NAJWYŻSZA IZBA KONTROLI

KSF.430.3.2026
Nr ewid. 98/2025/P/25/003/KAP

Informacja o wynikach kontroli

# REALIZACJA PROJEKTU CYBERBEZPIECZNY SAMORZĄD

**MISJĄ**

Najwyższej Izby Kontroli jest niezależna, profesjonalna kontrola zadań publicznych w interesie obywateli i państwa

p.o. Dyrektor Departamentu
Spójności i Infrastruktury

Jolanta Stawska
*/podpisano elektronicznie/*

Wiceprezes Najwyższej Izby Kontroli

Jacek Kozłowski
*/podpisano elektronicznie/*

Prezes Najwyższej Izby Kontroli

Mariusz Haładyj
*/podpisano elektronicznie/*

Warszawa, maj 2026

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
+48 22 444 50 00
nik@nik.gov.pl
*www.nik.gov.pl*

# SPIS TREŚCI

# WYKAZ SKRÓTÓW, SKRÓTOWCÓW I POJĘĆ

| | |
|---|---|
| **administrator systemów informatycznych (ASI)** | odpowiada za zarządzanie systemami informatycznymi, w tym systemami wykorzystywanymi w procesie przetwarzania danych osobowych. W zakresie przetwarzania danych osobowych współpracuje z Inspektorem ochrony danych; |
| **aktywa informacyjne** | zidentyfikowane zbiory danych urzędu; |
| **aktywa informatyczne** | oprogramowanie, dane, sprzęt, dokumentacja, zasoby administracyjne fizyczne, komunikacyjne lub ludzkie związane z działalnością informatyczną; |
| **Ankieta dojrzałości** | „Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego[1]", wypełniania w związku z przystąpieniem do projektu „Cyberbezpieczny Samorząd"; |
| **beneficjent** | beneficjent projektu „Cyberbezpieczny Samorząd" – Centrum Projektów Polska Cyfrowa; |
| **CPPC** | Centrum Projektów Polska Cyfrowa; |
| **cyberbezpieczeństwo** | dziedzina wiedzy zajmująca się zapewnieniem odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność posiadanych i przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy; |
| **DoD** | Decyzja o dofinansowaniu projektu „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027; |
| **EFRR** | Europejski Fundusz Rozwoju Regionalnego; |
| **FERC** | Program Fundusze Europejskie na Rozwój Cyfrowy 2021–2027; |
| **grant** | środki finansowe, które NASK/CPPC na podstawie umowy o powierzenie grantu powierzył grantobiorcy na realizację zadań służących osiągnięciu celu Projektu; |
| **grantobiorca** | podmiot, będący jednostką samorządu terytorialnego, uprawniony do udziału w konkursie, wybrany w procesie otwartego naboru, ogłoszonego przez CPPC, który realizuje Projekt na podstawie umowy o powierzenie grantu; |
| **Instytucja Pośrednicząca/IP** | podmiot, któremu została powierzona w drodze porozumienia albo umowy zawartej z instytucją zarządzającą realizacja zadań w ramach krajowego programu lub regionalnego programu. CPPC pełni rolę zarówno Beneficjenta, jak i Instytucji Pośredniczącej w Programie Fundusze Europejskie na Rozwój Cyfrowy 2021–2027; zadania te wykonują odrębne komórki w CPPC; |
| **jst** | jednostka samorządu terytorialnego; |
| **kwalifikowalność wydatków** | możliwość uznania kosztu za kwalifikowalny, czyli nadający się do dofinansowania. Zgodnie z DoD, wydatki kwalifikowalne to koszty i poniesione wydatki, uznane za kwalifikowalne i spełniające kryteria określone w dokumentach, o których mowa w § 4 ust. 1 pkt 1 i 2 DoD, |

[1] Wzór ankiety został określony w załączniku nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".

| | |
|---|---|
| | tj. w Wytycznych dotyczących kwalifikowalności wydatków na lata 2021–2027 oraz w Katalogu wydatków kwalifikowalnych II priorytetu programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027; |
| **LSI** | Lokalny System Informatyczny wykorzystywany przez CPPC, NASK i JST, przede wszystkim w zakresie wnioskowania o środki na dofinansowanie grantów (projektów), przeprowadzania procedur oceniających, ale także sprawozdawczości i raportowania; |
| **NASK** | Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy; |
| **Partner** | partner projektu Cyberbezpieczny Samorząd – Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy; |
| **Partner wiodący** | Partner wiodący projektu Cyberbezpieczny Samorząd – CPPC; |
| **polityka bezpieczeństwa informacji (PBI)** | zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w jednostce; |
| **Projekt** | Projekt „Cyberbezpieczny Samorząd" realizowany w ramach FERC. Łączny budżet Projektu wynosi około 1,5 mld zł; |
| **RODO** | Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[2]; |
| **rozporządzenie KRI** | obowiązujące od 23 maja 2024 r. 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[3]. Wcześniejsze rozporządzenie 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 obowiązywało do 22 maja 2024 r.[4]; |
| **systemy dziedzinowe** | wyspecjalizowane systemy informatyczne przeznaczone do obsługi określonego obszaru funkcjonowania organizacji (np. elektroniczny obieg dokumentów, system finansowo-księgowy, poczta elektroniczna); |
| **System Zarządzania Bezpieczeństwem Informacji (SZBI)** | część całościowego systemu zarządzania, oparta na podejściu wynikającym ze zidentyfikowanego ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji; |

[2] Dz. Urz. UE. L 119 z 04.05.2016, str. 1, ze zm.
[3] Dz. U. poz. 773.
[4] Dz. U. z 2017 r. poz. 2247.

| | |
|---|---|
| **UG** | Urząd Gminy; |
| **UM** | Urząd Miejski/Urząd Miasta; |
| **UMiG** | Urząd Miasta i Gminy; |
| **Umowa o partnerstwie/UoP** | umowa o partnerstwie w celu wspólnej realizacji projektu Cyberbezpieczny Samorząd w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, zawarta pomiędzy CPPC a NASK w lipcu 2023 r.; |
| **Umowa o powierzenie grantu** | umowa pomiędzy grantobiorcą i CPPC określająca w szczególności przedmiot umowy, zadania grantobiorcy objęte grantem, kwotę grantu, okres realizacji umowy o powierzenie grantu, warunki przekazania i rozliczenia grantu; |
| **ustawa o NIK** | ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[5]; |
| **ustawa wdrożeniowa** | ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027[6]; |
| **WoD** | Wniosek o Dofinansowanie; |
| **zarządzanie ryzykiem** | skoordynowane działania mające na celu kierowanie organizacją i kontrolowanie organizacji pod względem ryzyka. |

[5] Dz. U. z 2022 r. poz. 623.
[6] Dz. U. z 2022 r. poz. 1079, ze zm.

# 1. WPROWADZENIE

**Pytanie definiujące cel główny kontroli**

Czy projekt „Cyberbezpieczny Samorząd" był realizowany zgodnie z założeniami oraz skutecznie?

**Pytania definiujące cele szczegółowe kontroli**

1. Czy CPPC prawidłowo, terminowo i zgodnie z założeniami realizuje projekt „Cyberbezpieczny Samorząd"?

2. Czy NASK prowadzi skuteczne i zgodne z umową o partnerstwie działania na rzecz osiągania rezultatów określonych w projekcie „Cyberbezpieczny Samorząd"?

3. Czy gminy i powiaty w ramach projektu „Cyberbezpieczny Samorząd" podejmują skuteczne działania w celu zwiększenia poziomu bezpieczeństwa informacji w szczególności czy skutecznie osiągają założone rezultaty?

**Jednostki kontrolowane**

Kontrolą objęto 19 jednostek: 12 urzędów miast i gmin i 5 starostw powiatowych oraz CPPC i NASK.

**Okres objęty kontrolą**

Od 1 stycznia 2023 r. do dnia zakończenia kontroli[7].

Wraz ze wzrostem popularności usług cyfrowych i pojawianiem się nowych technologii rośnie także zagrożenie cyberprzestępczością. Dodatkowo sytuacja związana z wojną na Ukrainie i wojną hybrydową sprawia, że systematycznie rośnie liczba ataków hakerskich na instytucje publiczne. W takich okolicznościach szczególnie ważne jest zadbanie o cyberbezpieczeństwo podmiotów świadczących usługi publiczne i przetwarzających dane obywateli oraz zapewnienie ciągłości działania urzędów.

Celem projektu „Cyberbezpieczny Samorząd" jest zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie. Przyczynić się to powinno do ochrony danych, infrastruktury i zasobów publicznych na poziomie lokalnym i regionalnym.

Projekt „Cyberbezpieczny Samorząd" jest odpowiedzią na zidentyfikowane przez rząd potrzeby samorządów w zakresie poprawy cyberbezpieczeństwa. Skierowany został do wszystkich jednostek samorządu terytorialnego: 2477 gmin, 314 powiatów, 16 województw (łącznie do 2807 JST), które mogły otrzymać dofinansowanie w formie grantu z funduszy europejskich. W 80% środki te (łącznie 1,2 mld zł) zaplanowano na zakup infrastruktury sprzętowej, oprogramowania oraz usług wdrożeniowych. Pozostałe środki przewidziano na opracowanie procedur oraz przeprowadzenie audytów i szkoleń. Łączny budżet Projektu wynosi około 1,5 mld zł. Czas realizacji grantu to 24 miesiące od wejścia w życie umowy, nie dłużej niż do 30 czerwca 2026 r.

Projekt realizowany jest w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC), który w nowej perspektywie finansowej Funduszy Europejskich 2021–2027 stanowi kontynuację Programu Operacyjnego Polska Cyfrowa 2014–2020. Realizacja FERC ma wzmocnić kolejny etap cyfrowej transformacji kraju, m.in. ma poszerzyć dostęp do ultraszybkiego internetu szerokopasmowego, podnieść kompetencje cyfrowe pracowników instytucji sektora publicznego, zwiększyć dostęp do nowoczesnych e-usług i poprawić cyberbezpieczeństwo. Budżet FERC to około 2 mld euro. Zakładana forma wsparcia to dotacje.

[7] 5 września 2025 r.

