NAJWYŻSZA IZBA KONTROLI

Delegatura w Katowicach

LKA.410.12.1.2025

Dawid Rams
Starosta Gliwicki
Starostwo Powiatowe w Gliwicach,
ul. Zygmunta Starego 17, 44-100
Gliwice

WYSTĄPIENIE POKONTROLNE

P/25/003 – Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Delegatura w Katowicach
Ul. Powstańców 29, 40-039 Katowice
+48 32 784 42 00, lka@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Starostwo Powiatowe w Gliwicach, ul. Zygmunta Starego 17, 44-100 Gliwice[1]
Kierownik jednostki kontrolowanej	Dawid Rams, Starosta Gliwicki[2] od dnia 7 maja 2024 r. do chwili obecnej. Wcześniej, od dnia 27 października 2022 r. stanowisko *Starosty* zajmował Włodzimierz Gwiżdż.
Zakres przedmiotowy kontroli	Realizacja przez gminy i powiaty działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych w 2025 r.
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	Michał Nowak, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LKA/83/2025 z 5 maja 2025 r.

(akta kontroli str. 1-2)

[1] Dalej: *Starostwo* lub *Starostwo Powiatowe*.
[2] Dalej: *Starosta* lub *Starosta Gliwicki.*
[3] Dz. U. z 2022 r. poz. 623, dalej: *ustawa o NIK.*

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w badanym zakresie.

Uzasadnienie oceny ogólnej

W dokumentach strategicznych *Starostwa* nie uwzględniono wprost zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa w jednostce, jednakże zawarto w nich zapisy pośrednio odnoszące się tego zagadnienia. Rozpoznawanie potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa realizowane było na bieżąco, w ramach dostępnego budżetu, a także w związku z projektami dofinansowanymi ze środków zewnętrznych.

Starostwo Powiatowe przekazywało do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego[5] *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego*[6] zgodnie z wymogami umowy[7] o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0682/FERC.02.02-CS.01-001/23/2024[8] oraz *Regulaminu Konkursu Grantowego Cyberbezpieczny Samorząd*[9].

Środki z dofinansowania Projektu Cyberbezpieczny Powiat Gliwicki[10] zostały wykorzystane zgodnie z postanowieniami *Umowy,* choć w ramach jednego z zadań zakupiono dwa dodatkowe urządzenia access point. Były one jednak niezbędne dla zapewnienia pełnej integralności środowiska i bezpieczeństwa sieci bezprzewodowej.

W realizacji *Projektu* brały udział dwie jednostki organizacyjne Starostwa w zakresie umieszczenia ich zasobów na serwerach *Starostwa* oraz 12 jednostek w zakresie przekazania zakupionego oprogramowania antywirusowego. W związku z realizacją *Projektu* wyznaczono pracowników odpowiedzialnych za jego realizację. Ich liczba nie ulegała zmianie w okresie od rozpoczęcia realizacji *Projektu.* Dla realizowanego *Projektu* ustalono wskaźniki produktu i rezultatu, adekwatne do realizowanych działań. Zakupione przez *Starostwo* urządzenia oraz oprogramowanie zostały uruchomione (zainstalowane) i były wykorzystywane przez kontrolowaną jednostkę.

W *Starostwie Powiatowym* opracowano, ustanowiono i wdrożono System Zarządzania Bezpieczeństwem Informacji, na który składała się Polityka Bezpieczeństwa Informacji oraz Instrukcja zarządzania systemem informatycznym. Podlegały one corocznym przeglądom, zgodnie wewnętrznymi regulacjami jednostki kontrolowanej.

W badanym okresie w *Starostwie* przeprowadzane były okresowe audyty wewnętrzne z zakresu bezpieczeństwa informacji, realizowane przez osoby posiadające wymagane kompetencje.

Starostwo Powiatowe realizowało obowiązki informacyjne wynikające z *Umowy* w związku z dofinansowaniem na realizację *Projektu*.

---

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

[5] Dalej: *NASK.*

[6] Dalej: *Ankieta Dojrzałości Cyberbezpieczeństwa.*

[7] Dalej: *Umowa o powierzeniu grantu* lub *Umowa.*

[8] Zgodnie z §19 ust. 4 *Umowy o powierzenie grantu*, została ona zawarta i wchodzi w życie z dniem podpisania przez ostatnią ze Stron, tj. 2 maja 2024 r.

[9] Dalej: *Regulamin Konkursu.*

[10] Dofinansowanego w ramach Konkursu grantowego *Cyberbezpieczny Samorząd*, dalej: *Projekt.*

III. Opis ustalonego stanu faktycznego

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

Opis stanu faktycznego

1. Uwzględnienie w dokumentach strategicznych *Starostwa* zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa.

W okresie objętym kontrolą, w *Starostwie Powiatowym* obowiązywał dokument strategiczny pt. *Kierunki Strategicznego Rozwoju Powiatu Gliwickiego w perspektywie roku 2035*[11]. Na potrzeby *Starostwa* sporządzane były także roczne plany celów i zadań priorytetowych oraz rejestry ryzyk. W dokumentach tych nie zawarto zapisów bezpośrednio odnoszących się do zwiększenia poziomu cyberbezpieczeństwa. Jak wyjaśnił *Starosta*: *W dokumentach strategicznych nie zapisano wprost zagadnienia „zwiększanie poziomu cyberbezpieczeństwa". Działania w zakresie cyberbezpieczeństwa wpisują się pośrednio w kierunek działania związany m.in. z nowymi technologiami, e-usługami czy e-administracją. W Uchwale*(...)*wymienione są m.in. kierunki:*
K1.1.2. Wdrażanie technologii inteligentnego zarządzania powiatem ułatwiających mieszkańcom pozyskiwanie informacji i korzystanie z e-usług;
K.1.3.5. Wykorzystywanie współpracy międzynarodowej dla podnoszenia kapitału wiedzy powiatu oraz przyciągania podmiotów kreujących i wykorzystujących nowoczesne technologie;
K.2.3.13. Wdrażanie i promowanie rozwiązań w zakresie e-usług i e-administracji. Kwestie związane z zachowaniem cyberbezpieczeństwa traktujemy jako oczywiste, związane ze sprawnym, bieżącym funkcjonowaniem powiatu. Podobne podejście zastosowano przy określaniu rocznych planów celów i zadań priorytetowych oraz rejestrów ryzyk, zakładając iż zapewnienie bezpieczeństwa informacji (w tym cyberbezpieczeństwa) należy do podstawowych obowiązków powiatu i jako takie nie jest działaniem strategicznym.
Starosta Gliwicki wskazał również, że w jednostce obowiązywały dokumenty o charakterze strategicznym i operacyjnym dotyczące konkretnych dziedzin funkcjonowania samorządu powiatowego[12]. Ww. dokumenty strategiczne i operacyjne nie posiadały odniesień do zagadnień związanych z zapewnieniem cyberbezpieczeństwa. Zastosowano tu opisane powyżej podejście, identyczne jak w przypadku *Kierunków Strategicznego Rozwoju Powiatu Gliwickiego w perspektywie roku 2035* oraz planów celów i zadań priorytetowych oraz rejestrów ryzyk.
Starosta dodał: *Należy jednak wspomnieć, iż zagadnienia związane z zapewnieniem cyberbezpieczeństwa ujęte są w obowiązującym Planie Zarządzania Kryzysowego Powiatu Gliwickiego. W Procedurach Reagowania Kryzysowego ujęto zakres Przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CPR (Stopień alarmowy CRP jest wprowadzany w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej):*

