. osób w wyniku przeprowadzonych wdrożeń stwierdzono, iż obecne zasoby serwerowe są wystarczające do obsługi planowanych rozwiązań w zakresie cyberbezpieczeństwa. Podkreślili oni, że zakup nowych systemów backupu przyczyni się do zwiększenia poziomu realizacji wskaźników Projektu w większym stopniu niż pierwotnie planowany zakup serwerów.
Przedstawiciel NASK w dniu 27 sierpnia 2025 r. poinformował m.in., że ww. zamienny zakres rzeczowy wyszczególniony przez Gminę, na podstawie § 3 ust. 2 pkt 3 Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd"[33] i dokumentu pn. Schemat Grantowy Cyberbezpieczny Samorząd (rozdział „Wydatki kwalifikowalne i sposób rozliczania grantów" może być objęty kwalifikacją kosztów.

(akta kontroli str. 51-60, 1032-1038, 1062-1064)

W celu realizacji powyższych zadań Gmina zawarła[34] z wykonawcami cztery umowy:

- w dniu 15-ego grudnia 2023 r. na wykonanie w ramach Projektu usługi doradczej obejmującej m.in. analizę infrastruktury informatycznej Jednostki Samorządu Terytorialnego i konsultacje inżynierskie dla informatyka na potrzeby doboru technologii; pełną obsługę wniosku i wszystkich formalności związanych z pozyskaniem grantu; zarządzanie Projektem i nadzór nad prawidłową realizacją umowy grantowej jako Inżynier Projektu; przygotowywanie opisu przedmiotu zamówienia; udział w czynnościach wyboru dostawcy sprzętu i czynnościach odbiorowych; pełne wsparcie przy rozliczeniu programu, w tym rozliczenie finansowe. Wartość tego zamówienia wynosiła łącznie 6 999,99 zł brutto a terminy realizacji przedmiotu umowy

[33] Dalej: *Regulamin konkursu*. https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (dostęp: 16.06.2025).
[34] Do dnia 9 czerwca 2025 r.

ustalono na 30 kwietnia 2024 r. (analiza infrastruktury informatycznej jst, konsultacje inżynierskie dla informatyka na potrzeby doboru technologii; pełna obsługa wniosku i wszystkich formalności związanych z pozyskaniem grantu o wartości 3 500 zł) oraz do 30 czerwca 2026 r. (pozostała część przedmiotu umowy o wartości 3 499,99 zł). Wykonawca we właściwym terminie (8 kwietnia 2024 r.) dostarczył Urzędowi wymaganą dokumentację I etapu przedmiotu umowy, co potwierdził Specjalista ds. Informatyki i bezpieczeństwa systemów informatycznych. Wójt Gminy w dniu 18 listopada 2024 r. podpisał z wykonawcą protokół odbioru I etapu przedmiotu ww. umowy, co opisano w sekcji „Stwierdzone nieprawidłowości". Z tytułu realizacji I etapu zamówienia wykonawca w dniu 18 listopada 2024 r. wystawił fakturę[35] na prawidłową kwotę 3 500 zł brutto, którą Urząd opisał i ujął w ewidencji księgowej jako wydatek kwalifikowalny Projektu (z czego: 2 199,03 zł ze środków FERC, 418,86 zł ze środków budżetu państwa, 227,64 zł ze środków budżetu gminy i 654,47 zł ze środków budżetu gminy – część podatku VAT niepodlegającego odliczeniu).

(akta kontroli str. 341-371, 391-396)

- w dniu 31 października 2024 r. na zakup i dostawę oprogramowania, urządzeń informatycznych i usług dla Urzędu i jednostek podległych, mających na celu zwiększenie odporności na cyberataki i wycieki danych, tj.
  1) rozwinięcia oprogramowania antywirusowego dla Urzędu oraz podległych jednostek – na 100 stanowisk,
  2) rozwiązania sprzętowego do ochrony poczty wraz z licencją oraz wdrożeniem,
  3) programu do monitorowania i analizy logów z modułami bezpieczeństwa oraz wdrożeniem,
  4) urządzenia klasy UTM wraz z licencją oraz wdrożeniem,
  5) oprogramowania typu NAC wraz z wdrożeniem,
  6) usługi wdrożenia sprzętowego wraz z konfiguracją systemów.
  Wartość ww. zamówienia ustalono na 254 548,50 zł brutto a termin jego realizacji na 30 listopada 2024 r. Protokół odbioru końcowego przedmiotu ww. umowy został podpisany (bez uwag) w dniu 29 listopada 2024 r. W dniu 4 grudnia 2024 r. wykonawca wystawił fakturę[36] na prawidłową kwotę 254 548,50 zł brutto, która została opisana i ujęta w ewidencji księgowej jako wydatek kwalifikowalny Projektu (z czego: 159 930,96 zł ze środków FERC, 30 463,04 zł ze środków budżetu państwa, 16 556 zł ze środków budżetu Gminy i 47 598,50 zł ze środków budżetu Gminy – część podatku VAT niepodlegającego odliczeniu).

  (akta kontroli str. 397-443)

  Ww. zamówienie zostało udzielone przez Urząd bez zastosowania przepisów ustawy PZP, co opisano w sekcji „Stwierdzone nieprawidłowości".

- w dniu 13 grudnia 2024 r. na przeprowadzenie podstawowego szkolenia z zakresu bezpieczeństwa informacji dla pracowników Urzędu oraz podległych jednostek (1 szt.), nie później niż do 31 grudnia 2024 r. W umowie tej wskazano minimalny zakres tematyczny szkolenia, w ramach którego nie zobowiązano

[35] Nr FS.2024.156.
[36] Nr 135/2024.

wykonawcy do omówienia Polityki Bezpieczeństwa Teleinformatycznego Urzędu jako elementu obowiązującego SZBI. Dwa dwugodzinne szkolenia, które odbyły się w dniu 16 grudnia 2025 r., w formie stacjonarnej w grupach liczących 53 i 29 osób kosztowały Gminę 49 790 zł brutto. W szkoleniach tych wzięły udział łącznie 82 osoby, z czego 37 pracowników Urzędu i 45 pracowników z 12 podległych jednostek Gminy. W dniu 23 grudnia 2024 r. wykonawca wystawił fakturę[37] na prawidłową kwotę 49 790 zł netto/brutto, która została opisana i ujęta w ewidencji księgowej jako wydatek kwalifikowalny Projektu (z czego: 38 477,71 zł ze środków FERC, 7 329,09 zł ze środków budżetu państwa i 3 983,20 zł ze środków budżetu Gminy).

(akta kontroli str. 444-465)

W procedurze szacowania wartości i wyłaniania przez Urząd wykonawcy tego zamówienia (opisania przedmiotu umowy, sporządzenia i zawarcia umowy) wystąpiły stany, które zostały opisane w sekcji „Stwierdzone nieprawidłowości".

- w dniu 25 kwietnia 2025 r. na wykonanie usługi - audytów SZBI w oparciu o 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*[38]*,* ustawę z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*[39], normę ISO 27001[40] i *wytyczne Ministra Cyfryzacji dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych*[41] dla Urzędu oraz dla dziewięciu podległych jednostek objętych Projektem, w terminie do 28 listopada 2025 r. za kwotę 60 823,50 zł brutto. Do dnia zakończenia kontroli NIK usługa nie została zrealizowana.

(akta kontroli str. 513-519)

5. We wniosku o przyznanie grantu, w opisie koncepcji realizacji Projektu oprócz Urzędu, nie podano liczby i nazw jednostek podległych Gminie, mających skorzystać ze wsparcia. Zgodnie załącznikami do wniosku, oprócz Urzędu uczestnikami Projektu jest 10 podległych jednostek.
Zgodnie z informacją Wójta, w związku z tym, że Urząd i część podległych jednostek korzystała ze wspólnej infrastruktury i dostępu do zasobów, w realizacji Projektu, oprócz Urzędu, uwzględniono (w różnym zakresie) również 12 podległych jednostek organizacyjnych: (-) Gminny Ośrodek Pomocy Społecznej, (-) Gminny Zespół Obsługi Placówek Oświatowych, (-) Gminny Ośrodek Kultury i Rekreacji, (-) Gminny Zakład Wodociągów i Kanalizacji, (-) Gminna Biblioteka Publiczna, (-) po trzy szkoły podstawowe i przedszkola oraz gminny żłobek. W szkoleniach w formie stacjonarnej z zakresu bezpieczeństwa informacji mieli wziąć udział pracownicy Urzędu oraz wszystkich podległych jednostek. Przeprowadzenie audytów Systemów Zarządzania Bezpieczeństwem Informacji[42] i wdrożenie polityk bezpieczeństwa informacji przewidziano dla Urzędu i gminnych jednostek z wyjątkiem Gminnej Biblioteki, Ośrodka

[37] Nr 25/12/2024.
[38] Dz.U. z 2024 r., poz. 773.
[39] Dz.U. z 2024 r., poz. 1077, ze zm.
[40] *Systemy Zarządzania Bezpieczeństwem Informacji*.
[41] https://mc.bip.gov.pl/wytyczne/wytyczne-dla-kontroli-dzialania-systemow-teleinformatycznych-uzywanych-do-realizacji-zadan-publicznych.html, dostęp 19 maja 2025 r.
[42] Dalej: *SZBI*.