# 2. OCENA OGÓLNA

**CPPC nie wymagało od jst oceny poziomu bezpieczeństwa informacji popartej audytem. Dopuszczono możliwość jednoczesnego funkcjonowania systemów dziedzinowych i systemów bezpieczeństwa na serwerach nabywanych przez jst w ramach Projektu**

**Realizacja projektu „Cyberbezpieczny Samorząd" przebiegała zgodnie z jego założeniami i przyjętymi procedurami, jednak nie wiadomo w jakim stopniu przyczynił się on do zwiększenia bezpieczeństwa informacji w jednostkach samorządu terytorialnego (jst). Odpowiedzialne za koordynację programu Centrum Projektów Polska Cyfrowa (CPPC) nie wymagało bowiem od jst oceny poziomu bezpieczeństwa informacji popartej audytem na etapie składania wniosków o granty i nie wprowadziło wymogu wykazania zwiększenia poziomu bezpieczeństwa informacji po wykorzystaniu grantu. Wynikało to przede wszystkim z przyjętych w Projekcie założeń. W konsekwencji akceptowany był każdy wydatek znajdujący się na liście produktów i usług związanych z cyberbezpieczeństwem, a w ramach weryfikacji wydatków nie badano czy nabywane rozwiązanie (sprzęt, oprogramowanie) pozwoliło utworzyć spójny i skuteczny system bezpieczeństwa informacji.**

W blisko połowie kontrolowanych jst nabywano zaawansowane rozwiązania z zakresu cyberbezpieczeństwa nie mając jednocześnie ustanowionych podstawowych elementów ochrony, tj. Systemu Zarządzania Bezpieczeństwem Informacji oraz nie prowadząc obowiązkowych corocznych audytów bezpieczeństwa informacji, wymaganych na podstawie § 20 ust. 2 pkt 14 rozporządzenia KRI[8]. Tym samym CPPC akceptowało w Projekcie nakłady na systemy bezpieczeństwa, które nie były prawidłowo zdefiniowane i określone. W ocenie NIK wskazuje to na brak systemowego podejścia uczestników Projektu do kwestii cyberbezpieczeństwa.

Ponadto kontrola wykazała, że także w dokumentach strategicznych większości kontrolowanych JST (94%) nie uwzględniono zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa.

Zdefiniowane przez CPPC wskaźniki realizacji projektów grantowych, tak produktu, jak i rezultatu, nie były powiązane z faktycznym wzrostem poziomu cyberbezpieczeństwa u grantobiorców (jst), a jedynie z liczbą dokonanych zakupów i przeszkolonych osób. Ponadto przyjęty w Projekcie system monitorowania wskaźników nie dostarczał informacji na temat postępu rzeczowego, ponieważ CPPC dokumentowało i sprawozdawało monitorowanie tylko jednego wskaźnika, dotyczącego liczby podmiotów wspartych w zakresie cyberbezpieczeństwa.

CPPC właściwie prowadziło nadzór nad realizacją przez NASK (Partnera) zadań określonych w Umowie o Partnerstwie. Dopuszczono jednak możliwość jednoczesnego funkcjonowania systemów dziedzinowych i systemów bezpieczeństwa na serwerach nabywanych przez jst w ramach grantów przeznaczonych na zwiększenie

[8] Obowiązującego do 22 maja 2024 r. Odpowiednio § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

bezpieczeństwa informacji, co było niezgodne z wymogami § 15 ust. 1 rozporządzenia KRI[9].

NASK, jako partner CPPC, prowadził zgodne z umową o partnerstwie działania na rzecz osiągania rezultatów określonych w projekcie „Cyberbezpieczny Samorząd", jednak stwierdzono nieprawidłowości w zakresie rozliczania grantów. Weryfikacja przez NASK 13 z 15 objętych badaniem wniosków jst o rozliczenie grantu nie była należyta, co wskazuje na potrzebę podjęcia działań w NASK w celu prawidłowego przygotowania procesu rozliczenia grantów, który będzie szczególnie nasilony w II kwartale 2026 r.

[9] Z przepisu tego wynika wymóg stosowania norm oraz uznanych standardów i metodyk. Zasada separacji systemów wynika z normy ISO 27001 i NIST SP 800-53 rev.5

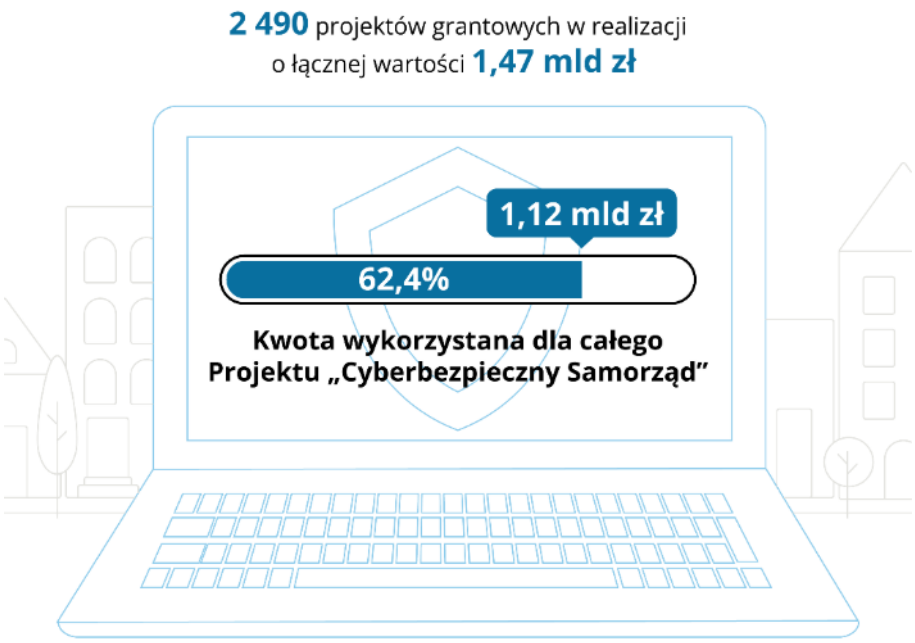
# 3. SYNTEZA

**Realizacja przez Centrum Projektów Polska Cyfrowa projektu Cyberbezpieczny Samorząd.**

**CPPC zorganizowało nabór wniosków**

W 2023 r. w ramach konkursu grantowego zorganizowano nabór wniosków, w którym jst złożyły 2614 wniosków na łączną kwotę 1,538 mld zł. Ocenie poddano 2515 wniosków (316 w 2023 r. i 2199 w 2024 r.) o łącznej wartości 1,486 mld zł. Wszystkie umowy o powierzenie grantu zawarto z JST w 2024 r. Było to 2497 umów na kwotę 1,475 mld zł. Na dzień 31 sierpnia 2025 r. realizowanych było 2490 projektów grantowych JST o łącznej wartości 1,471 mld zł. Na dzień 31 sierpnia 2025 r. grantobiorcy złożyli 26 wniosków o płatność rozliczających grant na kwotę 16 mln zł, z których do dnia zakończenia kontroli, tj. 5 września 2025 r. NASK rozliczył 17 na kwotę 10,7 mln zł. Na dzień 31 sierpnia 2025 r. kwota wykorzystana dla całego Projektu kształtuje się na poziomie 1,122 mld zł, co stanowi 62,4% całkowitej alokacji. [str. 21–23]

Infografika nr 1
„Cyberbezpieczny Samorząd" w liczbach na dzień 31 sierpnia 2025 r.




*Źródło: opracowanie własne NIK na podstawie danych z kontroli.*

**Brak mechanizmów kontrolnych w zarządzaniu ryzykiem**

W opracowanym przez CPPC Wniosku o Dofinansowanie (WoD) dla Projektu, w pkt H2 „Analiza ryzyka w projekcie", zidentyfikowano łącznie 11 ryzyk dotyczących Projektu, oszacowano prawdopodobieństwo ich wystąpienia, zdefiniowano skutek oraz wskazano mechanizmy zapobiegania. Zamiast wskazania mechanizmów kontrolnych, które pozwoliłyby na pozyskiwanie wiedzy na temat zagrożeń w obrębach poszczególnych ryzyk, CPPC zawarło w analizie ryzyka ogólne stwierdzenia, niewskazujące konkretnych działań, procedur, osób odpowiedzialnych ani narzędzi monitorowania. CPPC, w trakcie kontroli NIK, podjęło próbę wypracowania mechanizmów kontrolnych i procedur reagowania. [str. 24–26]

**Poniesienie przez CPPC wydatków przed planowanym terminem rozpoczęcia jednego z zadań**

W ramach zadania nr 5 „Ewaluacja, rozliczenie projektu", którego realizację zaplanowano na okres od 1 listopada 2025 r. do 31 grudnia 2027 r., poniesiono wydatki niezgodnie z WoD, tj. przed terminem rozpoczęcia zadania. Na dzień 31 maja 2025 r. wydatki w tym zadaniu (w pozycji 5.2 Personel projektu – Wynagrodzenia pracowników) wyniosły 828,3 tys. zł, co stanowiło 50% alokacji dla tego zadania. Realizację ww. zadania zaplanowano na okres od 1 listopada 2025 r. do 31 grudnia 2027 r. [str. 27]

**W Projekcie nie przewidziano oceny poziomu cyberbezpieczeństwa**

W dokumentacji konkursu grantowego CPPC nie przewidziało oceny poziomu cyberbezpieczeństwa u grantobiorców na etapie składania przez nich wniosków o grant ani nie przyjęto zasady, aby powiązać osiągnięty poziom cyberbezpieczeństwa po zakończeniu prac w ramach grantu z kwalifikowalnością wydatków, co było nierzetelne. Należy podkreślić, że celem Projektu grantowego jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych jst. Zdaniem NIK, brak oceny poziomu cyberbezpieczeństwa na etapie składania wniosków przez jst o przyznanie grantu może przyczynić się do nieefektywnego wykorzystywania środków w Projekcie, ponieważ CPPC jako Beneficjent nie może ocenić tego w jakim stopniu przyznany grant podniósł poziom bezpieczeństwa jst. [str. 27–28]

**Dopuszczenie przez CPPC możliwości jednoczesnego funkcjonowania na serwerach systemów dziedzinowych i systemów bezpieczeństwa**

W Projekcie, w ramach projektów grantowych, dopuszczono możliwość jednoczesnego funkcjonowania na serwerach zarówno systemów dziedzinowych, jak i systemów bezpieczeństwa, co należy uznać za niezgodne z § 15 ust. 1 rozporządzenia KRI. Współistnienie tych systemów zwiększa ryzyko, ponieważ aplikacja dziedzinowa – nawet jeśli nie jest dostępna z Internetu – może stanowić wektor ataku w sieci wewnętrznej. Dodatkowo prowadzi to do potencjalnego konfliktu o zasoby serwera, co obniża stabilność i niezawodność systemów bezpieczeństwa. NIK zauważa, że celem grantu jest zwiększenie poziomu bezpieczeństwa, a zatem serwer powinien być wykorzystywany do uruchamiania systemów bezpieczeństwa wdrożonych w ramach projektu grantowego, a wszelkie inne aplikacje powinny działać na odrębnej infrastrukturze. [str. 29–30]

**Wydłużone okresy zawierania umów przez CPPC z jst**

W wyniku badania 30 umów zawartych przez CPPC z grantobiorcami ustalono, że okres liczony od dnia zakończenia oceny ich wniosków o przyznanie grantu do dnia podpisania umowy wynosił od 3 do 8 miesięcy, czyli średnio około pół roku. Okres zawierania tych umów (liczony od dnia otrzymania od grantobiorców kompletnych i poprawnych dokumentów niezbędnych do podpisania umowy, o których mowa w § 6 ust. 4 Regulaminu konkursu grantowego „Cyberbezpieczny Samorząd", do dnia podpisania umowy przez CPPC) wynosił od 14 do 182 dni, czyli średnio około 3 miesięcy. Spowodowało to skrócenie okresu na realizację umów przez grantobiorców, gdyż zakończenie realizacji umów musi nastąpić do 30 czerwca 2026 r. [str. 30]

**CPPC właściwie nadzorowało realizację zadań przez NASK**

W ramach nadzoru nad realizacją przez Partnera (NASK) zadań określonych w Umowie o Partnerstwie, CPPC podejmowało działania polegające m.in. na udziale w cotygodniowych spotkaniach statusowych z Partnerem, na których omawiane były bieżące tematy związane z realizacją Projektu, postęp prac, występujące trudności i możliwe ryzyka.