Procedura 7.5. - Szczegółowe przedsięwzięcia na wypadek wprowadzenia I stopnia alarmowego CRP (ALFA - CRP);

Procedura 7.6. - Szczegółowe przedsięwzięcia na wypadek wprowadzenia II stopnia alarmowego CRP (BRAVO – CRP);

Procedura 7.7. - Szczegółowe przedsięwzięcia na wypadek wprowadzenia III stopnia alarmowego CRP (CHARLIE - CRP).

Ponadto (...) *Starosta udzielił akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego pk. „WIARUS-1" przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" przez zatwierdzenie dokumentacji*

[11] Przyjęty Uchwałą Rady Powiatu Gliwickiego Nr XXXIV/272/2021 z dnia 16 grudnia 2021 r. *w sprawie przyjęcia programu rozwoju strategicznego pod nazwą Kierunki Strategicznego Rozwoju Powiatu Gliwickiego w perspektywie roku 2035.*
[12] Np. Strategia Rozwiązywania Problemów Społecznych Powiatu Gliwickiego na lata 2021-2026.

bezpieczeństwa systemu teleinformatycznego: Szczególne Wymagania Bezpieczeństwa i Procedury Bezpiecznej Eksploatacji. Dokumenty zostały przedstawione i zaakceptowane przez Agencję Bezpieczeństwa Wewnętrznego. Kierownik jednostki wyznacza Inspektora Bezpieczeństwa Teleinformatycznego oraz Administratora Systemu Teleinformatycznego.

(akta kontroli str. 9, 12, 68-271, 350-625, 696, 700-701, 741-767)

2. Rozpoznawanie potrzeb w zakresie zwiększenia poziomu cyberbezpieczeństwa.

Opis stanu faktycznego

W kwestii określania potrzeb *Starostwa* dot. zwiększenia poziomu cyberbezpieczeństwa, *Starosta Gliwicki* wyjaśnił: *Powiat Gliwicki nie posiada sformalizowanego planu realizacji zadań z zakresu cyberbezpieczeństwa.* Zapewnienie cyberbezpieczeństwa w Starostwie należało do zadań Biura Informatyki, które (...) wykonywało m.in. następujące zadania:

- planowanie rozwoju systemów informatycznych;
- tworzenie infrastruktury teleinformatycznej;
- zakupy sprzętu i podzespołów;
- zapewnienie bezpiecznych warunków przetwarzania danych elektronicznych w systemie komputerowym (ochrona przed utratą lub nieuprawnionym dostępem);
- zapewnianie integralności danych w systemie informatycznym;
- zapewnianie ciągłości działania systemów informatycznych i łączy internetowych;
- zapewnianie i utrzymywanie w sprawności narzędzi informatycznych dla końcowych użytkowników systemu;
- odpowiedzialność za bezpieczeństwo informatyczne;

Starosta dodał, że: *Potrzeby sprzętowe oraz związane z zakupem oprogramowania, w tym oprogramowania do zapewnienia cyberbezpieczeństwa, dla Starostwa Powiatowego* (...) *określa Biuro Informatyki, uwzględniając koszty z tym związane w planach budżetu na kolejne lata. Mając na uwadze ograniczone środki finansowe Starostwa Biuro Informatyki we współpracy z Wydziałem Inwestycji, Funduszy i Zamówień Publicznych (właściwym m.in. dla zarządzania projektami dofinansowanymi ze środków zewnętrznych) występuje o przyznanie dofinansowania na działania związane m.in. z zapewnieniem cyberbezpieczeństwa. W 2023 r. zrealizowano projekt „Cyfrowy Powiat", w ramach którego zakupiono m.in. oprogramowanie typu SIEM i SOAR oraz przeszkolono pracowników w zakresie cyberbezpieczeństwa. W ramach projektu przeprowadzono również diagnozę cyberbezpieczeństwa. Realizowany obecnie projekt „Cyberbezpieczny Powiat Gliwicki" jest naturalną kontynuacją podejmowanych wcześniej działań. Informuję również, iż w 2024 r. został złożony projekt „Podniesienie jakości treści cyfrowych oraz rozwój e-usług w Powiecie Gliwickim" dotyczący przede wszystkim tworzenia/ modernizacji e-usług świadczonych przez Powiat Gliwicki, gdzie również zostały ujęte kwestie związane z cyberbezpieczeństwem. Projekt znajduje się obecnie w trakcie oceny.* (...) *potrzeby diagnozowane są na bieżąco i realizowane w ramach dostępnego budżetu, w tym w ramach projektów dofinansowanych ze środków zewnętrznych.*

(akta kontroli str. 9, 12-13, 696, 701-702, 768-870)

3. Przekazywanie do *NASK Ankiet Dojrzałości Cyberbezpieczeństwa.*

Opis stanu faktycznego

Starostwo, zgodnie z zapisami §4 ust. 1 pkt 4 ppkt a) *Umowy o powierzenie grantu*, przekazało *Ankietę Dojrzałości Cyberbezpieczeństwa* do *NASK* w terminie nieprzekraczającym 30 dni od dnia zawarcia ww. umowy[13]. Korekty ww. Ankiety, na wniosek *NASK* zostały przesłane przez *Starostwo Powiatowe* 6, 18 i 26 czerwca 2024 r. *Ankiety dojrzałości Cyberbezpieczeństwa* przesyłano każdorazowo na adres skrytki *NASK*: /NASK-Instytut/SkrytkaESP (temat: *przekazanie ankiety cyberbezpieczeństwa*). Były one zgodne z wzorem określonym w zał. Nr 6 do *Regulaminu Konkursu.*