Kultury i Rekreacji oraz żłobka. Wdrożenie rozwiązań monitorujących i zabezpieczających przed atakami przewidziano dla Urzędu i gminnych placówek (za wyjątkiem Gminnej Biblioteki, placówek oświatowych, przedszkoli i żłobka). Przeznaczenie środków grantu na techniczne wsparcie dwóch instytucji kultury posiadających osobowość prawną i przeszkolenie ich pracowników było. niezgodne z § 4 ust. 1 Regulaminu konkursu, co opisano w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 51-60, 292-293, 694-695, 799-802)

6. Według informacji Sekretarza Gminy, do realizacji Projektu (grantu) w Urzędzie wyznaczony został Kierownik Referatu i Promocji Gminy, który współpracuje z Inspektorem ds. Informatyki i bezpieczeństwa systemów informatycznych. Do zakresu obowiązków Inspektora należy m.in. cyberbezpieczeństwo, pełnienie obowiązków Administratora Systemów Informatycznych[43] Urzędu a także współpraca w zakresie opracowywania wniosków o fundusze unijne związane z informatyzacją jednostek. Ww. osoba miała wykształcenie i kwalifikacje potwierdzone m.in. certyfikatami szkoleń odpowiadające zajmowanemu stanowisku i przypisanym mu obowiązkom służbowym.

7. W okresie realizacji Projektu nie występowały problemy związane z fluktuacją kadry Urzędu.

(akta kontroli str. 7, 166, 172-179, 187)

8. We wniosku Gminy z dnia 20 listopada 2023 r. o udzielenie grantu na realizację Projektu nie zdefiniowano liczbowych wskaźników produktu, określonych w *Załączniku nr 9 – Opis wskaźników projektu Cyberbezpieczny Samorząd*[44] *do* Regulaminu konkursu. W części opisowej podano m.in., że Gmina planuje zakup nowego i bardziej zaawansowanego antywirusa, serwera lub serwerów, switchy zarządzalnych, rozwiązań uwierzytelniania wielopoziomowego, urządzenia ochrony brzegowej wraz ze wsparciem, rozwiązania do retencji i analizy logów, oprogramowania DLP, oprogramowania do zarządzania zasobami IT, nowego systemu kopii zapasowych danych Urzędu, systemów backupowych dla jednostek podległych, urządzeń UPS (zasilania awaryjnego bateryjnego) oraz wykupienie regularnej usługi kontrolowanego ataku typu phishing. 10 z powyższych elementów, zgodnie z postanowieniami Załącznika nr 9 odpowiadało wymaganiom opisu wskaźnika produktu zdefiniowanego jako *Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji*[45].
W części opisowej oraz w harmonogramie finansowym wniosku z listopada 2023 r. nie podano liczb licencji oprogramowania antywirusowego, systemów uwierzytelnia, systemów backupowych, serwerów, switchy, urządzeń UPS oraz usług ataków phisingowych, które Gmina zamierzała nabyć ze środków przyznanego grantu.

(akta kontroli str. 53-62, 95, 294-295, 699-705)

---

[43] Dalej: *ADI*.

[44] https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad, (dostęp: 10.06.2025 r.)

[45] Zgodnie z zapisami ww. Załącznika cele Projektu należało wyrazić za przy pomocy mierzalnych wskaźników produktu (powiązanych bezpośrednio z wydatkami ponoszonymi w projekcie, zrealizowanymi w okresie od rozpoczęcia do ukończenia projektu).

9. Pomimo potwierdzenia ze strony Urzędu, że umowa z dnia 31 października 2024 r. na zakup i dostawę oprogramowania i urządzeń informatycznych dla Urzędu i jednostek podległych została wykonana (łącznie z wdrożeniem) zgodnie z zakresem określonym w dokumentacji zamówienia, w tym SWZ, OPZ i umową, w wyniku przeprowadzonych oględzin ustalono, że nie wszystkie dostarczone i zainstalowane urządzenia, programy i aplikacje informatyczne działały prawidłowo a Urząd nie dysponował kompletną dokumentacją powdrożeniową. Powyższe szczegółowo opisano w sekcji „Stwierdzone nieprawidłowości". Stany nieprawidłowe stwierdzono także w toku szacowania przedmiotu zamówienia, prowadzenia postępowania o udzielenie zamówienia, zawierania, realizacji i odbioru przedmiotu umowy z 13 grudnia 2024 r. na przeprowadzenie podstawowego szkolenia z zakresu bezpieczeństwa informacji dla pracowników Urzędu oraz podległych jednostek.
Na urządzeniach technicznych posiadających pojemność przechowywania danych (w tym na zakupionym serwerze poczty elektronicznej) Urząd i podległe jednostki nie przewidują uruchamiania (instalacji) oprogramowania dziedzinowego[46].

(akta kontroli str. 397-465, 1032-1035)

10. Z uwagi na trwający okres realizacji umowy grantowej w Urzędzie dotychczas nie było konieczności podejmowania działań w celu utrzymania poziomu cyberbezpieczeństwa

11. W Urzędzie opracowano i wdrożono od 24 lipca 2023 r. Politykę Bezpieczeństwa Teleinformatycznego w Urzędzie[47], która jak podano w §1 ust. 1 pkt 1 ww. dokumentu, stanowiła wprowadzenie SZBI dla informacji wytwarzanych i przetwarzanych przez Gminę. Polityka została opracowania m.in. na podstawie rozporządzenia KRI z 2012 r.
Polityka zastąpiła zarządzenie[48] Wójta z dnia 22 grudnia 2022 r. w sprawie ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia SZBI w Urzędzie. Dokument o nazwie *SZBI* był załącznikiem do zarządzenia.
Zdaniem NIK Polityka z lipca 2023 r. zawierała niekompletne lub niezgodne z prawem, wewnętrznie i logicznie sprzeczne oraz nierzetelne postanowienia i zapisy, co opisano w sekcji „Stwierdzone nieprawidłowości".

12. Ww. zarządzenia i Polityka Bezpieczeństwa Teleinformatycznego składająca się na SZBI Urzędu nie były aktualizowane. Zgodnie z wnioskiem o przyznanie grantu aktualizacja lub stworzenie SZBI w oparciu o przeprowadzony audyt jest jednym z przewidzianych działań Projektu w ramach zadania 2. w obszarze kompetencyjnych i organizacyjnym.

(akta kontroli str. 58, 201-242, 585-608)

---

[46] Samodzielny i niezależny system informatyczny, stworzony do świadczenia usług tylko dla silnie określonego obszaru działania danej instytucji lub organizacji np. systemy EOD/EZD, serwery stron internetowych (www, BIP), poczta elektroniczna, usługi Active Directory, systemy finansowo-księgowe, systemy kadrowo-płacowe, systemy transakcyjne, systemy zarządzania zasobami, systemy baz danych.
[47] Załącznik do Zarządzenia Wójta nr W.0050.155.2023 podpisanego przez Zastępcę Wójta.
[48] Nr W.0050.318.2022.

13. W roku 2024 w Urzędzie nie zapewniono przeprowadzenia okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji do czego zobowiązywały przepisy rozporządzenia KRI z 2012 r. (do dnia 23 maja 2024 r.) i rozporządzenia KRI z 2024 r. (od 23 maja 2024 r.), co opisano w sekcji „Stwierdzone nieprawidłowości".
Wójt Gminy zlecił wykonanie audytów SZBI dla Urzędu oraz dla dziewięciu podległych jednostek w dniu 25 kwietnia 2025 r.[49] z terminem realizacji do 28 listopada 2025 r.

(akta kontroli str. 513-519, 939-942)

14. Urząd w grudniu 2024 r. opublikował w gminnym biuletynie informację o pozyskaniu środków finansowych na realizację projektu grantowego (oraz o koszcie całkowitym projektu) przedstawiając jego ogólny cel: *zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych*. Informację o podobnej treści, uzupełnioną o pięć szczegółowych celów projektu opublikowano na stronie internetowej Gminy[50]. Publikacje te nie zawierały wymaganego opisu realizowanego Projektu oraz podawały błędną kwotę pozyskanych środków w wysokości 850 tysięcy złotych. W mediach społecznościowych Urzędu[51] do dnia przeprowadzenia oględzin[52] nie zamieszczono natomiast jakichkolwiek informacji o pozyskaniu środków UE na realizację ww. przedsięwzięcia. Trzy plakaty informacyjne znajdujące się na terenie budynku Urzędu, pomimo odpowiedniej formy graficzno-kolorystycznej, nie zawierały właściwej kwoty przyznanego dofinansowania projektu z UE. Powyższe ustalenia szczegółowo opisano w sekcji „Stwierdzone nieprawidłowości". Powyższe informacje i publikacje były opatrzone znakiem Programu FERC, barw Rzeczpospolitej Polskiej, UE i CPPC, zgodnie z § 11 ust. 4 pkt 1 lit. a umowy grantowej i zapisami *Księgi Tożsamości Wizualnej marki Fundusze Europejskie 2021 – 2027*[53].