Ponadto, analizowano cotygodniowe raporty z realizacji prac, przesyłane przez NASK, weryfikowano przekazywane przez NASK dokumenty niezbędne do zawarcia umów o powierzenie grantu oraz weryfikowano wnioski o płatność składane przez NASK. [str. 30–31]

**Niezgłoszenie braku możliwości osiągnięcia wskaźnika produktu**

CPPC działając jako Beneficjent we WoD przewidziało dla Projektu 11 wskaźników produktu i cztery wskaźniki rezultatu. Do dnia zakończenia czynności kontrolnych, CPPC działając jako Beneficjent nie zgłosiło CPPC działającemu jako Instytucja Pośrednicząca faktu braku możliwości osiągnięcia jednego wskaźnika produktu – *Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji* i jednego wskaźnika rezultatu – *Liczba jst wspartych w zakresie cyberbezpieczeństwa*, określonych przez CPPC we WoD. Zważywszy na to, że nabór wniosków grantowych zakończył się 14 grudnia 2023 r., mając na względzie postanowienia § 22 ust. 2 pkt 2 DoD, w myśl których IP może uchylić decyzję o dofinansowaniu w przypadku, gdy Beneficjent nie zrealizował wskaźników produktu i rezultatu określonych we wniosku o dofinansowanie, niezgłoszenie do dnia zakończenia czynności kontrolnych faktu nieosiągnięcia ww. wskaźników należy uznać za nierzetelne. Jest to o tyle istotne, że z postanowień § 19 ust. 4 Decyzji o dofinansowaniu projektu „Cyberbezpieczny Samorząd" wynika, iż zmiany w obrębie wskaźników zdefiniowanych we WoD wymagają akceptacji Instytucji Pośredniczącej i są wprowadzane aneksem do decyzji. [str. 32]

**CPPC nie sprawozdawało na bieżąco wartości wskaźników**

CPPC działające jako Beneficjent do 1 lipca 2025 r. nie sprawozdawało na bieżąco we wnioskach o płatność wartości wskaźników, co naruszało postanowienia § 4 ust. 4 pkt 11 UoP oraz pkt 7 i 8 sekcji 2.1.3 „Wytycznych dotyczących monitorowania postępu rzeczowego realizacji programów na lata 2021–2027" Ministra Funduszy i Polityki Regionalnej. Powyższe postanowienia nakładają na Beneficjentów obowiązek bieżącego monitorowania postępu rzeczowego, czemu służą m.in. wartości wskaźników sprawozdawane we wnioskach o płatność. [str. 33]

**NASK zapewnił odpowiednią liczbę pracowników**

Od rozpoczęcia Projektu do 31 lipca 2025 r. w jego realizację było zaangażowanych łącznie 121 pracowników oraz 21 ekspertów ds. oceny formalnej oraz ds. oceny merytorycznej. [str. 34]

**Powoływanie przez NASK kluczowych pracowników w Projekcie**

Dyrektor NASK decyzją z 10 lipca 2023 r. powołał w NASK Komitet Sterujący Projektu[10] i Zespół projektowy realizujący Projekt[11] oraz m.in. określił ich skład i zadania. Dyrektor NASK z 3 lutego 2025 r. powołał na stanowisko Kierownika Projektu osobę, która faktycznie pełniła tę funkcję już od 17 lipca 2023 r., tj. została formalnie powołana dopiero po ponad 18 miesiącach od rozpoczęcia realizacji zadań Kierownika Projektu, co było nierzetelne.
Ponadto, Dyrektor NASK nie zrealizował obowiązków określonych w § 2 ust. 8 umowy o partnerstwie w jej pierwotnym brzmieniu (obowiązującym przed zawarciem aneksu z 12 marca 2025 r.), zgodnie z którym Partner wiodący (CPPC) i Partner (NASK) mieli obowiązek

[10] W skład którego wchodził przewodniczący oraz członkowie.
[11] W skład którego wchodził Kierownik Projektu, Kierownik Biznesowy Projektu, Lider merytoryczny Projektu oraz członkowie.

wyznaczyć swoich przedstawicieli do Zespołu Projektowego[12] oraz wzajemnie się o tym poinformować. [str. 35–36]

**Zapewnienie pracowników posiadających odpowiednie kompetencje**

Osoby pełniące funkcje Kierownika Projektu, Kierownika Biznesowego Projektu oraz Lidera Merytorycznego Projektu posiadały kwalifikacje adekwatne do wykonywanych zadań. Pracownicy, do których zadań należała ocena wniosków o przyznanie grantu pod względem merytorycznym (tj. 25 spośród 121 osób zaangażowanych w realizację Projektu), posiadali wykształcenie i doświadczenie zawodowe w zakresie cyberbezpieczeństwa. [str. 37]

**NASK zorganizował i zrealizował nabór wniosków o przyznanie grantu**

NASK, zgodnie z § 5 ust. 7 pkt 1 umowy o partnerstwie, zorganizował i zrealizował nabór wniosków o przyznanie grantu. Nabór odbywał się według Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" z wykorzystaniem narzędzia informatycznego (system LSI), za pomocą którego wnioskodawcy składali wnioski o przyznanie grantu. Wnioski te podlegały ocenie formalnej, a następnie ocenie merytorycznej przez ekspertów. [str. 37–38]

**Wsparcie NASK dla jst**

NASK, zgodnie z § 5 ust. 7 pkt 2 umowy o partnerstwie, zapewnił wparcie dla wnioskodawców (jednostek samorządu terytorialnego) podczas naboru wniosków. Wsparcie to jest również kontynuowane podczas realizacji Projektu. [str. 37–38]

**Prawidłowa weryfikacja przez NASK wniosków o przyznanie grantu**

W wyniku badania na próbie 15 grantów dla jst ustalono, że wnioski jst o przyznanie grantu spełniały kryteria formalne i merytoryczne określone w Regulaminie Konkursu. NASK po przeprowadzeniu oceny formalnej i merytorycznej wniosków opracowywał zestawienie wniosków zatwierdzonych do dofinansowania i przekazywał informacje o wynikach oceny do wnioskodawców. Następnie NASK gromadził dokumentację do zawarcia umów grantowych i przekazywał przygotowane umowy do CPPC celem ich podpisania. [str. 38]

**Nierzetelna weryfikacja wniosków o rozliczenie grantu**

W NASK ustanowiono 23 maja 2025 r. wewnętrzną *Procedurę weryfikacji wniosku rozliczającego zaliczkę (grant).* Stwierdzono jednak, że NASK nierzetelnie zweryfikował 13 z 15 badanych przez NIK wniosków o rozliczenie grantu złożonych przez jst i zatwierdził je, pomimo tego, że były sporządzone wadliwie lub nie zawierały wszystkich wymaganych załączników. [str. 38–42]

**Audyty na zakończenie grantu nie zostały ustandaryzowane**

Zgodnie z § 3 ust. 3 Regulaminu Konkursu grantobiorcy mieli obowiązek *przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI*[13], zgodnie z określonymi w Regulaminie Konkursu warunkami[14], oraz dostarczyć raport z tego audytu do NASK wraz z wnioskiem o rozliczenie grantu[15]. W dokumentacji konkursowej,

[12] O którym mowa była w § 1 ust. 17 umowy o partnerstwie – dalej: Zespół Projektowy.

[13] Obowiązującego do 22 maja 2024 r. Odpowiednio § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

[14] M.in. zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie jst miał obejmować zgodność z kryteriami zawartymi w § 20 ust. 2 rozporządzenia KRI z 2012 r. lub zgodność z wymaganiami normy PN-ISO/IEC 27001 (§ 3 ust. 3 pkt 1 Regulaminu Konkursu).