(akta kontroli str. 954, 971-975, 1044, 1052, 1073-1079,1082-1155)

4. Prawidłowość wykorzystania środków z grantu na zwiększenie poziomu bezpieczeństwa informacji.

Opis stanu faktycznego

Warunki dofinansowania w ramach Konkursu grantowego *Cyberbezpieczny Samorząd* określała *Umowa o powierzenie grantu* zawarta pomiędzy Skarbem Państwa, w imieniu którego działało Centrum Projektów Polska Cyfrowa[14], a Powiatem Gliwickim[15]. Z grantu miała być dofinansowana realizacja *Projektu. Projekt*, zgodnie z wnioskiem o powierzenie grantu[16] złożonym przez *Starostwo Powiatowe* miał na celu zwiększenie poziomu bezpieczeństwa cyfrowego w *Starostwie* i dwóch jednostkach organizacyjnych *Powiatu* i zakładał zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych. *Starostwo* zobowiązało się zrealizować *Projekt* w zakresie rzeczowym wynikającym z *Wniosku* w okresie maksymalnie 24 miesięcy od dnia wejścia w życie *Umowy*, ale nie dłużej niż do 30 czerwca 2026 r.

W ramach *Projektu* przewidziano następujące działania[17]:

- Zadanie 1 – Zakup, wdrożenie, konfigurację oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa – zakup i wdrożenie UTM[18] wraz z przełącznikami zarządzalnymi i ich utrzymanie i przeszkolenie personelu służb informatycznych. Realizacja zadania miała polegać na zakupie switchy zarządzalnych oraz UTM nowej generacji i zastąpieniu aktualnie posiadanych, którym kończyło się wsparcie producenta. Zakup nowych urządzeń, poza aktualną asystą producenta (aktualizacje i dłuższe wsparcie serwisowe), pozwolić miał na zwiększenie bezpieczeństwa ruchu sieciowego. Urządzenia nowej generacji miały zapewnić wyższą wydajność i skuteczność pod kątem ochrony przy jak najniższych opóźnieniach (szyfrowanie/deszyfracja protokołów SSL, inspekcja IPS, inspekcja aplikacji itd.). Zwiększeniu miała ulec liczba stacji końcowych bezpośrednio wpiętych do switchy zarządzanych w sieci. Zastosowanie tych urządzeń pozwolić miało na zastąpienie wielu rozwiązań typu: zapora sieciowa, filtry antyspamowe itp. jednym urządzeniem łączącym wszystkie te funkcje u użytkowników niepodłączonych do tej pory do posiadanej już infrastruktury.

[13] Zgodnie z §19 ust. 4 *Umowy o powierzenie grantu*, została ona zawarta i wchodzi w życie z dniem podpisania przez ostatnią ze Stron, tj. 2 maja 2024 r.; Data doręczenia *Ankiety Dojrzałości Cyberbezpieczeństwa*: 24 maja 2024 r.

[14] Określone w *Umowie* jako *Beneficjent, Grantodawca* lub *CPPC.*

[15] Określonym w *Umowie* jako *Grantobiorca.*

[16] Dalej: *Wniosek.*

[17] Opisane w zaakceptowanym *Wniosku*.

[18] Unified threat management – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia.

Przeszkolenie personelu miało pozwolić w odpowiedni sposób zarządzać ww. urządzeniami, co miało wpłynąć na zwiększenie bezpieczeństwa cyfrowego w *Starostwie*. Szacunkowa wartość zadania: 340 448,10 zł brutto.

- Zadanie 2 – Zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC). Realizacja zadania miała polegać na zakupie, wdrożeniu i utrzymaniu środowiska wirtualnego (serwery, macierze, licencje systemów operacyjnych i silników wirtualizacyjnych, zasilaczy awaryjnych ups) i przeszkolenie personelu służb informatycznych. W ramach zadania przewidziano rozszerzenie gwarancji (wydłużenie wsparcia do 24 miesięcy oraz rozszerzenie gwarancji o naprawę na miejscu instalacji serwera w następnym dniu roboczym po zgłoszeniu awarii). Realizacja zadania miała obniżyć koszty w jednostkach podległych przez nietworzenie serwerowni w różnych lokalizacjach, a jedynie w budynku *Starostwa Powiatowego*. Powstała infrastruktura miała stanowić zalążek dla stworzenia Centrum Usług Wspólnych dla *Starostwa*, Powiatowego Centrum Pomocy Rodzinie[19] i Zarządu Dróg Powiatowych[20] (jednostek organizacyjnych Powiatu Gliwickiego). Nowe zasoby umieszczone w serwerowni *Starostwa* jak i wszystkie już użytkowane w *Starostwie* miały być zabezpieczone pod kątem: niepowołanych dostępów (przez UTM, antywirus), utraty danych (backupy), braku zasilania (przez UPS). Do umieszczanych na tej infrastrukturze danych (baz danych programów i współdzielonych dokumentów) miał być zapewniony dużo szybszy, wygodniejszy dostęp użytkowników posiadających uprawienia dostępu. Szacunkowy koszt zadania: 503 999,65 zł brutto.
- Zadanie 3 – Zakup, wdrożenie i utrzymanie systemów teleinformatycznych – zakup oraz wdrożenie licencji posiadanego oprogramowania antywirusowego w wyższej wersji i przeszkolenie personelu służb informatycznych. Realizacja zadania miała polegać na zakupie oraz wdrożeniu wyższej wersji oprogramowania antywirusowego wraz z licencją na jego aktualizację. Wyższa wersja programu miała pozwolić przede wszystkim na pełne zabezpieczenie poczty elektronicznej poprzez skanowanie załączników pod kątem zagrożeń przed dostarczeniem ich do końcowego użytkownika, a także umożliwienie szyfrowania dysków twardych we wszystkich komputerach przenośnych wykorzystywanych w jednostkach *Starostwa*, co zapewniało bezpieczeństwo przechowywania danych. Konsekwencją rozbudowania do wyższej wersji miała być również chmurowa konsola do zarządzania, umożliwiająca zdalny dostęp do takich funkcji jak: instalacja oprogramowania, podgląd stanu ochrony sieci i zabezpieczonych urządzeń. Szacunkowy koszt zadania: 99 996,25 zł brutto.