(akta kontroli str. 197-200, 244-253, 257-161)

Stwierdzone nieprawidłowości

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

1. Inspektor ds. informatyki i bezpieczeństwa systemów informatycznych Urzędu nie przekazał do NASK Ankiety Dojrzałości Cyberbezpieczeństwa dotyczącej jednej z podległych jednostek[54]: Żłobka w Jankowicach. Natomiast przesłana przez Urząd Ankieta dotycząca Przedszkola w Jankowicach zawierała nieprawdziwe informacje o jego liczbie pracowników – zawyżone o 85,7 %[55].

[49] Umowa nr 0321-064.2025.
[50] swierklany.pl/cyberbezpieczny-samorzad-twoj-samorzad-chroniony-w-cyfrowym-swiecie.html (dostęp: 29.04.2025 r.).
[51] https://www.facebook.com/profile.php?id=61560241546606 (dostęp w dniu 7 maja 2025 r.) i https://www.youtube.com/@urzadgminyswierklany9873/videos (dostęp w dniu 7 maja 2025 r.).
[52] 7 maja 2025 r.
[53] https://www.rozwojcyfrowy.gov.pl/strony/dowiedz-sie-wiecej-o-programie/promocja-programu/#Podr%C4%99cznik%20informacji%20i%20promocji (dostęp w dniu 9 maja 2025 r.).
[54] Przewidzianych jako jednostki korzystające z grantu.
[55] Zamiast 42 osób, w Ankiecie podano 78 osób.

Ww. obowiązki informacyjne wynikały § 4 ust. 1 pkt 4 lit. a umowy grantowej oraz z treści Załącznika nr 6 do Regulaminu konkursu[56].

(akta kontroli str. 20-21, 96-165, 252-253, 647)

Inspektor ds. Informatyki i bezpieczeństwa systemów informatycznych Urzędu odpowiedzialny przygotowanie i przesłanie Ankiet wyjaśnił m.in., że w przypadku Żłobka nie opracowanie i nie przekazanie ww. dokumentu wynikało z niedopatrzenia, spowodowanego faktem, iż w okresie przygotowania koncepcji projektu ww. podmiot był nową jednostką[57]. W sprawie przekazanych nierzetelnych danych o liczbie pracowników Przedszkola w Jankowicach ww. wyjaśniła, że powodem rozbieżności była pomyłka Dyrektora tej placówki.

(akta kontroli str. 271-273, 281-282, 285-286)

2. Nieprawidłowe przeznaczenie środków grantu w kwocie 3 634,00 zł na techniczne wsparcie dwóch instytucji kultury posiadających osobowość prawną[58] i przeszkolenie trojga ich pracowników. Było to niezgodne z § 4 ust. 1 Regulaminu konkursu z listopada 2023 r. stanowiącym, że do udziału w konkursie grantowym uprawnione były jst wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia). W opracowanych przez CPPC *Najczęściej zadawanych pytaniach w konkursie „Cyberbezpieczny Samorząd"*[59] wskazano natomiast, że zgodnie z definicją jednostki podległej, ich charakterystyczną cechą jest to, że nie posiadają one własnej osobowości prawnej i korzystają z osobowości prawnej jst. Zgodnie z art. 14 ust. 1 ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej[60] przedmiotowe instytucje uzyskały osobowość prawną i mogły rozpocząć działalność z chwilą wpisu do rejestru prowadzonego przez organizatora. Pomimo tego zostały one włączone do uczestnictwa w Projektu i skorzystały z grantu ponieważ na siedmiu urządzeniach komputerowych należących do tychże jednostek uruchomiono programową ochronę antywirusową na licencji zakupionej przez Gminę ze środków grantu a ich pracownicy (trzy osoby) byli uczestnikami szkolenia z zakresu bezpieczeństwa informacji zorganizowanego przez Urząd w grudniu 2024 r. Koszt siedmiu licencji programu antywirusowego i przeszkolenia trzech osób wyniosła 1 812,41 zł i 1 821,59 zł i wydatki te nie spełniały warunku dla kosztu kwalifikowalnego wynikającego z przywołanego postanowienia Regulaminu konkursu.

(akta kontroli str. 274-280, 409, 413-418, 432-433, 451-458, 462-463)

Wyjaśniając przyczyny włączenia instytucji kultury do działań Projektu, Inspektor ds. Informatyki i bezpieczeństwa systemów informatycznych wyjaśnił, że

---

[56] Wzór *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)*, https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (dostęp 19 maja 2025 r.).

[57] Wpis do rejestru żłobków miał miejsce 4 października 2023 r. a rozpoczęcie działalności 6 listopada 2023 r.

[58] Gminnego Ośrodek Kultury i Rekreacji oraz Gminnej Biblioteki Publicznej w Świerklanach.

[59] Źródło: https://www.gov.pl/attachment/c1d1a90c-bc69-4930-837e-ece59e6a54c6, str. 81, dostęp: 14.08.2025 r.

[60] Dz.U. z 2024 r., poz. 87.

planując zakres ww. szkolenia wzięto pod uwagę to, że czynnik ludzki jest najczęstszą przyczyną wystąpienia ryzyka w obszarze ochrony informacji

i dlatego starano się dotrzeć z treścią szkolenia do pracowników jak największej liczby jednostek. Przez niedopatrzenie zostały włączone ww. instytucje.

(akta kontroli str. 271-273, 281, 285-286)

3. Wójt w dniu 18 listopada 2024 r. tj. z opóźnieniem wynoszącym siedem miesięcy i osiem dni podpisał z wykonawcą protokół odbioru I etapu przedmiotu umowy z 15 grudnia 2023 r.[61] tj. instrukcji zamykającej I etap działania w Projekcie (instrukcja wypełnienia wniosku o przyznanie grantu w Lokalnym Systemie Informatycznym[62]), opisu koncepcji programowej Projektu do formularza LSI i kartoteki programowej (zestawienia rzeczowego na potrzeby Projektu). Kompletne i poprawne dokumenty zostały prawidłowo przekazane Urzędowi w dniu 8 kwietnia 2024 r., natomiast zgodnie z § 5 ust. 4 ww. umowy zamawiający miał dwa dni robocze na sprawdzenie przekazanej dokumentacji i podpisanie protokołu jej odbioru, jeśli nie zawierała ona wad i braków lub na odmowę podpisania protokołu odbioru i wyznaczenie terminu na uzupełnienie braków i usunięcie wad. W przedmiotowym przypadku Wójt nie miał przesłanek do skorzystania z uprawnienia do odmowy podpisania protokołu a zatem najpóźniej w dniu 10 kwietnia 2024 r. powinien podpisać protokół odbioru.

(akta kontroli str. 343-344, 347-371,)

Wójt wyjaśnił, że zwłoka w potwierdzeniu powyższego protokołu odbioru usług doradczych wyniknęła z kilku czynników:

- błędu, bowiem zwyczajowo stosowane w Urzędzie praktyki rozliczeń z wykonawcami polegały na tym, że podpisanie protokołu odbioru stanowiło podstawę do wystawienia faktury i ten schemat został tu również zastosowany,
- zgodnie z zapisem § 6 ust. 1 pkt 1 umowy z 15 grudnia 2023 r. wynagrodzenie częściowe wykonawcy za realizację I etapu umowy miało zostać wypłacone w terminie 14 dni od daty wpłynięcia I transzy grantu na wyodrębniony rachunek Urzędu, a środków tych nie było na rachunku w kwietniu 2024 r.[63], gdy następował odbiór prac wykonanych w ramach I etapu,
- niedopatrzenia Zamawiającego gdyż protokół odbioru I etapu prac został podpisany 18 listopada 2024 r. z klauzulą, że jest on podstawą do wystawienia faktury VAT, co odbyło się bez zastrzeżeń ze strony Wykonawcy.

(akta kontroli str. 582-586)

Zdaniem NIK, skutkiem ww. nieprawidłowości był brak możliwości wystawienia przez wykonawcę faktury za prawidłowo wykonane usługi, a w konsekwencji opóźnienie w zapłacie należnego mu wynagrodzenia.

4. Wójt przy kontrasygnacie Skarbnika, w dniu 31 października 2024 r. udzielił zamówienia publicznego pn. „Wdrożenie urządzeń i oprogramowania dla Urzędu Gminy oraz jednostek podległych, zwiększających odporność na cyberataki i wycieki danych wraz z wdrożeniem w ramach realizacji grantu

[61] Nr 0321-005.2024.
[62] Dalej: *LSI.*
[63] Środki z grantu wpłynęły na wyodrębniony rachunek w dniu 12 lipca 2024 r.

Cyberbezpieczny Samorząd w ramach (...)"[64] o wartości 206 950 zł netto (254 548,50 zł brutto) z naruszeniem art. 2 ust. 1 pkt 1 w zw. z art. 4 pkt 1 ustawy PZP. Obowiązek zastosowania przez Urząd odpowiedniego trybu udzielania zamówień określonego ustawą PZP wynikał także z treści § 3 ust. 2 pkt 3 umowy grantowej stanowiącej m.in., że w zakresie potwierdzenia prawidłowości wyboru dostawców i wykonawców - na żądanie CPPC lub Operatora, Grantobiorca przedłoży dokumentację z postępowania o udzielenie zamówienia, zgodnie z *Wytycznymi kwalifikowalności* i dokumentami wydanymi na podstawie art. 6 ust. 2 ustawy z dnia 28 kwietnia 2022 r. *o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027*[65] w tym zakresie lub z ustawą PZP oraz z postanowieniami sekcji 3.2.2 pkt 2 *Wytycznych kwalifikowalności*.