[15] Zgodnie z § 4 ust. 10 Regulaminu Konkursu.

za której przygotowanie odpowiadało CPPC[16], audyty nie zostały w żaden inny sposób ustandaryzowane i nie sformułowano w niej obowiązku zamieszczenia w raportach z tych audytów oceny podniesienia poziomu odporności na cyberzagrożenia w związku z realizacją Projektu. Zastępca Dyrektora NASK wyjaśnił, że *Przeprowadzenie audytów KRI u Grantobiorców nie miało na celu oceny podniesienia poziomu odporności na cyberzagrożenia w związku z realizacją projektu Cyberbezpieczny Samorząd (...). Grantodawca[17] wymagał jedynie załączenia raportu z audytu KRI wykonanego na zakończenie realizacji grantu*. [str. 43]

**Monitorowano przebieg prac**

W NASK prowadzono bieżący monitoring wykonania umowy o partnerstwie, który odbywał się m.in. poprzez cotygodniowe wewnętrzne spotkania członków Zespołu projektowego, cotygodniowe spotkania z CPPC oraz spotkania w cyklach dwutygodniowych z przedstawicielami CPPC, Ministerstwa Cyfryzacji oraz Ministerstwa Funduszy i Polityki Regionalnej. Ze spotkań tych NASK sporządzało notatki. Do CPPC, a następnie do przedstawicieli Ministerstwa Cyfryzacji, co tydzień wysyłano również wiadomości mailowe, zawierające informacje o aktualnym stanie realizacji Projektu. [str. 43]

**JST w dokumentach strategicznych nie uwzględniały zwiększenia poziomu cyberbezpieczeństwa**

W dokumentach strategicznych większości kontrolowanych urzędów (16 spośród 17, tj. 94%) nie uwzględniono zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa. Tłumaczono to najczęściej małą istotnością tego zagadnienia w momencie opracowywania tych strategii, tj. w latach 2014–2020, a także brakiem prowadzenia analiz w tym zakresie i brakiem wymogów prawnych. W kontrolowanych jst podawano również, że prowadzone analizy w ówczesnych uwarunkowaniach społeczno-gospodarczych szczególny nacisk kładły na poprawę dostępności cyfrowej administracji. [str. 45–46]

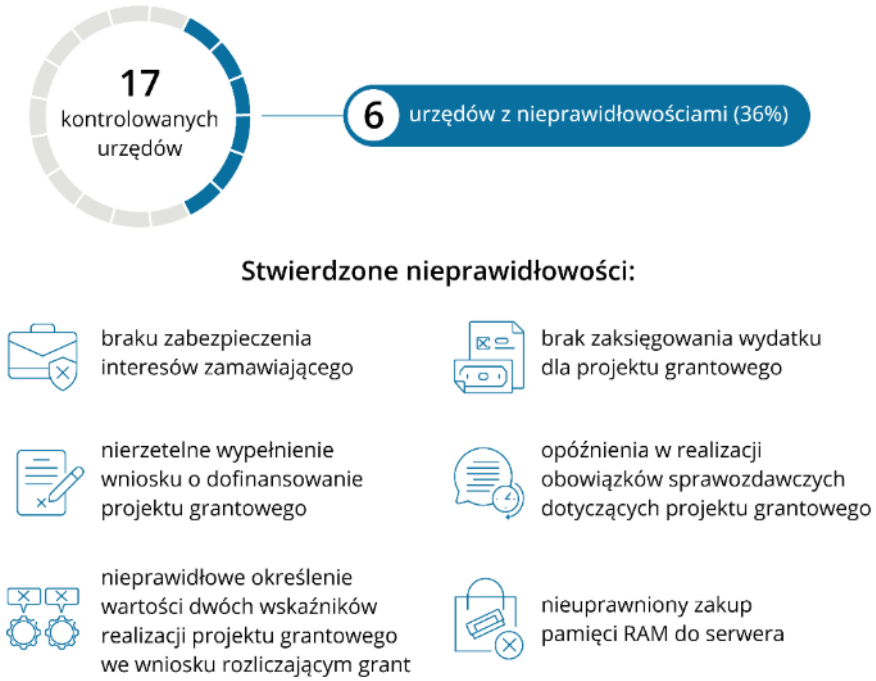
**Wartość kontrolowanych przez NIK grantów wyniosła 13 mln zł**

Badaniem objęto prawidłowość wykorzystania 17 najwyższych wartościowo grantów w ramach projektu „Cyberbezpieczny Samorząd" finansowane z Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, wybranych spośród tych urzędów jst, które najwcześniej otrzymały wszystkie transze grantu. Łączna wartość przyznanych kontrolowanym urzędom grantów wyniosła 13 mln zł. Na dzień zakończenia poszczególnych kontroli w badanych jst, wartość wydatkowanych przez JST środków wyniosła 7,7 mln zł (z uwzględnieniem wkładu własnego w łącznej kwocie 932 tys. zł), co stanowiło 59% środków przyznanych na realizację projektów grantowych. Ponadto, zaangażowanie w umowach jst z wykonawcami w ramach badanych umów grantowych wynosiło 1,5 mln zł, co stanowiło 11,8% łącznej kwoty środków przeznaczonych na realizację projektów grantowych w kontrolowanych jst. [str. 48–51]

[16] Zgodnie z § 4 ust. 4 pkt 9 umowy o partnerstwie.
[17] Tj. CPPC.

**Nieprawidłowości w realizacji grantów w JST**

Infografika nr 2
Nieprawidłowości w realizacji grantów




*Źródło: opracowanie własne NIK na podstawie danych z kontroli.*

Nieprawidłowości w realizacji grantów stwierdzono w sześciu z 17 kontrolowanych urzędów (36%). Nie miały one jednak zasadniczego wpływu na prawidłowość wykorzystania grantu, poza UG Świerklany. Dotyczyły m.in.:

- braku zabezpieczenia interesów zamawiającego, co było działaniem nierzetelnym (UMiG w Górze, UG Kłodzko);
- zakupu komponentów serwera w postaci 14 pamięci RAM o wartości 23 800,00 zł, co nie mieściło się bezpośrednio w katalogu działań (usług) na jakie można przeznaczyć środki projektu, określonym w § 3 ust. 2 pkt 3 Regulaminu Projektu. Ponadto zakup ten nie był ujęty we wniosku o przyznanie grantu (UMiG w Górze);
- wskazania we wniosku o dofinansowanie projektu *Poprawa cyberbezpieczeństwa Powiatu Białobrzeskiego*, informacji niezgodnej ze stanem faktycznym, że starostwo posiada wdrożony i audytowany system SZBI, a jego dokumentacja wymagać będzie jednak dalszej aktualizacji/poprawy i rozbudowy z uwzględnieniem planowanych rozwiązań, co było działaniem nierzetelnym (Starostwo Powiatowe w Białobrzegach);
- niezaksięgowania do dnia 18 czerwca 2025 r. w ewidencji księgowej wydatku dla projektu grantowego, w kwocie 11 070 zł, poniesionego w grudniu 2023 r., na usługi doradcze w zakresie przygotowania koncepcji projektu oraz przygotowania dokumentacji finansowej – budżetu projektu, co było niezgodne z postanowieniami § 4 ust. 1 pkt 6 umowy grantowej (Starostwo Powiatowe w Białobrzegach);

- opóźnienia w realizacji obowiązków sprawozdawczych dotyczących projektu grantowego, co stanowiło naruszenie § 7 ust. 2 umowy grantowej (Starostwo Powiatowe w Legionowie);
- nieprawidłowego określenia wartości dwóch wskaźników realizacji projektu grantowego we wniosku rozliczającym grant (UMiG Serock).

W przypadku UG Świerklany NIK negatywnie oceniła działalność Urzędu w zakresie realizacji projektu grantowego. Stwierdzono m.in. nieprawidłowości dotyczące: nieuzasadnionego opóźnienia odbioru I etapu przedmiotu umowy na wykonanie usługi doradczej w ramach grantu; udzielenia zamówienia publicznego na dostawę urządzeń i oprogramowania bez zastosowania przepisów ustawy z dnia 11 września 2019 r. *Prawo zamówień publicznych*[18] oraz nierzetelnej realizacji przedmiotu tego zamówienia przez wykonawcę; wdrożenia *Polityki Bezpieczeństwa Teleinformatycznego*, która zawierała nierzetelne zapisy i postanowienia niezgodne z przepisami rozporządzenia KRI, a także nieprzeprowadzenia w 2024 r. okresowego audytu w zakresie bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI. [str. 51–53]

**Wskaźniki realizacji projektów grantowych nie były powiązane z faktycznym wzrostem poziomu cyberbezpieczeństwa w jst**

Zgodnie z § 4 ust. 10 Regulaminu Konkursu, jst w ramach realizacji projektów grantowych były zobowiązane do realizacji wskaźników określonych w załączniku nr 9 do ww. Regulaminu.

Kontrola wykazała, że zdefiniowane przez CPPC wskaźniki realizacji projektów grantowych, tak produktu, jak i rezultatu, nie były w żaden sposób powiązane z faktycznym wzrostem poziomu cyberbezpieczeństwa u grantobiorców (jst), a jedynie z liczbą dokonanych zakupów i przeszkolonych osób. Co więcej, w kontrolowanych urzędach występowały sytuacje, gdy wartości wskaźników zostały wyznaczone na najniższym możliwym poziomie, tj. jeden projekt grantowy to jedna jednostka danego wskaźnika. W pięciu objętych kontrolą urzędach (29%) na etapie zawierania umowy o powierzenie grantu nie wskazano wskaźników produktu i rezultatu lub nie podano ich wartości. [str. 53–55]

**Wykorzystanie zakupionych urządzeń i dostarczonych usług**

Poza UG Świerklany, zakupione w ramach kontrolowanych projektów grantowych urządzenia i oprogramowanie zostały zainstalowane i były użytkowane lub były na etapie wdrożenia. Szkolenia zostały przeprowadzone lub były zaplanowane do realizacji. Zamówione w ramach grantu audyty bezpieczeństwa informacji zostały wykonane i sformułowano w nich wnioski/rekomendacje, z których część została wdrożona, a część była w trakcie realizacji lub została zaplanowana do realizacji. [str. 55]

**W ponad połowie kontrolowanych jst nie wdrożono SZBI**

Pomimo przystąpienia do projektu Cyberbezpieczny Samorząd, w ponad połowie kontrolowanych urzędów nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, który jest kluczowym elementem zapewnienia cyberbezpieczeństwa. Spośród dziewięciu urzędów, w których przed przystąpieniem do projektu grantowego brak było Systemu Zarządzania Bezpieczeństwem Informacji wymaganego rozporządzeniem KRI, w siedmiu z nich (77%) przewidziano opracowanie

[18] Dz. U. z 2024 r., poz. 1320, ze zm.

SZBI w ramach grantu w zakresie obszaru organizacyjnego. W pozostałych dwóch urzędach jst (23%) działania takie nie były planowane. [str. 56–57]

**W prawie połowie kontrolowanych jst nie przeprowadzono okresowego audytu z zakresu bezpieczeństwa informacji**

W ośmiu urzędach (47%) w 2023 r. lub 2024 r. nie przeprowadzono obowiązkowego audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI[19] lub audyt przeprowadzono nierzetelnie, bądź z naruszeniem zasady niezależności i obiektywizmu audytu. Powyższe nieprawidłowości tłumaczono m.in. brakiem pracowników posiadających niezbędną wiedzę i doświadczenie dla przeprowadzenia takiego audytu. [str. 57–58]

Infografika nr 3
Nieprawidłowości w zakresie zapewnienia bezpieczeństwa informacji


*Źródło: opracowanie własne NIK na podstawie danych z kontroli.*

**Inne stwierdzone nieprawidłowości związane z bezpieczeństwem informacji**

W siedmiu urzędach jst z 17 badanych (41%) stwierdzono inne niż ww. nieprawidłowości w zakresie bezpieczeństwa informacji. Nieprawidłowości te dotyczyły m.in.:

- niewłaściwego zabezpieczenia serwerowni, w tym przechowywania w nich materiałów łatwopalnych;
- niewłaściwego sporządzania kopii zapasowych;
- posiadania przez osoby, które zakończyły zatrudnienie uprawnień do systemów informatycznych;

[19] Obowiązującego do 22 maja 2024 r. Odpowiednio z § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

- niestosowania procedury przyznawania uprawnień w systemach informatycznych;
- ustawienia monitorów w sposób umożliwiający wgląd osobom postronnym w dane osobowe;
- ustanowienia Polityki Bezpieczeństwa Informacji zawierającej wewnętrznie sprzeczne i niezgodne z prawem postanowienia i zapisy.