Łączna wartość *Projektu*, zgodnie z *Wnioskiem* wynosiła 944 444,00 zł, z tego 850 000,00 zł z dofinansowania oraz 94 444,00 zł ze środków własnych. Dofinansowanie, zgodnie z §2 ust. 1 *Umowy* stanowiło 90.00% (w tym: dofinansowanie ze środków Unii Europejskiej: 76.50%, oraz dofinansowanie z budżetu państwa: 13.50%) kwoty wydatków kwalifikowalnych *Projektu*. Kwota środków otrzymanych z dofinansowania w ramach *Projektu* była zgodna z *Umową o powierzenie grantu* i wyniosła 850 000,00 zł. Łączna kwota środków

[19] Dalej: *PCPR.*
[20] Dalej: *ZDP.*

wykorzystanych[21] w ramach *Projektu* wyniosła 993 002,37 zł[22] i objęła następujące działania:

a) Zadanie 1 (301 397,97 zł[23]):
   - Dostawa urządzeń: Fortinet FortiGate 400F (2 szt.)[24], Fortinet FortiSwitch 1024E (1 szt.)[25], Fortinet FortiSwitch 148F stacjonarnych (4 szt.)[26], Fortinet FortiAP 431F (2 szt.)[27] oraz licencje i serwis;
   - Aktualizacje dla posiadanych urządzeń FortiSwitch i punktów dostępowych FortiAP;
   - Szkolenie dla informatyków zatrudnionych w *Starostwie.*

b) Zadanie 2 (639 329,40 zł[28]):
   - Dostawa urządzeń: Serwer (3 szt.), macierz (1 szt.), zasilacz awaryjny RACK (3 szt.) oraz gwarancja;
   - Dostawa oprogramowania – serwerowy system operacyjny;
   - Instalacja i konfiguracja dostarczonych urządzeń i oprogramowania;
   - Przeprowadzenie szkolenia (instruktaż) dla informatyków zatrudnionych w *Starostwie.*

c) Zadanie 3 (52 275,00 zł[29]):
   - Dostawa wraz z wdrożeniem 500 licencji oprogramowania antywirusowego w wersji ESET Protect Advanced;
   - Szkolenie (instruktaż) dla informatyków zatrudnionych w *Starostwie.*

Łączna wartość urządzeń teleinformatycznych zakupionych w ramach *Projektu*[30] wyniosła 797 818,17 zł i stanowiła 93,86% łącznej wartości grantu.

Wszystkie ww. zadania zostały wykonane w terminach określonych w umowach z wykonawcami[31].

Urządzenia i oprogramowanie zakupione w związku z Zadaniami 2 i 3 były zgodne z *Wnioskiem*. W ramach Zadania 1 zakupione zostały dodatkowo dwa urządzenia Fortinet FortiAP 431F[32], nieujęte we *Wniosku. Starosta Gliwicki* wyjaśnił, że ww. urządzenia zakupiono dla zapewnienia pełnej integralności

---

[21] Obszar kompetencyjny i obszar techniczny.

[22] Z tego 850 000,00 zł z dofinansowania *Projektu*, 94 444,00 zł ze środków własnych *Starostwa* (wydatki kwalifikowalne) oraz 48 558,37 zł ze środków własnych (wydatki niekwalifikowalne, co opisano niżej).

[23] Z tego 271 258,30 zł z dofinansowania *Projektu* oraz 30 139,67 zł wkładu własnego (wydatki kwalifikowalne).

[24] Urządzenia typu UTM.

[25] Urządzenie typu switch 1.

[26] Urządzenia typu switch 2.

[27] Urządzenia typu access point.

[28] Z tego 531 694,18 zł z dofinansowania *Projektu*, 59 076,85 zł ze środków własnych (wydatki kwalifikowalne) oraz 48 558,37 zł (wydatki niekwalifikowalne).

[29] Z tego 47 047,52 zł z dofinansowania *Projektu* oraz 5 227,48 zł wkładu własnego (wydatki kwalifikowalne).

[30] Bez dodatkowych licencji i serwisów. Z tego:
   - 209 999,13 zł w Zadaniu 1 (poz. 1, 3, 5 i 7 w fakturze nr BB-FV-18-8-2024 z dnia 16 sierpnia 2024 r.);
   - 587 819,04 zł w Zadaniu 2 (poz. 1, 2, 3, 5 i 7 w fakturze nr BB-FV-33-11.2024 z dnia 20 listopada 2024 r.) , po uwzględnieniu w cenie serwerów również systemu operacyjnego.

[31] Zadanie 1 – Umowa WIF-RZPO.273.00388.2024 z dnia 6 sierpnia 2024 r.; Termin dostarczenia sprzętu – do 30 dni od zawarcia umowy; Protokół odbioru z dnia 8 sierpnia 2024 r.
Zadanie 2 – Umowa WIF.RZPO.273.520.2024 z dnia 8 października 2024 r.; Termin dostarczenia sprzętu – do 45 dni od zawarcia umowy; Protokół odbioru z dnia 19 listopada 2024 r.;
Zadanie 3 – Umowa WIF-RZPO.273.00494.2024 z dnia 16 września 2024 r.; Termin wykonania przedmiotu umowy – do 30 dni od zawarcia umowy; Protokół odbioru z dnia 30 września 2024 r.

[32] Urządzenia typu access point.

środowiska i bezpieczeństwa sieci bezprzewodowej. Miały one pracować w jednym systemie zarządzania uprawieniami i dostępem, co odpowiadało założonemu celowi projektu, czyli zwiększeniu poziomu bezpieczeństwa cyfrowego w *Starostwie*. Jak dodał *Starosta*, zmiany te mają zostać wykazane w rozliczeniu końcowym, zgodnie z §15 *Umowy o powierzenie grantu* oraz informacją w tym zakresie przekazaną *Starostwu* przez Grantodawcę.