(akta kontroli str. 397-408, 720-740)

Odpowiadający za realizację Projektu Kierownik Referatu Rozwoju i Promocji Gminy wyjaśnił: *W związku z charakterem zamówienia jego opracowaniem i przeprowadzeniem zajął się D.C.[66]. Przyznaję, że z mojej strony nadzór nad realizacją Projektu, w tym udzielaniem zamówień nie był wystarczający*. Powyższy Inspektor wyjaśnił, że nie zwrócił uwagi na konieczność zastosowania ustawy PZP. Podał, że nie uzyskał w tej sprawie pomocy ze strony komórki zamówień publicznych w Urzędzie oraz, że nie wie dlaczego pracownicy firmy pełniącej funkcję Inżyniera Projektu nie zwrócili uwagi na konieczność zastosowania przepisów ww. ustawy. Wyjaśnił, że nie posiada żadnej notatki lub protokołu z przeprowadzenia ww. postępowania. Inspektor dysponował wyłącznie notatką z szacowania wartości zamówienia[67] oraz ofertami uzyskanymi od dwóch wykonawców.

(akta kontroli str. 718-719, 741-755)

Zdaniem NIK, powyższa nieprawidłowość, zgodnie z § 5 ust. 6 umowy grantowej, skutkuje brakiem możliwości rozliczenia w ramach grantu wydatku na powyższą dostawę jako kwalifikowalny oraz zwrotem jego kwoty, ponieważ nie został on poniesiony zgodnie z przepisami ustawy PZP, stosownie do postanowień sekcji 3.2.1. pkt 1 lit. b *Wytycznych kwalifikowalności*).

(akta kontroli str. 23-24)

Skarbnik Gminy wyjaśniła m.in., że nie była świadoma niezachowania obowiązujących przepisów i procedur a zapis w umowie o przeprowadzeniu stosownego postępowania oraz, że podpis pracownika merytorycznego upewnił ją osobę w przekonaniu, że postępowanie przetargowe zostało przeprowadzone w sposób prawidłowy.

Zgodnie z wyjaśnieniami Wójta, w przedmiotowym postępowaniu zamówieniowym, nie wszystkie wymogi wynikające z przepisów ustawy PZP zostały dochowane. Według Wójta doszło do tego wskutek zaniechań, których dopuścili się pracownicy Urzędu: inspektor ds. zamówień publicznych i inspektor w Pionie Informatycznym. Druga z tych osób wprowadziła Wójta w błąd co do

[64] Sygnatura IB.271.2.1.2024.
[65] Dz.U. 2022 r. poz. 1079, ze zm.
[66] Inspektor ds. informatyki i bezpieczeństwa systemów informatycznych Urzędu.
[67] Na kwotę 207 237,50 zł netto, uzyskaną od pracownika Inżyniera Projektu.

przeprowadzenia procedury zamówieniowej zgodnie z przepisami ustawy PZP. Przedłożona Wójtowi do podpisu umowa zawierała preambułę o następującej treści: „*Zgodnie z wynikiem przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie podstawowym bez przeprowadzenia negocjacji, art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U z 2023 r. poz.1605 ze zm.), (nr referencyjny postepowania: IB.271.2.1.2024), strony zawierają umowę*". Wójt wyjaśnił też, że powyższy inspektor postanowił przeprowadzić ww. postępowanie samodzielnie, nie konsultując z nikim swojej decyzji. Wójt podał: *Działanie takie stanowiło w mojej ocenie ciężkie naruszenie podstawowych obowiązków pracowniczych przez Pana D.C., który o zaistniałej sytuacji powinien był poinformować swojego bezpośredniego przełożonego oraz kierownictwo tut. Urzędu Gminy zamiast prowadzić samodzielnie postępowanie zamówieniowe, nie mając po temu stosownej wiedzy, doświadczenia oraz kompetencji.* Zdaniem Wójta, mimo niezastosowania przepisów ustawy PZP, zamawiający dołożył wszelkich starań, aby zabezpieczyć interesy wykonawców oraz interes zamawiającego a podjęte przez niego działania były zgodne z zasadami uczciwej konkurencji, równego traktowania wykonawców oraz przejrzystości procesu udzielania zamówienia a przeprowadzone postępowanie spełniło wymogi wynikające z podstawowych zasad ustawy PZP: uczciwej konkurencji, równości, bezstronności i obiektywizmu, efektywności, jawności, przejrzystości, pisemności i prowadzenia postępowania w języku polskim oraz nie naruszyło innych zasad wynikających z ww. ustawy. Według Wójta, Gmina nie poniosła żadnej szkody.

(akta kontroli str. 805-816, 808-818)

Zdaniem NIK, powyższe wyjaśnienia wskazują, że Inspektor ds. informatyki i bezpieczeństwa systemów informatycznych Urzędu wykonał szereg czynności związanych z przeprowadzeniem ww. postępowania o zamówienie publiczne bez wiedzy i niezbędnego nadzoru ze strony Sekretarza Gminy i z całkowitym pominięciem postanowień Zarządzenia[68] Wójta z dnia 4 marca 2021 r. *w sprawie Regulaminu postępowania w sprawach o zamówienie publiczne, których wartość szacunkowa wynosi co najmniej 130 000 zł oraz regulaminu prac komisji przetargowej*. Odnosząc się do wyjaśnień Wójta, NIK wskazuje, że z załączonych do wyjaśnień dokumentów składających się na opis przedmiotu ww. zamówienia wynika, że jego autor zawarł w nich zapisy (m.in. na pierwszej, trzeciej, piątej, 18, 22 stronie załącznika nr 1 do tego postępowania) niezgodne z zasadami uczciwej konkurencji, równości, bezstronności i obiektywizmu. Wskazano w nich znak towarowy (markę oprogramowania antywirusowego) oraz szczegółowe opisy cech i funkcjonalności rozwiązań teleinformatycznych dostarczanych przez konkretnego wykonawcę, co mogło doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów[69]. Takich działań zabrania przepis art. 99 ust. 4 ustawy PZP. Nadto w przedmiotowym postępowaniu nie miały zastosowania ustawowe przepisy w zakresie środków ochrony prawnej i pozasądowego rozwiązywania sporów.

[68] Nr W.0050.38.2021.

[69] W postępowaniu oferty złożyło dwóch wykonawców na dokładnie te same urządzenia i programy.

(akta kontroli str. 652, 745-754, 846-905, 933-937, 1046-1061)

5. Pomimo stwierdzenia, w dniu 29 listopada 2024 r. przez Inspektora ds. informatyki i bezpieczeństwa systemów informatycznych Urzędu, że zamówienie to wykonano zgodnie z zakresem określonym w jego dokumentacji, w tym SWZ, OPZ i umową, w wyniku przeprowadzonych w dniu 3 czerwca 2025 r. oględzin ustalono m.in., że:

- jedno z urządzeń sieciowych i współpracujące z nim oprogramowanie systemowe o wartości 52 644 zł, mające służyć do ochrony poczty elektronicznej Urzędu, pomimo jego fizycznego uruchomienia nie spełniało swoich funkcji ochronnych z uwagi na nieukończoną przez pracowników Pion Informatycznego Urzędu od dnia 29 listopada 2024 r. konfigurację serwera poczty elektronicznej. Inspektor ds. informatyki i bezpieczeństwa systemów informatycznych tłumaczył to brakiem czasu i nagromadzeniem się innych obowiązków. Ponadto w dniu oględzin Inspektor ds. informatyki i bezpieczeństwa systemów informatycznych nie dysponował dokumentacją potwierdzającą fizyczną datę wdrożenia w Urzędzie ww. oprogramowania i urządzenia[70] jak i dokumentu z warunkami licencji oprogramowania[71] i działania ww. urządzenia, a zapytany o tą sprawę wyjaśnił *Nie pamiętam tej kwestii* (podobne wyjaśnienia uzyskano w sprawie braku dokumentacji z wdrożenia urządzenia wraz z oprogramowaniem służącym jako elementy wielofunkcyjnej zapory sieciowej);
- nie działało oprogramowanie (nie uruchamiał się system teleinformatyczny) do monitorowania i analizy logów wraz z modułami bezpieczeństwa o wartości 53 013 zł. Inspektor nie dysponował dokumentacją potwierdzającą datę wdrożenia ww. oprogramowania jak i dokumentu z warunkami licencji[72]. W powyższej sprawie Inspektor wyjaśnił, że program nie działał z uwagi na niezaktualizowanie bibliotek „.NET"[73]. Osoba ta podała, że będzie to wyjaśniane z gwarantem zamówienia;
- oprogramowanie typu NAC o wartości 56 334 zł mające służyć do kontroli dostępu do sieci oraz działających w niej urządzeń nie wykonywało docelowych funkcji ochronnych i kontrolnych w sieci budynku Urzędu z uwagi na nieukończony docelowy rozdział zasobów i urządzeń sieciowych (segmentacji sieci) różnych jednostek i nieukończoną konfigurację wszystkich urządzeń. W tym przypadku również nie dysponowano dokumentacją potwierdzającą datę wdrożenia ww. oprogramowania jak i dokumentu z warunkami licencji. Inspektor wyjaśnił, *że system będzie wymagał dodatkowej konfiguracji po ostatecznym wdrożeniu serwerów i segmentacji sieci w budynku*. Braku niezbędnej dokumentacji Inspektor nie umiał wyjaśnić.