[str. 58–59]

# 4. WNIOSKI

**NIK wnosi o:**

**Minister Cyfryzacji we współpracy z Ministrem Funduszy i Polityki Regionalnej oraz Dyrektorem CPPC**

Zapewnienie powiązania kwalifikowalności wydatków z osiągnięciem zakładanego wzrostu poziomu cyberbezpieczeństwa w przypadku realizowania kolejnych projektów w tym obszarze, w szczególności poprzez:

- uwzględnienie w przyszłych projektach wymogu przeprowadzenia ustandaryzowanego audytu bezpieczeństwa informacji zarówno przed przystąpieniem do projektu, jak i po jego zakończeniu,
- określenie wskaźników realizacji projektów grantowych, tak produktu, jak i rezultatu, pozwalających na zmierzenie wpływu działań zrealizowanych w ramach uczestnictwa w projekcie na poziom cyberbezpieczeństwa.

# 5. WAŻNIEJSZE WYNIKI KONTROLI

## 5.1. REALIZACJA PRZEZ CENTRUM PROJEKTÓW POLSKA CYFROWA PROJEKTU „CYBERBEZPIECZNY SAMORZĄD”

**CPPC zorganizowało konkurs grantowy w ramach projektu „Cyberbezpieczny Samorząd” zgodnie z obowiązującymi regulacjami**

CPPC prawidłowo zorganizowało nabór wniosków do Konkursu Grantowego Cyberbezpieczny Samorząd (dalej: konkurs grantowy), określiło kryteria wyboru projektów grantowych i zapewniło jst równy dostęp do środków grantowych.

**Organizacja prac w ramach Projektu**

Ustanowiono struktury zarządcze, w tym wyznaczono pracowników odpowiedzialnych za realizację Projektu. Określono system monitorowania wskaźników produktu i rezultatu dla Projektu. W ramach systemu monitorowania organizowano cotygodniowe spotkania z przedstawicielami NASK, podczas których omawiano bieżące tematy związane z realizacją Projektu, postępy prac, trudności i ryzyka. Analizowano raporty Partnera z realizacji Projektu w zakresie liczby podpisanych umów, zleconych i wypłaconych przelewów, złożonych wniosków o kolejne transze, wniosków końcowych i sprawozdań.

W dokumentacji konkursu grantowego nie przewidziano oceny poziomu cyberbezpieczeństwa jst na etapie składania wniosków o grant oraz nie powiązano kwalifikowalności wydatków ponoszonych w ramach umów o powierzeniu grantów ze wzrostem poziomu cyberbezpieczeństwa jst po wykorzystaniu grantu.

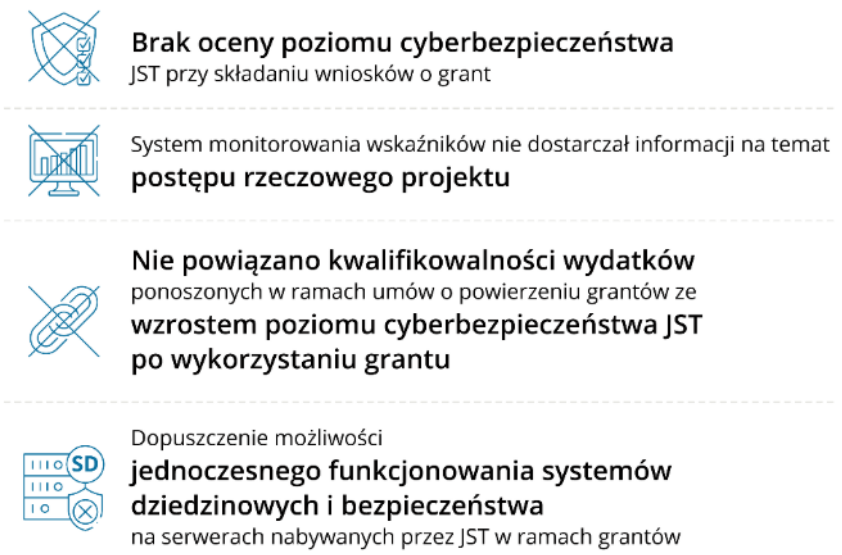
W związku z realizacją Projektu przewidziano zarządzanie ryzykiem i zidentyfikowano 11 ryzyk, jednak w analizie ryzyka zamiast wymaganych mechanizmów kontrolnych opisano mechanizmy zapobiegania, które, zdaniem NIK, nie zapewniały bezzwłocznego podjęcia działań zaradczych w przypadku wystąpienia ryzyka, co było działaniem nierzetelnym i ogranicza skuteczność systemu zarządzania Projektem.

Przyjęty w Projekcie system monitorowania wskaźników nie dostarczał informacji na temat postępu rzeczowego, ponieważ CPPC dotychczas dokumentowało i sprawozdawało monitorowanie tylko jednego wskaźnika dotyczącego liczby podmiotów wspartych w zakresie cyberbezpieczeństwa, co było działaniem nierzetelnym.

W ramach Projektu CPPC dopuściło możliwość jednoczesnego funkcjonowania systemów dziedzinowych i bezpieczeństwa na serwerach nabywanych przez jst w ramach grantów na zwiększenie bezpieczeństwa informacji, co było niezgodne z wymogami § 15 ust. 1 rozporządzenia KRI.

Ponadto, stwierdzone nieprawidłowości polegały m.in. na:
- poniesieniu przez CPPC jako Beneficjenta w ramach zadania nr 5 „Ewaluacja, rozliczenie projektu” wydatków w wysokości 828,3 tys. zł przed planowanym terminem jego rozpoczęcia, co było niezgodne z postanowieniami § 5 ust. 8 DoD, a także z § 4 ust. 3 UoP;
- niewystąpieniu Beneficjenta do Instytucji Pośredniczącej w sprawie potrzeby zmiany wskaźników w związku z brakiem możliwości osiągnięcia dwóch zaplanowanych wskaźników w ramach Projektu, co było nierzetelne.

Infografika nr 4
Nieprawidłowości w CPPC




*Źródło: opracowanie własne NIK na podstawie danych z kontroli.*

**Struktura zarządcza Projektu**

Decyzją Zastępcy Dyrektora CPPC ustanowiono strukturę zarządczą Projektu, która podlegała zmianom w zależności od etapu przedsięwzięcia i zachodzących zmian w zatrudnieniu. W okresie objętym kontrolą Zespół projektowy liczył 11 osób. Zarządzeniem Dyrektora CPPC wprowadzono zasady rozdzielności funkcji odnośnie do projektów własnych, pomiędzy IP a Beneficjentem. Według tych zasad, do zadań Beneficjenta należy w szczególności: przygotowanie, podpisanie i złożenie wniosku o dofinansowanie, podpisanie umowy (w przypadku przedmiotowego projektu decyzji) o dofinansowanie, aneksów, utworzenie zespołu projektowego, realizacja projektu i poddanie się kontroli zgodnie z postanowieniami umowy (tu: decyzji) o dofinansowanie. W zasadach określono też, że zespół Beneficjenta stanowią pracownicy Biura Projektów Własnych lub Kierownik projektu oraz wskazani w decyzji o powołaniu zespołu projektowego pracownicy komórek wspierających, a pracownicy IP nie biorą udziału w zadaniach wykonywanych przez zespół Beneficjenta. CPPC działające jako IP wykonuje swoje zadania zgodnie z dyspozycjami art. 9 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (dalej: ustawa wdrożeniowa), z uwzględnieniem Porozumień oraz właściwych wytycznych i instrukcji wykonawczych obowiązujących w CPPC.

**Nabór wniosków w ramach Projektu**

W 2023 r. w ramach konkursu grantowego zorganizowano nabór wniosków, w którym złożono 2614 wniosków na łączną kwotę 1 538 611,8 tys. zł. Ocenie poddano 2515 wniosków (316 w 2023 r. i 2199 w 2024 r.) o łącznej wartości 1 486 209,5 tys. zł. Wszystkie umowy o powierzenie grantu zawarto z JST w 2024 r. Było to 2497 umów na kwotę 1 475 253,3 tys. zł. Na dzień 31 sierpnia 2025 r. realizowanych było 2490 projektów grantowych o łącznej wartości 1 471 218,6 tys. zł. Na dzień 31 sierpnia 2025 r. grantobiorcy złożyli 26 wniosków o płatność rozliczających grant na kwotę 16 072,6 tys. zł, z których do dnia

zakończenia kontroli NASK rozliczył 17 na kwotę 10 753,5 tys. zł. Na dzień 31 sierpnia 2025 r. kwota wykorzystana dla całego Projektu kształtuje się na poziomie 1 122 238,9 tys. zł, co stanowi 62,4% całkowitej alokacji.

W ramach Projektu zaplanowano jeden nabór grantowy. Tryb wyboru wniosków o dofinansowanie określono w jednym z elementów dokumentacji konkursu grantowego – Schemacie grantowym (dalej: Schemat), który został przekazany do IP przez Beneficjenta 18 lipca 2023 r., a zatem na dzień przed rozpoczęciem naboru grantowego. Ostatecznie dokumentacja konkursu grantowego wraz ze Schematem została zaakceptowana przez Instytucję Zarządzającą oraz IP w dniu 11 sierpnia 2023 r., a zatem 17 dni roboczych po terminie rozpoczęcia naboru. Mając na względzie ten termin, zakres zmian oraz jednoczesne przedłużenie terminu składania wniosków o granty, NIK uznaje, że ogłoszenie konkursu z warunkowo zaakceptowaną dokumentacją naboru nie miało wpływu na przebieg konkursu. Zgodnie z treścią Schematu realizacja konkursu pn. „Cyberbezpieczny Samorząd" nastąpiła w formie projektu grantowego w rozumieniu art. 41 ustawy wdrożeniowej. Nabór, wraz ze wszystkimi dokumentami, ogłoszono na stronie internetowej Projektu w dniu 29 sierpnia 2025 r.