(akta kontroli str. 1020-1030, 1039-1044, 1049-1051, 1173-1187, 1236-1241, 1255-1264, 1291-1315, 1336-1342, 1369-1382, 1406-1411, 1423-1427, 1553-1554, 1561-1562, 1571-1573, 1607, 1614)

Wydatki w kwocie 944 000,00 zł przewidziane we *Wniosku* stanowiły wydatki kwalifikowalne. Jednocześnie w ramach Zadania 2 przewidziano wydatki niekwalifikowalne w kwocie 48 558,37 zł[33], związane z wydłużoną gwarancją na serwery oraz macierz. Jak wyjaśnił *Starosta Gliwicki*: *W ramach umowy nr WIF.RZPO.273.520.2024 z 8 października 2024 r. zostały zakupione sprzęty z gwarancją i licencje bezterminowe na oprogramowanie. Kosztami niekwalifikowanymi była gwarancja na sprzęt wykraczająca poza standardowy 24-miesięczny okres (w tym przypadku dodatkową gwarancję zakupiono na okres 36 miesięcy). Przy szacowaniu wartości zamówienia okazało się, że bardziej uzasadnioną ekonomicznie opcją jest zakup 60-miesięcznej gwarancji niż rozdzielanie na części - czyli 24 miesiące w ramach grantu, a później dokupienie kolejnych 36 miesięcy.* Dodał, iż wydatki niekwalifikowalne w ramach *Projektu* zostały pokryte ze środków własnych Powiatu Gliwickiego.

(akta kontroli str. 1020-1029, 1156-1161, 1173-1187, 1236-1241, 1554, 1563, 1607, 1614)

5. Udział jednostek organizacyjnych *Starostwa* w realizacji grantu.

Opis stanu faktycznego

Zgodnie z założeniami *Projektu*, zakupiona infrastruktura służyć miała *Starostwu Powiatowemu* oraz dwóm jego jednostkom organizacyjnym – *PCPR* oraz *ZDP*. Zakupiony sprzęt i oprogramowanie stanowiły własność *Starostwa*, natomiast na rzecz pozostałych dwóch jednostek organizacyjnych świadczone miały być przez *Starostwo* jedynie usługi związane z zachowaniem cyberbezpieczeństwa. Założenia takie wpisano do *Wniosku* w ramach Zadania 2 – *Zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych*, jak również w Zadaniu 3 – *Zakup, wdrożenie i utrzymanie systemów teleinformatycznych*.

Starosta podał, iż obecnie trwa proces przenoszenia danych /usług/zasobów *Starostwa* z fizycznych ponad 12-letnich sprzętów z systemami operacyjnymi Microsoft Windows Server 2008 na nowe, wirtualne środowisko oprogramowania Hyper-V, oparte na Microsoft Windows Server 2022. Trwa również monitoring nowego środowiska pod kątem wydajności i kompatybilności. Przeniesienie zasobów dwóch jednostek organizacyjnych (PCPR i ZDP) znajduje się w fazie uzgodnień. Zweryfikowano możliwości bezpiecznego połączenia *Starostwa* z ww. jednostkami. Konieczne jest podjęcie decyzji, jakie usługi sieciowe jednostki chcą przenieść na zasoby sprzętowe *Starostwa*. Proces ten zakończy się podpisaniem umów o współpracy (powierzania i przechowywania danych) pomiędzy *Starostwem* a każdą z dwóch wymienionych wyżej jednostek.

Starosta Gliwicki ocenił, że dopiero po przeniesieniu zasobów *Starostwa* na nowe wirtualne środowisko, po jego skonfigurowaniu i uruchomieniu ważniejszych usług jednostek możliwe będzie stwierdzenie, iż założenia

[33] Pozycja 4 i 6 w fakturze nr BB-FV-33-11-2024 z dnia 20 listopada 2024 r.

Projektu zostały w tym zakresie osiągnięte. Zakupiona w ramach ww. zadania 3 licencja na oprogramowanie antywirusowe została udostępniona ww. jednostkom organizacyjnym oraz 10 innym wraz ze szczegółami dotyczącymi licencji.

W ramach *Projektu* nie założono monitoringu działań prowadzonych przez jednostki organizacyjne, poza przeprowadzeniem *Ankiety Dojrzałości Cyberbepieczeństwa na wejściu* (jej przeprowadzenie było zobowiązaniem warunkującym wypłatę zaliczki) i *na wyjściu* (niezbędne do rozliczenia grantu).

W sprawie braku monitoringu *Starosta* wyjaśnił: *Mając na uwadze fakt, iż odpowiedzialność za realizację zadania polegającego na udostepnieniu zasobów serwerowych zlokalizowanych w Starostwie leży po stronie Starostwa, nie zaplanowano monitoringu działań prowadzonych przez jednostki organizacyjne. Rola jednostek organizacyjnych w projekcie polega jedynie na wykorzystaniu zasobów udostępnianych przez Starostwo.*

(akta kontroli str. 9, 13-15, 696-698, 703-740, 1020-1023)

6. Pracownicy odpowiedzialni za realizację prac dotyczących *Projektu*.

Opis stanu faktycznego

Pracownicy *Starostwa Powiatowego* odpowiedzialni za realizację *Projektu* zostali wskazani w Uchwale Nr 1664/2023 Zarządu Powiatu Gliwickiego z dnia 11 października 2023 r. *w sprawie: przystąpienia do projektu Cyberbezpieczny Powiat Gliwicki w ramach Konkursu Grantowego Cyberbezpieczny Samorząd, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC).* Do założenia konta grantobiorcy w systemie LSI[34] dla FERC[35] i złożenia *Wniosku* upoważniono Zastępcę Naczelnika Wydziału Inwestycji, Funduszy i Zamówień Publicznych. Natomiast wykonanie ww. uchwały powierzono Naczelnikowi Wydziału Inwestycji, Funduszy i Zamówień Publicznych w zakresie złożenia *Wniosku* oraz Kierownikowi Biura Informatyki w zakresie przygotowania merytorycznego *Projektu.* Pracownicy realizujący *Projekt* posiadali niezbędne kompetencje.

(akta kontroli str. 9, 16, 871-935, 949-950)

7. Wpływ fluktuacji kadr na sprawną realizację *Projektu*.

Opis stanu faktycznego

Odnosząc się do pytania o wpływ fluktuacji kadr na sprawną realizację *Projektu Starosta* podał: *W ramach komórek organizacyjnych zaangażowanych w realizację projektu, tj. Referatu Inwestycji i Funduszy oraz Biura Informatyki nie nastąpiły do tej pory żadne ruchy kadrowe mające wpływ na realizację projektu. Wszystkie osoby uczestniczące w procesie przygotowania i wdrażania projektu są ciągle pracownikami tych komórek.*

(akta kontroli str. 9, 16, 871-935, 949-950, 1554, 1565)

8. Realizacja ustalonych wskaźników produktu i rezultatu.

Opis stanu faktycznego

Zgodnie z §4 ust. 10 *Regulaminu Konkursu*, *Starostwo* w ramach realizacji *Projektu* było zobowiązane do realizacji wskaźników określonych w zał. nr 9 do ww. Regulaminu. Jak wskazano w ww. załączniku: Opis wskaźników *Projektu* Cyberbezpieczny Samorząd, cele *Projektu* należało wyrazić adekwatnymi, mierzalnymi wskaźnikami:

- produktu (powiązanymi bezpośrednio z wydatkami ponoszonymi w *Projekcie*, zrealizowanymi w okresie od rozpoczęcia do ukończenia

[34] Lokalny System Informatyczny wykorzystywany przez CPCC, *NASK* i jst przede wszystkim w zakresie wnioskowania o środki na dofinansowanie grantów (projektów), przeprowadzania procedur oceniających, ale także sprawozdawczości i raportowania.