(akta kontroli str. 411-413, 425-443, 502-506)

Odnosząc się do powyższych wyjaśnień, NIK wskazuje na nierzetelnie przeprowadzone czynności odbiorowe technicznego wdrożenia jednego

---

[70] W kolejnym dniu przedłożono wydruk z którego wynikało, że przedmiotowe urządzenie zostało zarejestrowano w systemie producenta w dniu 20 listopada 2024 r.

[71] Ważnej do 18 kwietnia 2026 r.

[72] W kolejnym dniu przedłożono wydruk certyfikatu licencyjnego systemu, z którego wynikało, że ograniczona bezterminowa licencja dla Gminy została wykupiona 27 listopada 2024 r.

[73] .NET to bezpłatna międzyplatformowa platforma deweloperów typu open source do tworzenia wielu rodzajów aplikacji (https://learn.microsoft.com/pl-pl/dotnet/core/introduction, dostęp: 6.06.2025)

z dwóch zainstalowanych urządzeń sieciowych oraz poprawności instalacji i konfiguracji trzech z pięciu systemów teleinformatycznych, jak też na niewyegzekwowanie od wykonawcy obowiązku dostarczenia kompletnej, niezbędnej dokumentacji: protokołów dostaw sprzętu (z opisem jego danych i cech identyfikacyjnych), protokołów instalacji, wdrożenia i konfiguracji oprogramowania.

Zdaniem NIK, powyższe nieprawidłowości są także wynikiem nieprawidłowej kolejności zakupu ww. urządzeń sieciowych i oprogramowania[74] na skutek rozdzielenia wszystkich zaplanowanych zakupów sprzętu i systemów teleinformatycznych na co najmniej dwa zamówienia. Ostateczne wdrożenie zabezpieczeń technicznych i systemowych powinno następować po uprzedniej dostawie i fizycznej instalacji nowych elementów infrastruktury sieciowej zaplanowanych w budynku Urzędu[75] (m.in. serwerów z przestrzenią dyskową, przełączników zarządzalnych, dodatkowych modułów), ich skonfigurowaniu oraz po przeprowadzeniu procesu segmentacji sieci i procesu tworzenia kopii zapasowych danych informatycznych Urzędu (backupu, który umożliwi ich przywrócenie w razie utraty lub uszkodzenia), bądź równolegle. Tymczasem zgodnie z wyjaśnieniami Wójta wyłonienie wykonawcy obszaru technicznego i dostawa sprzętu i pozostałego oprogramowania było zaplanowane odpowiednio na 15 lipca i 30 września 2025 r.[76]

(akta kontroli str. 51-54, 56-58, 579-580)

6. Kierownik Referatu Rozwoju i Promocji Gminy ustalając wartość szacunkową zamówienia na potrzeby postępowania dotyczącego *przeprowadzenia szkolenia pracowników w zakresie bezpieczeństwa informacji dla Urzędu i jednostek podległych* naruszył postanowienia sekcji 3.2.2.[77] obowiązujących wówczas *Wytycznych kwalifikowalności* z 18 listopada 2022 r. W pkt 3 zabraniały one dzielenia zamówienia skutkującego zaniżeniem jego wartości szacunkowej w celu wyłączenia zamówienia z zakresu stosowania zasady konkurencyjności (określonej w podrozdziale 3.2. *Wytycznych kwalifikowalności*), natomiast w pkt 4 zobowiązywały do tego aby szacując wartość zamówienia brać pod uwagę konieczność łącznego spełnienia trzech przesłanek: tożsamości przedmiotowej[78], tożsamości czasowej[79] i tożsamości podmiotowej[80]. Zaakceptowany wniosek o przyznanie grantu na realizację Projektu przewidywał zakup 12 szkoleń przeznaczonych dla pracowników gminnych jednostek o sumarycznej wartości 66 000 zł: 10 szkoleń z zakresu bezpieczeństwa informacji i dwóch szkoleń specjalistycznych dla pracowników IT, celem zwiększenia ich kompetencji ogólnych.

Zdaniem NIK, oba szkolenia niewątpliwie spełniały łącznie trzy ww. przesłanki: obejmowały usługi podobne (o tym samym kodzie CPV), mogły być przeprowadzone w tym samym czasie (z uwzględnieniem konieczności podziału

---

[74] Za wyjątkiem rozwinięcia oprogramowania antywirusowego.
[75] O przewidywanej wartości 260 000 zł.
[76] Pod warunkiem złożenia prawidłowej oferty przez przynajmniej jednego wykonawcę lub nieskorzystania ze środków ochrony prawnej przez wykonawców.
[77] Postępowanie o udzielenie zamówienia.
[78] Usługi, dostawy oraz roboty budowlane są tożsame rodzajowo lub funkcjonalnie, przy czym tożsamość rodzajowa dostaw obejmuje dostawy podobne.
[79] Możliwe jest udzielenie zamówienia w tym samym czasie.
[80] Możliwe jest wykonanie zamówienia przez jednego wykonawcę.

pracowników na oddzielne grupy szkoleniowe) oraz mogły być zrealizowane przez jednego wykonawcę (np. z rynku informatycznego działającego w branży cyberbezpieczeństwa, w tym szkoleń). W dniu 19 listopada 2024 r. ww. Kierownik dokonał faktycznego nieuprawnionego podziału potencjalnego zamówienia na usługi szkoleniowe[81] dla pracowników Urzędu i oszacował wartość zamówienia wyłącznie w zakresie ogólnych szkoleń z zakresu bezpieczeństwa informacji, na kwotę 47 166 zł netto. Wskutek tego Urząd, niezgodnie z postanowieniami sekcji 3.2.1. ust. 1 lit a *Wytycznych kwalifikowalności* wyłączył stosowanie zasady konkurencyjności nakładającej na zamawiającego m.in. obowiązek zachowania uczciwej konkurencji, równego traktowania wykonawców, przejrzystości i proporcjonalności oraz obowiązek publikacji zapytania ofertowego w Bazie Konkurencyjności[82].

(akta kontroli str. 23, 52, 57, 521, 641, 648-662, 675-680, 696-698, 707-717)

Kierownik wyjaśnił m.in., że ustalając wartość szacunkową zamówienia na usługi szkoleniowe, faktycznie dokonano podziału zamówienia na szkolenia ogólne dla pracowników jednostek gminnych z zakresu cyberbezpieczeństwa i na szkolenia specjalistyczne dla pracowników IT, zgodnie z poz. 1 i 4 wniosku o przyznanie grantu[83]. Podziału tego dokonano, kierując się analizą zakresu tematycznego obu szkoleń, planowanymi uczestnikami obu szkoleń oraz ofertą podmiotów realizujących szkolenia i uznając, że treść i zakres obu szkoleń jest odmienny. Według kierownika szkolenie specjalistyczne dedykowane w ramach projektu grantowego pracownikom IT wymagają specjalnej certyfikacji[84] i są oferowane przez nieliczne podmioty, nie tożsame z podmiotami oferującymi standardowe szkolenia z zakresu cyberbezpieczeństwa dla przeciętnych użytkowników. Ponadto Kierownik wskazał, że działał zgodnie z przepisami ustawy PZP przywołując przepisy tej ustawy, orzecznictwo oraz opinię Urzędu Zamówień Publicznych.

(akta kontroli str. 783-789)

Zdaniem NIK, przewidziane przez Urząd rodzaje szkoleń finansowanych ze środków grantu powinny dotyczyć bezpośrednio zagadnienia cyberbezpieczeństwa, bezpieczeństwa informacji i dedykowanych tej sferze rozwiązań informatyczno-organizacyjnych. Z pewnością różnią się one grupami uczestników, tematyką i poziomem merytorycznym. Jednakże zdaniem NIK szkolenia te mogły być przygotowane i zrealizowane przez jednego wykonawcę. Przywołana w wyjaśnieniach certyfikacja[85] jest potwierdzeniem uczestnictwa w szkoleniu prowadzonego przez jednego z potencjalnych wykonawców w zakresie funkcjonalności i obsługi jego produktu (programu

[81] Kierownik w protokole z ustalenia wartości szacunkowej zamówienia nie uzasadnił okolicznościami faktycznymi i obiektywnymi przyczyn podziału zamówienia zakupu usług szkoleniowych w ramach Projektu.

[82] Dalej: (BK2021). Strona internetowa prowadzona przez ministra właściwego do spraw rozwoju regionalnego przeznaczona do zamieszczania zapytań ofertowych zgodnie z zasadą konkurencyjności określoną w podrozdziale 3.2 *Wytycznych kwalifikowalności* (https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/).