Beneficjent zrealizował zadania w zakresie przygotowania konkursu grantowego i naboru do Projektu zgodnie z harmonogramem określonym we WoD. We wniosku tym wskazano, że rozpoczęcie realizacji Projektu nastąpiło 1 lipca 2023 r., przygotowanie konkursu grantowego trwało od 1 do19 lipca 2023 r., a uruchomienie naboru rozpoczęto 19 lipca 2023 r. Według wyjaśnień Dyrektora CPPC, datę rozpoczęcia realizacji Projektu, czyli 1 lipca 2023 r., Beneficjent wyznaczył wcześniej niż datę uruchomienia naboru, ponieważ w tym czasie prowadził prace przygotowawcze. Obejmowały one m.in. przygotowanie dokumentacji naborowej dla grantobiorców oraz inne działania niezbędne do sprawnego uruchomienia konkursu. Następnie 19 lipca 2023 r. Beneficjent uruchomił konkurs grantowy.

W ramach Projektu nie wyczerpano pełnej puli środków przewidzianej na jego realizację (alokacja wynosiła 1 874 294,0 tys. zł, w tym 1 494 000,0 tys. zł z budżetu środków europejskich i 380 294,3 tys. zł z budżetu państwa, a bez wkładu własnego grantobiorców 1 798 235,4 tys. zł). Do 31 sierpnia 2025 r. kwota niewykorzystanych środków w Projekcie wynosiła 675 996,5 tys. zł (tj. 36,1%).

Beneficjent rozwiązał siedem umów grantowych, wszystkie na wniosek grantobiorców, na łączną kwotę 4132,7 tys. zł. Z uwagi na to, że w konkursie grantowym wzięło udział 89% jednostek uprawnionych, Beneficjent nie badał powodów odstąpienia pozostałych jst od udziału w naborze. Beneficjent nie przewiduje dodatkowych naborów. Odnośnie powodów, dla których nie przewidziano dodatkowych naborów dyrektor CPPC wyjaśnił, że *decyzja o nieuruchamianiu kolejnych naborów została podjęta po analizie zainteresowania projektem, możliwości realizacyjnych jednostek samorządu terytorialnego (jst), oraz efektywności wykorzystania dostępnych środków. Należy zauważyć, że pomimo wydłużenia terminu trwania pierwotnego naboru, w dalszym ciągu nie wszystkie jst zdecydowały się na udział w nim. Samorządy, które były zdecydowane na udział, złożyły wnioski w wyznaczonym czasie. Grupa,*

*która nie złożyła wniosków wynosiła około 10% wszystkich jst, co wskazuje na brak szerszego zapotrzebowania na dodatkowe nabory. Także wśród samorządów, które początkowo złożyły wnioski, występowały przypadki niepodpisania Umowy, lub zdecydowania się na jej rozwiązanie w trakcie realizacji. Analiza budżetu projektu w kontekście powstałych oszczędności wykazała, że ewentualny dodatkowy nabór mógłby być:*

- *ograniczony wyłącznie do jst, które nie złożyły wniosków wcześniej. Jednakże, jak wynika z dotychczasowych obserwacji, ta grupa nie wykazywała zainteresowania projektem,*
- *otwarty dla wszystkich jst (przy założeniu udziału ok. 2000–2500 jednostek) – co jednak skutkowałoby kilkukrotnym obniżeniem wysokości nowych grantów, czyniąc je nieatrakcyjnymi i nieefektywnymi przy podobnym koszcie obsługi nowego grantu,*
- *ograniczony do określonej liczby wniosków z zasadą "kto pierwszy, ten lepszy", co jednak nie byłoby optymalnym rozwiązaniem. Taka formuła mogłaby dyskryminować mniejsze jst, które często nie są w stanie szybko przygotować i złożyć wniosków. Stałoby to w sprzeczności z celem projektu zakładającym dotarcie do szerokiego spektrum jednostek, w tym tych mniejszych. Z naszej kilkuletniej współpracy z samorządami także w innych projektach (Zdalna Szkoła, Zdalna Szkoła Plus, Cyfrowa Gmina) wiemy, że niestety nie wszystkie JST dysponują odpowiednim potencjałem kadrowym, oraz zasobami niezbędnymi do szybkiej realizacji dodatkowych zadań projektowych.*

*Wobec powyższej analizy stwierdziliśmy, że dodatkowy nabór mógłby prowadzić do niskiej efektywności i ryzyka niewykorzystania środków, lub nieosiągnięcia zakładanych celów. Organizacja dodatkowych naborów w ramach tego Projektu, mogłaby także nie spełniać kryteriów celowości, efektywności i gospodarności wydatkowania środków publicznych. Priorytetem pozostaje skuteczna realizacja Projektu, przy zachowaniu jakości i adekwatności wsparcia.*

**Wnioski jst o przedłużenie okresu kwalifikowalności wydatków w ramach grantu**

Do 31 sierpnia 2025 r. prośbę o wydłużenie okresu kwalifikowalności wydatków/realizacji Projektu zgłosiło trzech grantobiorców:

- Województwo Podlaskie – w związku z wydłużeniem terminu zawarcia umowy z CPPC i tym samym skróceniem okresu, w jakim grantobiorca przewidywał realizację projektu grantowego;
- gmina Cieszanów – w związku z równoległą realizacją przez gminę innego projektu pn. „Przyjazny e-urząd w Cieszanowie" dofinansowanego w ramach priorytetu FEPK.01 „Konkurencyjna i Cyfrowa Gospodarka", działanie FEPK.01.02 „Cyfryzacja programu regionalnego Fundusze Europejskie dla Podkarpacia na lata 2021–2027";
- Starostwo Powiatowe w Mrągowie – w związku z koniecznością ponownej analizy wniosku o dofinansowanie grantu przez nowo wybrany Zarząd Powiatu i zmiany omyłkowo opisanego wskaźnika w zakresie liczby jednostek organizacyjnych powiatu i liczby usług wsparcia realizowanych przez ekspertów z zakresu cyberbezpieczeństwa.

**Zgłoszenia w sprawie potencjalnych nieprawidłowości w ramach Projektu**

W I półroczu 2025 r. CPPC otrzymało pięć zgłoszeń od sygnalisty w sprawie potencjalnych nieprawidłowości dotyczących kwalifikowalności wydatków w Projekcie dokonywanych przez grantobiorców na zakup serwerów, przeznaczonych na zapewnienie cyberbezpieczeństwa, ale jednocześnie wykorzystywanych do obsługi aplikacji dziedzinowych, co było według sygnalisty niezgodne z założeniami Projektu. Sygnalista poinformował o dokonaniu takich zakupów przez jst po analizie kilkudziesięciu upublicznionych postępowań ogłoszonych w ramach Projektu.

CPPC działając jako IP otrzymało również pięć zgłoszeń za pośrednictwem Prezesa Urzędu Zamówień Publicznych (dalej: UZP) w sprawie nieprawidłowości w realizacji przez pięciu grantobiorców zamówień publicznych (gmina Węgliniec, gmina Bierawa, powiat strzeliński, gmina Siechnice oraz gmina Czastary: znaki spraw: CPPC-D03B00-W04.72.1.6.2.2025/MJ, CPPC-D03B00-W04.72.1.2.3.2025/MJ, CPPC-D03B00-W04.72.2.6.2.2024/MJ). CPPC w odpowiedzi do Prezesa UZP poinformowało, że NASK, zgodnie z procedurą monitorowania i kontroli, na etapie rozliczania Projektu przeprowadzi weryfikację wydatków grantobiorców. Dodatkowo CPPC poinformowało, że Partner (NASK) przeprowadzi u trzech grantobiorców (powiat strzeliński, gmina Siechnice oraz gmina Czastary) w 2025 r. kontrolę doraźną w celu weryfikacji zgłoszonych nieprawidłowości. Odnośnie do gmin Bierawa i Węgliniec poinformowano, że CPPC wspólnie z Partnerem ustali zakres i terminy kontroli, którą Partner będzie prowadził u grantobiorców.

CPPC działając jako Beneficjent otrzymało jedno zgłoszenie złożone przez przedsiębiorcę dotyczące podejrzenia nieprawidłowości w procedurze wyboru wykonawcy w przetargu organizowanym przez gminę miasto Sochaczew. CPPC na dzień zakończenia kontroli było na etapie analizowania sprawy.

Ponadto, CPPC działając jako Beneficjent otrzymało zgłoszenie złożone za pośrednictwem Ministerstwa Funduszy i Polityki Regionalnej przez organizacje pozarządowe dotyczące podejrzenia nieprawidłowości przy przyznaniu dofinansowania beneficjentowi (gmina Odrzywół) w ramach FERC. Na dzień zakończenia kontroli sprawa była rozpatrywana przez CPPC.

**Zarządzanie ryzykiem w Projekcie**

W opracowanym przez CPPC WoD, w pkt H2 „Analiza ryzyka w projekcie", zidentyfikowano łącznie 11 ryzyk dotyczących Projektu, oszacowano prawdopodobieństwo ich wystąpienia, zdefiniowano skutek oraz wskazano mechanizmy zapobiegania. Zidentyfikowane ryzyka dotyczyły braku możliwości wniesienia wkładu własnego przez jst, niedoszacowania lub przeszacowania budżetu Projektu, niewystarczającego poziomu zainteresowania konkursem grantowym, niepoprawnie działającej aplikacji naboru wniosków grantowych, braku odpowiedniej infrastruktury w jst do modernizacji w ramach projektu, niestabilnej sytuacji w obszarze cen towarów, usług oraz kursów walut, problemów z płynnością dostaw rozwiązań IT, braku chęci do użytkowania zakupionych i zmodernizowanych rozwiązań i usług przez jst, problemów z pozyskaniem wykwalifikowanej kadry przez jst do obsługi wdrożonych rozwiązań, opóźnień w realizacji projektu, niepodpisania oraz rozwiązania części umów grantowych. Zidentyfikowane ryzyka w ramach Projektu do dnia zakończenia kontroli nie były aktualizowane.

**W ramach zarządzania ryzykiem nie wskazano wymaganych mechanizmów kontrolnych**

Dla dwóch ryzyk skutkujących opóźnieniem realizacji Projektu Beneficjent wskazał mechanizmy zapobiegania ich wystąpieniu z pominięciem elementów kontroli. We WoD opisano je następująco:

- dla ryzyka dotyczącego problemów z płynnością dostaw rozwiązań IT związanych np. z ograniczeniami gospodarczymi wynikającymi ze zbrojnej agresji Rosji w Ukrainie i obostrzeniami epidemiologicznymi, o dużej sile oddziaływania ryzyka i średnim prawdopodobieństwie wystąpienia – sposób zarządzania ryzykiem poprzez zmiany w harmonogramie Projektu i dostosowanie go do sytuacji. Łagodzeniem ryzyka będzie poszukiwanie rozwiązań alternatywnych, które mogą zastąpić niedostępne rozwiązania;
- dla ryzyka dotyczącego opóźnienia realizacji Projektu, o dużej sile oddziaływania ryzyka i średnim prawdopodobieństwie wystąpienia – Wnioskodawca planując etapy Projektu założył ramy czasowe obejmujące dodatkowy bufor, uwzględniający nagłe zdarzenia wpływające na czas realizacji zadania. Ponadto Wnioskodawca w przypadku wystąpienia tego ryzyka dokona powtórnej analizy procesu realizacji Projektu, m.in. pod kątem możliwości zaangażowania zespołu projektowego do realizacji wymaganych w tym czasie zadań.