[35] Program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

Projektu. Osiągnięte wartości muszą zostać wykazane najpóźniej we wniosku rozliczającym o którym mowa w par. 3. ust. 2. pkt 2. *Umowy o powierzenie grantu*);

- rezultatu (odnoszącymi się do bezpośrednich efektów realizowanego *Projektu*, osiągniętymi w wyniku realizacji *Projektu*) zdefiniowanymi we *Wniosku.*

Jak podał *Starosta*: *We wniosku o dofinansowanie grantu nie znalazło się* (...) *specjalne miejsce na wylistowanie tych wskaźników. Można to było uczynić jedynie w części opisowej. We wniosku Powiatu Gliwickiego znalazł się jedynie zapis:*
„W efekcie realizacji projektu zwiększy się poziom cyberbezpieczeństwa trzech jednostek organizacyjnych Powiatu Gliwickiego poprzez:

1. modernizację bazy sprzętowej (zakup switchy zarządzanych i urządzeń UTM nowej generacji, co zwiększy bezpieczeństwo ruchu sieciowego)

2. budowę infrastruktury pozwalającej na zarządzanie danymi i zapewnienie bezpieczeństwa cyfrowego w trzech jednostkach organizacyjnych Powiatu Gliwickiego (wdrożenie klastra serwerów, macierzy dyskowej z licencjami systemów operacyjnych i silnikiem środowiska do wirtualizacji zasobów wraz przeszkoleniem personelu)

3. zwiększenie bezpieczeństwa antywirusowego (zakup programu antywirusowego).”(...).

Dodał, iż rozliczanie wskaźników zgodnie z listą podaną w załączniku nr 9 do *Regulaminu Konkursu* miało następować w ramach wniosków sprawozdawczych oraz rozliczających zaliczkę.
We wniosku sprawozdawczym złożonym przez *Starostwo* w dniu 28 maja 2025 r. na podstawie §7 ust. 2 *Umowy*[36] zamieszczono m.in. tabelę ze wskaźnikami rezultatu. Wykazany stan realizacji wskaźników przedstawiał się następująco:

- Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (Mężczyźni); Jednostka miary: Szt.; Wartość bazowa: 0,00; Rok bazowy: 2023; Wartość osiągnięta: 4,00;
- Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji: Jednostka miary: Szt.; Wartość bazowa 1,00; Rok bazowy: 2023; Wartość osiągnięta: 1,00;
- Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych: Jednostka miary: Szt.; Wartość bazowa 0,00; Rok bazowy: 2023; Wartość osiągnięta: 500,00;
- Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST: Jednostka miary: Szt.; Wartość bazowa 0,00; Rok bazowy: 2023; Wartość osiągnięta: 12,00.

(akta kontroli str. 954, 967, 971, 976-987, 1020-1028, 1169-1172, 1199, 1204-1205, 1255-1262, 1291-1315, 1336-1342, 1369-1382, 1406-1411, 1423-1427)

9. Wykorzystanie urządzeń/oprogramowania zakupionego w ramach grantu.

Opis stanu faktycznego

[36] *Grantobiorca zobowiązuje się do przekazania za pomocą systemu służącego do rozliczania wniosków, dostępnego na stronie internetowej konkursu pn. „Cyberbezpieczny Samorząd” informacji o postępie rzeczowym realizacji Projektu w formie wskazanej przez Operatora w terminie 30 dni następujących po upływie 12 miesięcy od podpisania Umowy.*

Oględziny przeprowadzone w siedzibie *Starostwa Powiatowego* wykazały, iż zakupione urządzenia i oprogramowanie zostały zainstalowane w obiekcie i były wykorzystywane przez *Starostwo.*

(akta kontroli str. 1255-1262, 1291-1315, 1336-1342, 1369-1382, 1406-1411, 1423-1427, 1489-1516)

10. Utrzymanie poziomu cyberbezpieczeństwa po zakończeniu realizacji grantu.

Opis stanu faktycznego

Zgodnie z §13 ust. 1 *Umowy o powierzenie grantu, Starostwo Powiatowe* było zobowiązane do utrzymania efektów *Projektu*, w tym do opracowania oraz wdrożenia procedury monitorowania utrzymania efektów *Projektu* tj. utrzymania środków trwałych i usług nabytych w ramach *Projektu* przez okres min. dwóch lat od zakończenia *Projektu* oraz utrzymania trwałości *Projektu*. Jak wyjaśnił *Starosta*: *Trwałość projektu rozumiana jako utrzymanie i wykorzystanie powstałej w jego ramach infrastruktury będzie zapewniona poprzez działania bieżące, realizowane ze środków własnych przez Biuro Informatyki. Środki finansowe na ten cel są co roku zapewniane w ramach budżetu Powiatu Gliwickiego.*

Dla zadania 2 – „Zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa (SOC), także jako element Centrum Usług Wspólnych" już na etapie postępowania na wyłonienie wykonawcy zaplanowano działania mające na celu zapewnienie trwałości projektu, wymagając co najmniej 3-letniej gwarancji na urządzenia. Dodatkowy 2-letni okres gwarancji stanowił kryterium oceny ofert. Wszyscy wykonawcy zaoferowali 5-letni okres gwarancji. Ze wstępnego rozeznania rynku wynikało bowiem, że wydłużenie gwarancji jest znacznie bardziej efektywne ekonomicznie niż późniejsze wydłużenie jej.

Dzięki realizacji zadania 1 – „Zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa" i zadania 3 – „Zakup, wdrożenie i utrzymanie systemów teleinformatycznych" podniesiono poziom bezpieczeństwa (funkcjonalności) już wcześniej używanych przez nas rozwiązań. Odnawianie licencji będzie realizowane ze środków własnych w kolejnych latach.