[83] W części dotyczącej budżetu na realizację zadania 2.

[84] Np. szkolenie [...] Certified Administrator.

[85] Nie wymieniona przez Ministra Cyfryzacji w Wykazie certyfikatów uprawniających do przeprowadzania audytu stanowiącym załącznik do rozporządzenia z dnia 12 października 2018 r. *w sprawie certyfikatów uprawniających do przeprowadzenia audytu* (Dz.U. poz. 1999).

informatycznego[86]). Ma ono na celu przekazanie wiedzy na temat skutecznego zarządzenia siecią firmową, oprogramowaniem i urządzeniami oraz monitorowania aktywności użytkowników sieci przy pomocy tego produktu. W ograniczony stopniu dotyczy ono cyberbezpieczeństwa. Natomiast wykonawca ten także posiadał w swojej ofercie szkolenie z zakresu cyberbezpieczeństwa (w formie webinaru[87] na własnej platformie).

(akta kontroli str. 794-798)

7. Inspektor ds. informatyki i bezpieczeństwa systemów informatycznych Urzędu przeprowadził postępowanie dotyczące zakupu usług szkoleniowych na potrzeby Projektu, wyłączając z niego szkolenia specjalistyczne dla dwóch pracowników IT, nie uzasadniając tej okoliczności notatce z procedury wyboru wykonawcy usług szkoleniowych i nie publikując zapytania ofertowego w BK2021, co NIK ocenia jako działanie nierzetelne.
Inspektor wyjaśnił: *wynikało to mojej niewiedzy ponieważ sądziłem iż szkolenie specjalistyczne było inną usługą niż szkolenie podstawowe z zakresu bezpieczeństwa informacji*. Odpowiadając na pytanie z jakiego powodu rozpoczynając ww. postępowanie odstąpił od obowiązku publikacji zapytania ofertowego w BK2021 wyjaśnił, że *stało się tak, gdyż z szacunku przedmiotu zamówienia wynikało, że jego wartość nie przekroczy 50 000 zł netto. Gdyby oszacowana kwota przekroczyła 50 000 zł to wówczas był obowiązek publikacji zapytania ofertowego w Bazie Konkurencyjności*.

(akta kontroli str. 521, 718-719)

Ponadto, prowadzając czynności w ww. postępowaniu Inspektor naruszył postanowienia § 1 ust. 3 obowiązującego w Urzędzie *Regulaminu udzielania zamówień publicznych o wartości szacunkowej nieprzekraczającej kwoty 130 000 zł*[88] stanowiącego, że przy udzielaniu zamówień należy przestrzegać zasad: równego traktowania wykonawców, uczciwej konkurencji, przejrzystości postępowania i udzielania zamówień w sposób celowy i oszczędny. W zapytaniu ofertowym z dnia 25 listopada 2024 r.[89] na przeprowadzenie szkoleń pracowników z zakresu bezpieczeństwa informacji, sformułował on nadmierne, nieproporcjonalne do przedmiotu zamówienia warunki udziału wykonawców w tym postępowaniu[90], które utrudniały dostęp do niego części z nich:

(-) dysponowania co najmniej jednym audytorem posiadającym uprawnienia (certyfikat) wyłącznie Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001,
(-) posiadania doświadczenia w zakresie przeprowadzania szkoleń z zakresu cyberbezpieczeństwa w minimum dwóch jednostkach samorządu terytorialnego.

Ustalenie ww. warunków nie było zgodne z postanowieniami Regulaminu konkursu nie przewidującymi obowiązku organizacji i prowadzenia

[86] Którego Urząd był już użytkownikiem.
[87] Tj. seminarium internetowego, czyli formy edukacji lub prezentacji prowadzonej online, która umożliwia interakcję między prowadzącym a uczestnikami, zazwyczaj poprzez chat lub pytania.
[88] Wprowadzonego zarządzeniem nr W.0050.235.2020 Wójta Gminy Świerklany z dnia 28 grudnia 2020 r.
[89] Nr IB.271.2.2.2024, które zostało wysłane do trzech wybranych wykonawców.
[90] Przy jednoczesnym zaniechaniu wskazania sposobu dokonywania oceny ich spełniania.

podstawowych szkoleń z zakresu bezpieczeństwa informacji przez jednostki spełniające tak wygórowane warunki dotyczące kwalifikacji oraz doświadczenia[91]. Ponadto, ww. Inspektor w opisie przedmiotu zamówienia publicznego podał bardzo szczegółową ramową tematykę szkolenia oraz istotny wymóg organizacyjny przewidujący realizację 10 szt. odrębnych szkoleń dla pracowników Urzędu oraz dziewięciu wskazanych jednostek[92] (łącznie 96 osób).

Zdaniem NIK, określone w zapytaniu ofertowym warunki udziału i dodatkowe wymogi ograniczały zasadę uczciwej konkurencji i mogły doprowadzić do sztucznego, co najmniej 10-krotnego, zawyżenia cen wszystkich trzech ofert różniących się od siebie o 50 i 60 zł (49 900, 49 850 i 49 790 zł), tj. zaledwie o 0,1 %.

Na podstawie wyników ww. postępowania i dodatkowych ustnych uzgodnień Inspektora z wykonawcą, Wójt w umowie z dnia 13 grudnia 2024 r.[93] ustalił dla wyłonionego podmiotu znacznie korzystniejsze warunki realizacji tego zamówienia (od warunków w zapytaniu ofertowym[94]): obowiązek przeprowadzenia wyłącznie jednego (1 szt.) dwugodzinnego szkolenia (dla pracowników Urzędu i podległych jednostek) w terminie do dnia 31 grudnia 2024 r. zamiast przewidzianych w zapytaniu ofertowym 10 szkoleń w terminie do 19 grudnia 2024 r. W § 3 ust. 2 umowy wprowadzono też dodatkową możliwość zmiany terminu realizacji przedmiotu umowy, po uprzednim kontakcie pomiędzy stronami i potwierdzeniu zmiany terminu realizacji umowy przynajmniej w formie mailowej a uzgodniona w ten sposób zmiana terminu realizacji zwalniała wykonawcę z ryzyka zapłaty kar umownych za zwłokę w wykonaniu przedmiotu umowy. Ustalenie warunków realizacji przedmiotu umowy na znacznie korzystniejsze dla Wykonawcy, od warunków zawartych w zapytaniu ofertowym oraz wyznaczenie dłuższego terminu jego realizacji (podlegającego dodatkowej negocjacji) również było przejawem naruszania obowiązujących zasad uczciwej konkurencji, tj. nierównego traktowania wykonawców i prowadzenia nieprzejrzystych uzgodnień z wyłonionym wykonawcą. W wyniku zawarcia i realizacji umowy nie dopełniono wymogu udzielenia zamówienia w sposób określony w art 44 ust. 3 pkt 1 ustawy z dnia 27 sierpnia 2009 r. *o finansach publicznych*[95], co skutkowało wypłatą przez Urząd wykonawcy wynagrodzenia w wysokości 49 790 zł, zawyżonego w stosunku do ustalonej wartości rynkowej tej usługi o kwotę około 44 840 zł.

(akta kontroli str. 444-450, 457, 502-506, 521-569, 628, 640, 663-674, 756-765, 768-782, 803-804)

Inspektor wyjaśnił, że ustalając warunki udziału wykonawców w ww. postępowaniu kierował się m.in. chęcią zapewnienia pracownikom

---

[91] Według postanowień Regulaminu konkursu podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST powinny odbywać się poprzez zakup i organizację szkoleń stacjonarnych lub / i online dedykowanych dla pracowników JST zorganizowanych przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu takich szkoleń. Regulamin konkursu dopuszczał także uczestnictwo w szkoleniach poprzez zapewnienie pracownikom dostępu do platform szkoleniowych.

[92] Według zapytania ofertowego 10 szkoleń miało zostać zrealizowane do dnia 19 grudnia 2024 r.

[93] Nr 0321-123.2024 o świadczenie usług szkoleniowych o wartości 49 790 zł brutto.

[94] Z 25 listopada 2024 r.

[95] Dz.U. 2024 r., poz. 1530.

szkolenia o wysokim poziomie merytorycznym, z większą gwarancją przygotowania treści szkolenia w sposób profesjonalny i możliwością udzielenia przez Audytora Wiodącego odpowiedzi na pytania ze strony jego uczestników. Warunek posiadania doświadczenia w realizacji dwóch szkoleń z zakresu cyberbezpieczeństwa dla JST Inspektor ustalił ponieważ uznał, że podmiot szkolący, posiadający takie wcześniejsze doświadczenie będzie miał lepsze przygotowanie do realizacji szkolenia z uwzględnieniem specyfiki działania podmiotów publicznych jakim są JST. Chcąc spełnić warunek kwalifikowalności wydatku wynikający z punktu 7.3.d Regulaminu konkursu Inspektor uznał, że „twardym" poświadczeniem posiadania stosownej wiedzy jest m.in. posiadania w zasobach kadrowych osoby z certyfikatem Audytora Wiodącego, którego wiedza i doświadczenie jest potwierdzone dokumentem uzyskanym w wyniku szkolenia oraz zdania egzaminu przed jednostką certyfikującą.