Dyrektor CPPC poinformował, że dotychczas nie wystąpiło żadne z ryzyk wskazanych we WoD, a Beneficjent na bieżąco kontroluje sytuację i jest przygotowany do podjęcia odpowiednich działań, jeśli pojawi się taka potrzeba.

W „Instrukcji użytkownika Aplikacji WOD2021. Wnioski o dofinansowanie. Wnioskodawca" (stan na dzień 17 marca 2023 r., wersja 1.8) w pkt 1.2.8. dotyczącym sekcji H „Analiza ryzyka" zawarto tabelę z instrukcją jej wypełnienia umieszczoną w sekcji H2 WoD. W tabeli tej, w opisie dotyczącym rubryki „Mechanizmy zapobiegania" (str. 49), zawarto wymaganie, aby opisać krótko mechanizmy kontrolne, które Beneficjent zamierza zastosować, aby obniżyć opisywane ryzyko.

CPPC wskazało we WoD ryzyka, przy czym dla żadnego z nich nie wskazano konkretnych mechanizmów kontrolnych, tj. instrukcji, procedur i narzędzi monitorowania. Wskazane w analizie ryzyka mechanizmy zapobiegania dla 11 zidentyfikowanych ryzyk nie zostały opisane w sposób gwarantujący bezzwłoczne podjęcie działań zaradczych, co było działaniem nierzetelnym. Zamiast wskazania mechanizmów kontrolnych, które pozwoliłyby na pozyskiwanie wiedzy na temat zagrożeń w obrębach poszczególnych ryzyk, CPPC zawarło w analizie ryzyka ogólne stwierdzenia, niewskazujące konkretnych działań, procedur, osób odpowiedzialnych ani narzędzi monitorowania. CPPC na etapie realizacji Projektu, w trakcie kontroli NIK, podjęło próbę wypracowania mechanizmów kontrolnych i procedur reagowania.

Dyrektor CPPC wyjaśnił m.in., że od momentu uruchomienia naboru CPPC wdraża konkretne działania ograniczające ryzyko opóźnień w realizacji Projektu, polegające m.in. na wdrożeniu infolinii projektowej i adresu e-mail, strony internetowej Projektu, czy też organizacji webinarów dla grantobiorców.

Zdaniem NIK, opisane w analizie ryzyka mechanizmy zapobiegania nie identyfikują faktycznego zagrożenia, a przeciwdziałają skutkom zaistnienia ryzyka opóźnienia w realizacji Projektu dopiero w reakcji na zgłoszenie z zewnątrz. Świadczy o tym fakt, że do dnia 31 sierpnia 2025 r. odnotowano szereg sygnałów mogących świadczyć o występowaniu istotnych zagrożeń dla terminowej realizacji Projektu, w tym: trzy jednostki samorządu terytorialnego wystąpiły z wnioskami o przedłużenie okresu kwalifikowalności wydatków lub realizacji Projektu, zarejestrowano pięć zgłoszeń sygnalisty dotyczących wątpliwości w zakresie kwalifikowalności wydatków, pięć zgłoszeń wpłynęło za pośrednictwem Prezesa UZP i dotyczyło możliwych nieprawidłowości w zakresie zamówień publicznych realizowanych przez pięć różnych jst, dodatkowo jedno zgłoszenie zostało przekazane bezpośrednio do CPPC jako Beneficjenta. W reakcji na te zagrożenia CPPC przesłało rekomendacje do jst o konieczności zakończenia Projektu zgodnie z dotychczasowymi założeniami i uruchomiło proces opracowywania procedury kontroli zasygnalizowanych nieprawidłowości w zakresie zamówień publicznych. Należy zauważyć, że zgłaszane problemy w obszarze realizacji zamówień publicznych dotyczą jednego z kluczowych ryzyk wpływających na ewentualne opóźnienia w realizacji Projektu, a działania CPPC polegające na uzgadnianiu procesu kontrolnego podejmowane są dopiero po zaistnieniu zdarzeń mogących mieć wpływ na terminową realizację Projektu.

**Zidentyfikowane przez CPPC problemy w realizacji Projektu**

Z ustaleń kontroli wynika, że CPPC posiadało Informacje o problemach, jakie występują w trakcie realizacji Projektu. Beneficjent brał udział w regularnych spotkaniach z Partnerem Projektu, które były organizowane raz w tygodniu. Na spotkaniach omawiane były bieżące tematy związane z realizacją Projektu, postępy prac, trudności i ryzyka, jakie dostrzegają partnerzy wraz z propozycją rozwiązania problemu. Na spotkaniach wspólnie planowano działania na najbliższe tygodnie.

W sporządzonych przez Partnera Projektu notatkach, w których zawarto ustalenia z cotygodniowych spotkań z CPPC wskazano problemy związane z realizacją Projektu dotyczące m.in.:

- wydłużenia okresu realizacji Projektu, gdyż coraz więcej jst zgłaszało prośby o wydłużenie okresu kwalifikowalności wydatków/realizacji Projektu. Podjęto decyzję, że zostaną skierowane pisma do jst z informacją o konieczności zakończenia Projektu w założonym terminie;
- kwestii nieprawidłowości zgłaszanych przez sygnalistów na etapie prowadzenia postępowań przetargowych w jst. Postanowiono, że należy uzgodnić z NASK proces kontroli na obsługę tego typ zdarzeń;
- procedury rozliczania wniosków o płatność przez CPPC oraz NASK i ustalenia jak będzie przebiegał ten proces oraz czy będzie on polegał na weryfikacji dokumentów przez dwóch pracowników. Przyjęto, że wskazane jest, aby wnioski były weryfikowane przez dwie osoby.

**Harmonogram prac nad Projektem**

Harmonogram prac nad Projektem określono we WoD. W ramach zmiany WoD wprowadzonej aneksem nr FERC.02.02-IP.01-0001/23-02 wcześniej rozpoczęto realizację zadania nr 4 Monitorowanie naboru i realizacji projektów grantowych, kontrola projektów grantowych, lecz pozostało to bez wpływu na termin jego zakończenia. Prace były realizowane zgodnie z harmonogramem.

**Poniesienie przez CPPC wydatków przed planowanym terminem rozpoczęcia jednego z zadań**

W ramach zadania nr 5 „Ewaluacja, rozliczenie projektu", którego realizację zaplanowano na okres od 1 listopada 2025 r. do 31 grudnia 2027 r., poniesiono wydatki niezgodnie z WoD, tj. przed terminem rozpoczęcia zadania. Na dzień 31 maja 2025 r. wydatki w tym zadaniu (w pozycji 5.2 Personel projektu – Wynagrodzenia pracowników) wyniosły 828,3 tys. zł, co stanowiło 50% alokacji dla tego zadania. Realizację ww. zadania zaplanowano na okres od 1 listopada 2025 r. do 31 grudnia 2027 r.

Dyrektor CPPC potwierdził, *że zadanie nr 5 zgodnie z aktualną wersją Wniosku o dofinansowanie powinno rozpocząć się 1.11.2025 r. Jednakże już w styczniu 2025 r. do Partnera Projektu wpłynęły pierwsze wnioski rozliczające grant, co wymusiło wcześniejsze rozpoczęcie czynności w tym zakresie (...) Beneficjent przekaże do Instytucji Pośredniczącej wniosek o zgodę na wprowadzenie zmiany terminu rozpoczęcia zadania nr 5 przy planowanym aneksie do Decyzji o dofinansowaniu. W odniesieniu do danych zawartych we wniosku o płatność nr 10 – Partner błędnie przypisał wszystkie koszty osobowe z 2025 r. do zadania nr 5, podczas gdy część z tych wynagrodzeń dotyczy faktycznie zadań realizowanych w ramach zadania nr 3. Błąd ten został zidentyfikowany i Beneficjent przygotuje wyjaśnienia do Instytucji Pośredniczącej, wraz z prośbą o możliwość korekty wniosku nr 10 i odpowiednie przypisanie kosztów do zadań nr 3 i 5.*

**W dokumentacji konkursu grantowego nie przewidziano oceny poziomu cyberbezpieczeństwa u grantobiorców na etapie składania przez nich wniosków o grant**

W dokumentacji konkursu grantowego CPPC nie przewidziało oceny poziomu cyberbezpieczeństwa u grantobiorców na etapie składania przez nich wniosków o grant oraz nie przyjęto zasady, aby powiązać osiągnięty poziom cyberbezpieczeństwa po zakończeniu prac w ramach grantu z kwalifikowalnością wydatków, co było nierzetelne. Należy podkreślić, że celem Projektu grantowego jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych jst.

Dyrektor CPPC wyjaśnił, że *na etapie składania wniosków przewidziano ocenę poziomu cyberbezpieczeństwa na podstawie kryteriów nr 6 i 8. Kolejnym etapem oceny jest dwukrotne dostarczenie ankiety dojrzałości cyberbezpieczeństwa – zarówno po podpisaniu umowy, jak i na etapie rozliczenia grantu. (...) Do udziału w naborze były uprawnione wszystkie jednostki samorządu terytorialnego (dalej jst). Dla każdej jst określono maksymalną kwotę grantu o jaką mogły się ubiegać. Tym sposobem jst nie konkurowały ze sobą np. wysokością zadeklarowanego poziomu cyberbezpieczeństwa (...) Bezpośrednie powiązanie wyników oceny ankiety dojrzałości z kwalifikowalnością wydatków zdaniem Beneficjenta jest nieuzasadnione. W ramach Projektu przyjmuje się, że poziom bezpieczeństwa jednostki podniesie się względem stanu, gdyby Projekt nie został w niej wdrożony. Często wdrożenie nowych rozwiązań może skutkować utrzymaniem poziomu bezpieczeństwa lub dostosowaniem do zmieniających się regulacji*

*(w tym nadchodzącej implementacji dyrektywy NIS2) obowiązujących Jednostki Samorządu Terytorialnego.*

Zdaniem NIK, brak oceny poziomu cyberbezpieczeństwa na etapie składania wniosków przez jst o przyznanie grantu może przyczynić się do nieefektywnego wykorzystywania środków w Projekcie, ponieważ CPPC jako Beneficjent nie może ocenić tego w jakim stopniu przyznany grant podniósł poziom bezpieczeństwa jst.