(akta kontroli str. 1044, 1068, 1553, 1559)

11. Opracowanie, ustanowienie i wdrożenie w *Starostwie* Systemu Zarządzania Bezpieczeństwem Informacji.

Opis stanu faktycznego

Starostwo posiadało w badanym okresie opracowaną i zatwierdzoną politykę bezpieczeństwa informacji oraz instrukcję zarządzania systemem informatycznym, wprowadzone kolejno następującymi aktami[37]:

- Zarządzeniem Nr 32/2018 Starosty Gliwickiego z dnia 24 maja 2018 r. *w sprawie polityki bezpieczeństwa informacji oraz instrukcji[38] zarządzania systemem informatycznym*[39];
- Zarządzeniem Nr 64/2023 Starosty Gliwickiego z dnia 28 lipca 2023 r. o tym samym tytule[40].

---

[37] Dalej: *PBI.*

[38] Instrukcja zawierała następujące procedury: monitorowania systemów teleinformatycznych, zarządzania bezpieczeństwem sieci, dostępu do sieci teleinformatycznej oraz zapewnienia bezpieczeństwa okablowania sieciowego, wykonywania oraz przechowywania kopii bezpieczeństwa, wykonywania czynności serwisowych oraz likwidacji nośników danych.

[39] Zmienionym Zarządzeniem Nr 18/2020 Starosty Gliwickiego z dnia 9 kwietnia 2020 r. *w sprawie zmiany Zarządzenia Nr 32/2018 Starosty Gliwickiego z dnia 24 maja 2018 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemem informatycznym.*

[40] Instrukcja Zarządzania Systemem Informatycznym, stanowiąca załącznik do Zarządzenia zawierała następujące procedury: monitorowania systemów teleinformatycznych, zarządzania

Pracownicy *Starostwa* zapoznali się z pierwszym z dokumentów, potwierdzając to stosownym oświadczeniem, którego wzór stanowił załącznik do zarządzenia. Po przyjęciu drugiego z zarządzeń, zostało ono rozesłane do wszystkich pracowników za pomocą elektronicznego systemu zarządzania dokumentacją FINN, wykorzystywanego w *Starostwie*.

Za aktualizację i weryfikację treści *PBI*, zgodnie z zapisami §8 ust. 1 obu *PBI* odpowiedzialny był Inspektor Ochrony Danych[41] zatrudniony w *Starostwie Powiatowym* przy udziale Administratorów Informacji, czyli kierowników komórek organizacyjnych *Starostwa*.

(akta kontroli str. 9-10, 17-47, 272-349, 671-695, 1199, 1202-1206, 1215)

12. Aktualizacja regulacji wewnętrznych stanowiących System Zarządzania Bezpieczeństwem Informacji.

Opis stanu faktycznego

Zgodnie z §8 *PBI z 2018 r. i PBI z 2023 r. – Zasady aktualizacji dokumentu Polityka Bezpieczeństwa Informacji*, podlegał on aktualizacji i weryfikacji treści. Aktualizację i weryfikację treści miał przeprowadzać *IOD* przy udziale Administratorów Informacji, czyli kierowników komórek organizacyjnych *Starostwa*. Aktualizacja miała się odbywać w przypadku wystąpienia któregokolwiek z poniższych warunków:

- Zgłoszenia przez pracowników *Starostwa* do *IOD* ważnych problemów i trudności w przestrzeganiu zasad zawartych w dokumencie aktualnie obowiązującej *PBI*;
- Wykrycia przez *IOD* nieprawidłowości w aktualnie obowiązującym dokumencie *PBI*;
- Wystąpienia zmian w obowiązujących ustawach i rozporządzeniach związanych z *PBI*;
- Wystąpienia innych sytuacji mogących powodować niezgodność dokumentu *PBI* z rzeczywistymi działaniami *Starostwa* lub/i ogólnymi przepisami prawa;

Aktualizacji projektu dokumentu *PBI* do nowej wersji miał dokonywać *IOD*, oznaczając ją odpowiednią datą modyfikacji i numerem Zarządzenia *Starosty Gliwickiego.* Ponadto tryb postępowania w zakresie aktualizacji wszystkich zarządzeń *Starosty* opisany został w §10 Zarządzenia nr 74/2018 Starosty Gliwickiego z dnia 21 listopada 2018 r. *w sprawie trybu tworzenia i postępowania z zarządzeniami Starosty Gliwickiego*, zgodnie z którym raz w roku, na wniosek Wydziału Organizacyjnego, Kadr i Szkoleń, w terminie do 30 listopada, kierownicy komórek organizacyjnych mieli dokonywać analizy zarządzeń z zakresu działania kierowanej przez nich komórki organizacyjnej i informować o konieczności lub braku konieczności ich aktualizacji. Po przeprowadzeniu analizy aktualizacji zarządzeń, Wydział Organizacyjny, Kadr i Szkoleń miał przedstawić Sekretarzowi Powiatu Gliwickiego sprawozdanie w terminie do 15 grudnia.

W latach 2023-2024 dokonywano corocznych przeglądów zarządzenia *Starosty Gliwickiego* dotyczących polityki bezpieczeństwa informacji oraz zarządzania systemem informatycznym w *Starostwie.* W ich wyniku stwierdzono, że dokument nie wymaga aktualizacji. Przegląd w roku 2025 jest planowany do przeprowadzenia w terminie do 30 listopada 2025 r.

(akta kontroli str.9-10, 17-18, 272-349, 1199, 1206, 1210-1215, 1555, 1564-1565, 1574-1605)

---

bezpieczeństwem sieci, dostępu do sieci teleinformatycznej oraz zapewnienia bezpieczeństwa okablowania sieciowego, wykonywania oraz przechowywania kopii bezpieczeństwa, wykonywania czynności serwisowych oraz likwidacji nośników danych.

[41] Dalej: *IOD.*

13. Przeprowadzanie w *Starostwie* okresowego audytu z zakresu bezpieczeństwa informacji.

Opis stanu faktycznego

Zgodnie z zapisami Rozporządzeń Rady Ministrów z dnia 12 kwietnia 2012 r.[42] i 21 maja 2024 r.[43] *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[44], zarządzanie bezpieczeństwem informacji w podmiotach realizujących zadania publiczne miało polegać m.in. na zapewnieniu okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. W badanym okresie audyt taki został przeprowadzony dwukrotnie[45].