Według Wójta, Zamawiający działał z pełną świadomością obowiązku stosowania *Wytycznych kwalifikowalności* w zakresie zasad ustalania wartości zamówienia Zdaniem Wójta działanie zamawiającego w zakresie ustalenia szacunkowej wartości zamówienia zawierało wszystkie cechy staranności i nie daje podstaw do twierdzenia, że doszło do naruszenia określonych przepisów, jak też nie może zostać określone jako nieprawidłowość[96], tzn. powodujące lub mogące spowodować szkodę w budżecie Unii Europejskiej. Ponadto Wójt wyjaśnił, że dłuższy niż wskazano w zapytaniu ofertowym termin realizacji umowy nr 0321-123.2024 o świadczenie usług szkoleniowych wraz z możliwością negocjacji, nie był zamierzonym działaniem Urzędu, lecz wynikiem błędu podczas sporządzania treści umowy wynikłym z zastosowania jako wzoru umowy na inną usługę szkoleniową. Harmonogram szkolenia i jego termin został ustalony z przedstawicielem Wykonawcy przez Inspektora w dniu 10 grudnia 2014 r.[97] drogą telefoniczną. Obyło się to zgodnie z ustaleniami poczynionymi w korespondencji mailowej z przedstawicielem Wykonawcy 9 grudnia 2024 r. W tejże rozmowie telefonicznej ustalono termin szkolenia na dzień 16 grudnia 2024 r. i w tym dniu szkolenie się odbyło. Według Wójta Inspektor podczas telefonicznego ustalania terminu szkolenia z Wykonawcą pilnował jego zgodności z zapisami zapytania ofertowego. Przez nieuwagę Inspektora sporządzającego umowę w jej treści pojawiły się zapisy wskazujące na terminy wykraczające poza ustalenia zapytania ofertowego i miało to związek z wykorzystaniem jako wzoru dla tej umowy innej umowy na usługę szkoleniową. Zdaniem Wójta Urząd prowadził postępowanie w sposób niezakłócający zachowanie uczciwej konkurencji.

(akta kontroli str. 686-690, 939-944)

Odnosząc się do powyższych wyjaśnień NIK wskazuje, że certyfikat Audytora Wiodącego nie był jedynym certyfikatem potwierdzającym zgodność ze standardami lub wymaganiami branży cyberbezpieczeństwa i bezpieczeństwa

[96] W rozumieniu art. 2 pkt 36 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z 17.12.2013 r. *ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego, oraz ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylające rozporządzenie Rady (WE) nr 1083/2006* (Dz.Urz.UE.L.347.2013.320).

[97] Winno być 2024 r. – uwaga NIK.

informacji. Oprócz niego w warunkach wolnorynkowych funkcjonowały wówczas inne certyfikaty takie jak CISSP[98], CISM®[99], CISA[100], CIA[101] wymienione przez Ministra Cyfryzacji w Wykazie certyfikatów uprawniających do przeprowadzania audytu[102] a także CEH[103] i CompTIA Security+[104].

Zdaniem NIK, wszystkie ww. certyfikaty potwierdzały odpowiedni poziom merytoryczny osoby trenera, możliwość profesjonalnego przygotowania treści szkolenia oraz możliwość zadawania pytań. Nadto NIK wskazuje, że spełnienie oczekiwanych przez Urząd warunków formalnych w praktyce nie było weryfikowalne ponieważ w zapytaniu ofertowym i umowie nie zamieszczono opisu dokonywania oceny spełniania warunków w zakresie kwalifikacji (certyfikatu) i doświadczenia. Wskutek tego Inspektor dopuścił do przeprowadzenia szkolenia inną osobę niż wskazaną w ofercie wybranego wykonawcy, która nie dysponowała wymaganym doświadczeniem w przeprowadzaniu szkoleń w JST.

Zdaniem NIK, ograniczenie tego warunku do szkoleń prowadzonych wyłącznie w JST także było nieadekwatne bowiem analogiczne zasady w zakresie cyberbezpieczeństwa dotyczą działalności ogółu podmiotów publicznych, w tym jednostek samorządowych.

Zgodnie z § 5 ust. 6 umowy grantowej kwoty wykorzystane przez grantobiorcę z naruszeniem procedur (tj. m.in.: postanowień umowy, wytycznych, o których mowa w § 4 ust. 1 pkt 1 lit. a i b i innych dokumentów programowych dotyczących FERC), pobrane w nadmiernej wysokości, jako wydatki niekwalifikowalne podlegają zwrotowi wraz z odsetkami w wysokości określonej jak dla zaległości podatkowych.

(akta kontroli str. 23-24, 289-290, 502-503)

8. Opracowana i wdrożona w dniu 24 lipca 2023 r. *Polityka Bezpieczeństwa Teleinformatycznego w Urzędzie*[105], stanowiąca wprowadzenie SZBI wytwarzanych i przetwarzanych przez Gminę, zawierała wewnętrznie sprzeczne, niezgodne z prawem oraz nierzetelne postanowienia i zapisy. Z jednej strony Zarządzenie było wewnętrznym dokumentem wykonawczym Wójta jako kierownika jednostki budżetowej (Urzędu), przy pomocy której wykonywał on gminne zadania publiczne[106] a z drugiej strony, zgodnie z tytułem Załącznika, metryką dokumentu oraz § 1 ust. 1 i ust. 3 pkt 1 *Polityki* miała ona stanowić akt prawodawstwa ukierunkowanego na informacje wytwarzane i przetwarzane

---

[98] Certified Information Systems Security Professional - certyfikat w obszarze bezpieczeństwa teleinformatycznego potwierdzający ekspercką wiedzę z zakresu zarządzania cyberbezpieczeństwem organizacji.

[99] Certified Information Security Manager - certyfikat ten potwierdza wiedzę i doświadczenie w zakresie zarządzania bezpieczeństwem informacji, tworzenia i zarządzania programami bezpieczeństwa informacji, zarządzania incydentami bezpieczeństwa i zarządzania ryzykiem.

[100] Cerified Information System Auditor.

[101] Certified Internal Auditor.

[102] Załącznik do rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. *w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu* (Dz.U. poz. 1999).

[103] Certified Ethical Hacker (pol. Certyfikowany Etyczny Haker) – specjalista pracujący zazwyczaj w środowisku 'red team', skoncentrowany na atakowaniu systemów komputerowych i uzyskiwaniu dostępu do sieci, aplikacji, baz danych i innych krytycznych danych w zabezpieczonych systemach.

[104] Certyfikat, który potwierdza podstawową wiedzę i umiejętności z zakresu bezpieczeństwa IT.

[105] Załącznik nr 1 do Zarządzenia nr W.0050.155.2023 Wójta z 24 lipca 2023 r. Dalej: *Polityka*.

[106] Patrz: tytuł Zarządzenia z 24 lipca 2023 r. oraz postanowienie § 1 Zarządzenia.

przez Gminę, której pojęcia na potrzeby wdrażanej Polityki nie zdefiniowano[107]. Zdaniem NIK, było to także niezgodne z § 20 ust. 1 *rozporządzenia KRI z 2012 r.*, bowiem przepis ten przewidywał, że każdy podmiot realizujący zadania publiczne (a zatem osoba kierująca każdą jednostką organizacyjną Gminy) miał obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji[108]. W ramach wprowadzonego SZBI Wójt nie zapewnił w *Polityce* warunków – procedury przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko (stosownie do wyników przeprowadzonej analizy), do czego zobowiązywał § 20 ust. 2 pkt 3 *rozporządzenia KRI z 2012 r.* Jako nierzetelne NIK ocenia m.in., że:

(-) w *Polityce*, nie ustalono i nie wskazano osoby odpowiadającej za jej opracowanie (jej autora), wdrożenie, ocenę i przeglądy. Zdaniem NIK osobą odpowiadającą za ww. trzy ostatnie czynności był ASI. W *Polityce* określono bowiem, że ASI Urzędu odpowiadał zasadniczo za techniczną sferę funkcjonowania procedur bezpieczeństwa i uwierzytelniania dostępu do systemów teleinformatycznych; kontrolę przepływu informacji w postaci elektronicznej; utrzymanie systemów w należytym stanie i wykonywanie okresowych konserwacji sprzętu IT, systemów, aplikacji oraz elektronicznych nośników służących do zapisu danych osobowych; tworzenie kopii zapasowych zasobów danych osobowych, programów oraz za okresowe sprawdzanie ich poprawności dla zapewnienia ciągłości zarządzania;

(-) w § 1 ust. 4 pkt 13 *Polityki* w sposób nieodpowiedni do stanu faktycznego zdefiniowano miejsce działania sieci lokalnej LAN (tj. jako urząd, szkołę, laboratorium, biuro) oraz nie określono jej zakresu[109] i sposobu działania[110];

(-) w *Polityce*, pomimo iż stanowiła ona wdrożenie SZBI nie zdefiniowano pojęć oraz rodzajów innych informacji (danych) niemających cech danych osobowych, gromadzonych i przetwarzanych w systemach teleinformatycznych Urzędu[111].

(akta kontroli str. 172-173, 201-242)

Odnosząc się do powyższej nieprawidłowości Wójt podał m.in., że

- w nowo przygotowanej dokumentacji wadliwe sformułowania zostaną ujednolicone w sposób jasno wskazujący, że Polityka służy do wewnętrznych regulacji kwestii bezpieczeństwa informacji w Urzędzie (jako jednostce), zaś zakres podmiotowego obowiązywania dokumentacji zostanie odpowiednio doprecyzowany,

---

[107] Jak również nie wskazano gminnych jednostek organizacyjnych (nazw), w których miała obowiązywać ww. *Polityka*.

[108] W obecnie obowiązującym stanie prawnym analogiczne obowiązki podmiotu realizującego zadania publiczne (w tym wójta jako organu administracji publicznej i gminy jako osoby prawnej) wynikają z § 19 ust. 1 i 2 w związku z § 2 pkt 13 rozporządzenia Rady Ministrów z 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* (Dz.U., poz. 773), stosownie do art. 30 ust. 1 i art. 31 ustawy z dnia 8 marca 1990 r. *o samorządzie gminnym* (Dz.U z 2024 r., poz. 1465).

[109] Np. sieć łącząca urządzenia sieciowe wyłącznie w ramach Urzędu lub w całym budynku lub urządzenia położone w wielu budynkach.

[110] Sieć przewodowa i/lub bezprzewodowa.

[111] Np. dane geodezyjne, ewidencja oraz dokumentacja księgowa i finansowa, rejestry i informacje publiczne.

- zostaną doprecyzowane lub zmienione definicje ADO, ASI i sieci LAN Urzędu oraz zostanie wprowadzona nowa definicja informacji podlegających ochronie, innych niż dane osobowe,
- zostanie przeprowadzona weryfikacja zakresów obowiązków pracowników Urzędu i dostosowanie do rzeczywistych zadań i zajmowanych stanowisk,
- nadzór nad wdrażaniem nowej dokumentacji SZBI, w tym Polityki zostanie wzmocniony i powierzony Sekretarzowi Gminy,
- opracowanie procedur przeprowadzania analiz ryzyka zostanie uwzględnione w podczas opracowania nowej dokumentacji SZBI.

(akta kontroli str. 609-616)

9. Niezapewnienie przez Wójta przeprowadzenia w 2024 r. w Urzędzie audytu wewnętrznego w zakresie bezpieczeństwa informacji do czego zobowiązywał § 20 ust. 2 pkt 14 rozporządzenia KRI z 2012 r. (do 23 maja 2024 r.) oraz §19 ust. 2 pkt 14 rozporządzenia KRI z 2024 r. (od 23 maja 2024 r.). Według wyjaśnień Wójta powodem nieprzeprowadzenia audytu był m.in. brak zatrudnienia w Urzędzie odpowiedniej osoby posiadającej kompetencje do przeprowadzenia audytu wewnętrznego, jak też brak wystarczającej świadomości w przedmiotowym zakresie pracowników merytorycznych odpowiedzialnych za tę tematykę. Wójt poinformował, że audyt ten zostanie przeprowadzony bezzwłocznie i zostanie ujęty w planach działań na kolejne lata.

(akta kontroli str. 939-944)

NIK, odnosząc się do wyjaśnień Wójta, wskazuje, że brak zatrudnienia w Urzędzie audytora wewnętrznego nie może być uzasadnieniem braku realizacji ustawowych obowiązków. Tym bardziej, że zgodnie z art. 274 ust. 3 ustawy *o finansach publicznych*, w związku z § 1 uchwały nr 483/LXXIV/23 Rady Gminy z dnia 14 grudnia 2023 r. *w sprawie budżetu Gminy Świerklany na rok 2024*[112] jednostka ta była ustawowo zobowiązana do prowadzenia w 2024 r. audytu wewnętrznego. Zgodnie z art. 275 ww. ustawy audyt wewnętrzny może prowadzić audytor zatrudniony w jednostce albo zewnętrzny usługodawca - niezatrudniony w jednostce, spełniający wymogi określone w art. 286 ustawy.

(akta kontroli str. 945)

10. Realizacja przez Kierownika Referatu Rozwoju i Promocji Gminy w Urzędzie obowiązków w zakresie informowania i promowania dofinansowania uzyskanego na realizację Projektu odbywała się w sposób niezgodny z §11 umowy grantowej lub nierzetelny. Na podstawie wyników przeprowadzonych w dniach 7 i 9 maja 2025 r. oględzin stwierdzono bowiem, że:
- w mediach społecznościowych Urzędu (Gminy)[113] przez ponad rok od dnia. zawarcia umowy grantowej (tj. od 18 kwietnia 2024 r.) nie zamieszczono informacji o uzyskaniu unijnego dofinansowania do realizacji Projektu i jego opisu, co było obowiązkiem wynikającym z §11 ust. 4 pkt 3 umowy;
- informacja o pozyskaniu środków Programu FERC i celach Projektu[114] znajdująca się na stronie internetowej Urzędu także nie zawierała wymaganego

[112] Dz. Urz. Woj. Śl. z 19 grudnia 2023 r., poz. 9804.
https://dzienniki.slask.eu/WDU_S/2023/9804/akt.pdf (dostęp: 17.06.2025 r.).
[113] W serwisach [...] oraz [...].
[114] Ogólnym i pięciu celach szczegółowych.

umową opisu Projektu a podana w niej kwota dofinansowania (850 tys. zł) była niezgodna z wnioskiem o przyznanie grantu, według którego wynosiła ona 781 724,01 zł;
- w informacji opublikowanej w gminnym biuletynie informacyjnym z grudnia 2024 r.[115] także podano ww. niewłaściwą (zawyżoną o 8,7 %) kwotę pozyskanych środków finansowych;
- do chwili przeprowadzenia oględzin[116] wszystkie trzy plakaty informacyjne[117] znajdujące się na terenie budynku Urzędu (o odpowiedniej formie graficzno-kolorystycznej) zawierały nierzetelną kwotę przyznanego dofinansowania Projektu ze środków UE (podano kwotę łącznego dofinasowania 781 724,01 zł zamiast kwoty wkładu UE wynoszącego 656 648,19 zł).

(akta kontroli str. 35-36, 244-253, 257-261, 263)

Ww. Kierownik wyjaśnił, że brak zamieszczenia obowiązkowej informacji o uzyskaniu unijnego dofinansowania do realizacji Projektu jak też jego opisu w mediach społecznościowych Urzędu, opublikowanie nierzetelnych informacji na stronie internetowej Gminy i w gminnym biuletynie informacyjnym oraz wywieszenie na terenie Urzędu błędnych plakatów informacyjnych wynikał z jego niedopatrzenia. Kierownik poinformował, że wymagana informacja na koncie [...] Urzędu została uzupełniona 14 maja 2025 r. zaś niedopatrzenie stwierdzone na koncie [...] zostanie naprawione przy tworzeniu najbliższego odcinka filmu informacyjno-promocyjnego pn. „Echa Regionu Świerklany". Błędne kwoty w komunikacie na stronie internetowej oraz w treści plakatów zostały poprawione w dniu 13 maja 2025 r. natomiast niedopatrzenie związane z wadliwą informacją w „Kurierze Gminy Świerklany" zostanie naprawione poprzez zamieszczenie nowej, prawidłowej publikacji w jego lipcowym wydaniu.

(akta kontroli str. 264-270)

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

1. Zapewnienie przestrzegania postanowień umowy grantowej, zobowiązujących Gminę do stosowania odpowiednich trybów lub procedur udzielania zamówień publicznych wynikających z ustawy PZP, Wytycznych kwalifikowalności i wewnętrznych regulaminów Urzędu.
2. Terminowe potwierdzanie odbioru wykonania przedmiotu umów o zamówienia publiczne.

Wnioski

1. Zapewnienie przeprowadzania w Urzędzie corocznego okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.
2. Doprowadzenie do pełnej zgodności realizacji obowiązków w zakresie informowania i promowania dofinansowania uzyskanego na realizację Projektu, przestrzegając §11 umowy grantowej.

---

[115] W numerze 4 (120), który został także udostępniony na stronie internetowej Gminy: https://swierklany.pl/kurier-rok-2024.html (dostęp w dniu 12 maja 2025 r.).
[116] 9 maja 2025 r.
[117] Wymagane § 11 ust. 4 pkt 2 umowy grantowej.

3. Zwrot środków grantu pobranych przez Gminę w nadmiernej wysokości z tytułu niespełniania przez wskazane wydatki warunków kwalifikowalności (poniesionych bez zastosowania przepisów ustawy PZP lub z naruszeniem procedur i wytycznych FERC) wraz z odsetkami, w wysokości określonej jak dla zaległości podatkowych, stosownie do postanowień § 10 ust. 16 w związku z ust. 1 umowy grantowej.
4. Przekazanie NASK brakującej Ankiety Dojrzałości Cyberbezpieczeństwa i skorygowanie jednej z przekazanych Ankiet, zawierającej nierzetelne informacje.

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 Najwyższej Izby Kontroli w Katowicach. 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.

Katowice, dnia 9 września 2025 r.

Kontroler

Artur Stekla

Gł. specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Delegatura w Katowicach

p.o. Dyrektor

Marcin Wesoły

/podpisano elektronicznie/