W jednym przypadku zalecenie poaudytowe ma zostać zrealizowane w bieżącym roku, ze względu na wcześniejsze przesunięcie środków na inny cel. W trzech przypadkach, po dokonaniu wewnętrznych analiz i konsultacji stwierdzono, że nie ma potrzeby wprowadzania rekomendowanych zmian. Pozostałe wnioski sformułowane w wyniku przeprowadzonych audytów zostały zrealizowane.

Ww. zadania audytowe zostały przeprowadzone przez osoby posiadające odpowiednie kompetencje w tym zakresie.

(akta kontroli str. 10, 18, 48-66, 626-670, 1198, 1202, 1223-1235)

14. Obowiązki informacyjne w związku z dofinansowaniem na realizację *Projektu*.

Opis stanu faktycznego

Jak wskazano w §11 ust. 4 *Umowy*, *Starostwo Powiatowe* było zobowiązane w szczególności do:

a) oznaczania znakiem Unii Europejskiej, barwy Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich:
   - wszystkich prowadzonych działań informacyjnych i promocyjnych dotyczących *Projektu*;
   - wszystkich dokumentów związanych z realizacją *Projektu*, podawanych do wiadomości publicznej;
   - wszystkich dokumentów i materiałów dla osób i podmiotów uczestniczących w *Projekcie*, w tym zaświadczeń o uczestnictwie lub innych certyfikatów, zawierających stwierdzenie, że *Projekt*

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

[43] Dz. U. poz. 773.

[44] Odpowiednio §20 ust. 2 pkt 14 oraz §19 ust. 2 pkt 14.

[45] **Pierwszy z audytów**: Data rozpoczęcia zadania: 20 września 2023 r.; Data sporządzenia sprawozdania z audytu: 24 listopada 2023 r.; Temat zadania: *Bezpieczeństwo informacji w Starostwie Powiatowym w Gliwicach.* Zakres przedmiotowy zadania: 1. Formalnie ustanowione zasady systemu kontroli zarządczej obejmujące zapewnienie bezpieczeństwa informacyjnego; 2. Wdrożenie, utrzymanie i doskonalenie systemu bezpieczeństwa informacji, w tym struktury zarządzania oraz ochrony danych osobowych; 3. Polityki i instrukcje, analizy ryzyka utraty poufności, dostępności i integralności danych, sprawdzenia zgodności przetwarzania danych z przepisami, standardami, normami i wymogami technicznymi oraz nadzór nad opracowywaniem i aktualizowaniem tej dokumentacji.
Drugi z audytów: Data rozpoczęcia zadania: 12 grudnia 2024 r.; Data sporządzenia sprawozdania z audytu: 5 maja 2025 r.; Temat zadania: *Bezpieczeństwo informacji w Starostwie Powiatowym w Gliwicach.* Zakres przedmiotowy zadania: 1. Formalnie ustanowione zasady systemu kontroli zarządczej obejmujące zapewnienie bezpieczeństwa informacyjnego; 2. Wdrożenie, utrzymanie i doskonalenie systemu bezpieczeństwa informacji, w tym struktury zarządzania oraz ochrony danych osobowych; 3. Polityki i instrukcje, analizy ryzyka utraty poufności, dostępności i integralności danych, sprawdzenia zgodności przetwarzania danych z przepisami, standardami, normami i wymogami technicznymi oraz nadzór nad opracowywaniem i aktualizowaniem tej dokumentacji; 4. Urządzenia i inny sprzęt, ich rodzaj oraz konfiguracje, środki przetwarzania informacji, w tym ochrony fizycznej, środowiskowej i logicznej.

jest wspierany przez program operacyjny i finansowany przez Unię Europejską z danego funduszu;

b) umieszczenia przynajmniej jednego plakatu o minimalnym formacie A3;
c) umieszczania opisu *Projektu* na swojej stronie internetowej i w mediach społecznościowych;
d) przekazywania opinii publicznej i podmiotom uczestniczącym w *Projekcie* informacji, że *Projekt* uzyskał unijne dofinansowanie przynajmniej w formie odpowiedniego oznakowania;
e) dokumentowania działań informacyjnych i promocyjnych prowadzonych w ramach *Projektu*.

Na tablicy ogłoszeń zawierającej informacje o projektach realizowanych przez Powiat Gliwicki umieszczono dwa plakaty, w tym jeden w formacie A3, informujące o uzyskanym dofinansowaniu w ramach *Projektu*. Opis *Projektu* zamieszczono również na stronie internetowej *Starostwa* oraz na profilu w portalu społecznościowym Facebook. Dokumenty udostępniane publicznie były oznaczone zgodnie z wymogami określonymi w umowie. Odnośnie dokumentowania działań informacyjnych i promocyjnych prowadzonych w ramach *Projektu*, *Starosta* wyjaśnił: *projekt ma charakter „backoffice", jedyne działania informacyjno-promocyjne to działania związane z umieszczeniem informacji na stronie Powiatu Gliwickiego oraz na FB.*

Wszystkie prowadzone działania informacyjne i promocyjne dotyczące *Projektu* (informacja na stronie internetowej *Starostwa* oraz na jego profilu Facebook), dokumenty związane z realizacją *Projektu* podawane do wiadomości publicznej (np. dokumentacja z postępowań zmierzających do wyboru wykonawców dofinansowanych zadań – Specyfikacja Warunków Zamówienia, wzory umów), a także dokumenty i materiały dla osób i podmiotów uczestniczących w *Projekcie* (np. umowy z wykonawcami, protokoły odbioru) były oznaczone znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich.

(akta kontroli str. 1044, 1066-1067, 1199-1200, 1207-1209, 1216-1222, 1255, 1263, 1269, 1297, 1322, 1336, 1354, 1373, 1392, 1406, 1415, 1426, 1446, https://starostwo.gliwice.pl/cyberbezpieczny-powiat-gliwicki, https://www.bip.powiatgliwicki.finn.pl/bipkod/36017264, https://www.bip.powiatgliwicki.finn.pl/bipkod/36010818, https://www.bip.powiatgliwicki.finn.pl/bipkod/35693375)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

IV. Uwagi i wnioski

W związku z niestwierdzeniem nieprawidłowości Najwyższa Izba Kontroli nie formułuje uwag i wniosków.

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 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, 8 sierpnia 2025 r.

Kontroler

Michał Nowak

Starszy inspektor k. p.

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Delegatura w Katowicach

Dyrektor

z up. Jacek Kościelniak

p.o. Wicedyrektor

/podpisano elektronicznie/