W ramach kryterium 6. *Zasadność kosztów w Projekcie* „weryfikacji podlega czy Wnioskodawca grantowy wystarczająco uzasadnił potrzebę wskazanych wydatków oraz ich racjonalność w kontekście celu projektu oraz potrzeb Wnioskodawcy", zaś w ramach kryterium 8. *Opis koncepcji projektu* „weryfikacji podlega, czy Wnioskodawca grantowy przedstawił opis koncepcji Projektu zawierający informacje: o potrzebach Wnioskodawcy grantowego w zakresie cyfryzacji urzędu w tym zwiększenia poziomu bezpieczeństwa informacji urzędu (...), celach i efektach Projektu, w tym w odniesieniu do celów FERC".

W żadnym z ww. kryteriów nie jest zatem oceniany stan początkowy oraz wzrost poziomu cyberbezpieczeństwa, który będzie skutkiem realizacji Projektu grantowego. W § 3 ust. 3 Regulaminu konkursu grantowego przewidziano konieczność przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji i przekazanie raportu z tego audytu wraz z wnioskiem rozliczającym projekt, lecz nie połączono wyników tego audytu z oceną wzrostu poziomu cyberbezpieczeństwa osiągniętym w wyniku realizacji Projektu grantowego i kwalifikowalnością wydatków w tym zakresie.
W związku z powyższym NIK sformułowała wniosek pokontrolny aby w przypadku prowadzenia kolejnych projektów dotyczących cyberbezpieczeństwa, uwzględniono wymóg oceny poziomu cyberbezpieczeństwa na etapie składania wniosków o przyznanie grantu, a także po zakończeniu jego realizacji w powiązaniu z kwalifikowalnością wydatków. W odpowiedzi Dyrektor CPPC wskazał, że w kolejnych projektach związanych z cyberbezpieczeństwem zostanie wprowadzony obowiązek oceny poziomu cyberbezpieczeństwa na etapie składania wniosków o przyznanie grantu.

Zgodnie z § 3 ust. 3 Regulaminu konkursu grantobiorcy na etapie rozliczenia grantu mieli obowiązek przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI[20] oraz zgodnie z określonymi w Regulaminie konkursu warunkami, a także dostarczyć raport z tego audytu do NASK wraz z wnioskiem rozliczającym Projekt . W dokumentacji konkursowej, za której przygotowanie odpowiadało CPPC, audyty nie zostały w żaden inny sposób ustandaryzowane. W szczególności nie sformułowano obowiązku zamieszczenia w raportach z tych audytów oceny podniesienia poziomu odporności jst na cyberzagrożenia w związku z realizacją Projektu. Ustalenia dokonane w ramach tych audytów nie zostały powiązane z kwalifikowalnością wydatków.

[20] Obowiązującego do 22 maja 2024 r. Odpowiednio § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

**Dopuszczenie przez CPPC możliwości jednoczesnego funkcjonowania na serwerach zarówno systemów dziedzinowych jak i systemów bezpieczeństwa**

W Projekcie, w ramach projektów grantowych, dopuszczono możliwość jednoczesnego funkcjonowania na serwerach zarówno systemów dziedzinowych[21], jak i systemów bezpieczeństwa, co należy uznać za niezgodne z § 15 ust. 1 rozporządzenia KRI, stanowiącym, że systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk. Współistnienie tych systemów zwiększa ryzyko eskalacji (podniesienia) uprawnień, ponieważ aplikacja dziedzinowa – nawet jeśli nie jest dostępna z Internetu – może stanowić wektor ataku w sieci wewnętrznej. Dodatkowo prowadzi to do potencjalnego konfliktu o zasoby serwera, co obniża stabilność i niezawodność systemów bezpieczeństwa.

NIK zauważa, że celem grantu jest zwiększenie poziomu bezpieczeństwa, a zatem serwer powinien być wykorzystywany do uruchamiania systemów bezpieczeństwa wdrożonych w ramach projektu grantowego, a wszelkie dodatkowe aplikacje powinny działać na odrębnej infrastrukturze.

Dyrektor CPPC wyjaśnił, że *Beneficjent dopuścił taką możliwość, ponieważ kategoryczne wyłączenie takiej możliwości, a przez to potencjalny brak kwalifikowalności wydatku, byłoby niewskazane w wypadku stanu wyższej konieczności, w którym każda decyzja pozwalająca na przywrócenie możliwości świadczenia usług warta jest rozważenia. (...) Utrzymanie ciągłości pracy systemów jest ważnym celem mieszącym się w obszarze odporności na zagrożenia. Dopuszcza się, że w ramach serwera fizycznego zainstalowany jest system wirtualizacyjny. (...) Analogicznie mogą funkcjonować również systemy dziedzinowe, które zostaną zainstalowane na oddzielnych innych maszynach wirtualnych w ramach tego samego serwera fizycznego (w tym w klastrach wysokiej dostępności). (...) Należy jednak zauważyć, że o ile zakup serwerów i oprogramowanie zapewniające bezpieczeństwo są ujęte w katalogu kosztów kwalifikowalnych, to już użytkowanie oraz obsługa wszelkich aplikacji dziedzinowych, ich komponentów oraz serwerów bazodanowych na zakupionym sprzęcie będą uznawane za koszty niekwalifikowalne w ramach projektu.*

Mając na względzie ogólne cele programu FERC, jak wsparcie transformacji cyfrowej kraju przez realizację przedsięwzięć, które zapewnią m.in. skuteczne działanie krajowego systemu cyberbezpieczeństwa, jak i cel szczegółowy interwencji określony dla działania 2.2, tj. inwestycje zwiększające poziom bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych, nie sposób zgodzić się z podejściem zaprezentowanym przez CPPC. Separacja systemów dziedzinowych i bezpieczeństwa pozwala ograniczyć zakres ataków i zmniejszyć skalę ewentualnych strat, ułatwia zarządzanie całą infrastrukturą i nie wpływa negatywnie na jej wydajność[22]. Kluczowe jest bowiem faktyczne i możliwe najwyższe

[21] Na przykład w UG Wilkowice na serwerze pełniącym funkcje bezpieczeństwa zainstalowano system zdalnego nauczania.

[22] Wynika to z zasad zarządzania IT i jest zgodne normami i dobrymi praktykami, np. ISO 27001 i NIST SP 800-53 rev.5.

zwiększenie poziomu cyberbezpieczeństwa. Zdaniem NIK, przyjęte w konkursie grantowym rozwiązanie narusza zasadę separacji funkcji, zgodnie z którą systemy bezpieczeństwa i aplikacje użytkowe nie powinny współdzielić zasobów tego samego serwera.

Biorąc pod uwagę powyższe, NIK sformułowała wniosek pokontrolny aby w przypadku realizacji kolejnych projektów w zakresie wdrażania rozwiązań informatycznych zapewnić wymóg separacji systemów dziedzinowych i bezpieczeństwa na serwerach. Dyrektor CPPC w odpowiedzi na wystąpienie pokontrolne podał, że w kolejnych podobnych projektach zostanie zapewniony wymóg separacji systemów dziedzinowych od systemu bezpieczeństwa, zgodnie z dobrymi praktykami i standardami bezpieczeństwa.

**Długotrwały proces zawierania umów przez CPPC z grantobiorcami**

W wyniku badania 30 umów zawartych przez CPPC z grantobiorcami ustalono, że okres liczony od dnia zakończenia oceny WoD do dnia podpisania umowy wynosił od 3 do 8 miesięcy, czyli średnio około pół roku, przy czym okres zawierania tych umów (liczony od dnia otrzymania od grantobiorców kompletnych i poprawnych dokumentów niezbędnych do podpisania umowy, o których mowa w § 6 ust. 4 Regulaminu konkursu grantowego Cyberbezpieczny samorząd do dnia podpisania umowy przez CPPC) wynosił od 14 do 182 dni, czyli średnio około 3 miesięcy. Spowodowało to skrócenie okresu na realizację umów przez grantobiorców, gdyż zakończenie realizacji umów musi nastąpić do 30 czerwca 2026 r.

Najdłuższy okres zawierania umowy miał miejsce w przypadku następujących grantobiorców: miasto i gmina Bochnia – 182 dni, Urząd Marszałkowski Województwa Lubelskiego w Lublinie – 166 dni, gmina Baranów – 154 dni, Urząd Marszałkowski Województwa Pomorskiego w Gdańsku – 143 dni, miasto stołeczne Warszawa – 140 dni.
Dyrektor CPPC podał m.in., że kluczowym powodem takiego stanu rzeczy był wydłużający się proces oceny formalnej i merytorycznej oraz etap przygotowania poprawnej dokumentacji przez jst. Ponadto Dyrektor CPPC podkreślił znaczenie skali całego przedsięwzięcia i liczby pracowników zajmujących się obsługą wniosków i podpisywaniem umów (ok. 23 osób w CPPC i NASK). Dyrektor wskazał też, że długi czas trwania procedury zawarcia umowy nie był efektem bezczynności po stronie Beneficjenta, ale złożonego i rozciągniętego w czasie procesu po stronie grantobiorcy i Partnera.

**Nadzór CPPC nad realizacją zadań przez NASK**

W ramach nadzoru nad realizacją przez Partnera (NASK) zadań określonych w UoP, CPPC podejmowało działania polegające m.in. na:

- udziale w cotygodniowych spotkaniach statusowych z Partnerem, na których omawiane były bieżące tematy związane z realizacją Projektu, postęp prac, występujące trudności i możliwe ryzyka. W trakcie spotkań planowane były działania na kolejne tygodnie;

W tej ostatniej normie zawarto następujące reguły kontrolne: SC-2 – Separation of System and User Functionality – Mechanizmy bezpieczeństwa (security functions) powinny być realizowane oddzielnie od funkcjonalności użytkowej systemu; SC-3 – Security Function Isolation Funkcje bezpieczeństwa muszą być izolowane od innych funkcji w systemie informatycznym; SA-14 – Criticality Analysis (uzupełniająca) – Podkreśla konieczność identyfikacji i odseparowania elementów krytycznych (np. usług bezpieczeństwa) od reszty systemu.

- analizie cotygodniowych raportów z realizacji prac, przesyłanych przez Partnera, zawierających m.in. dane z obsługi helpdesk, statystyki z liczby podpisanych umów, zleconych i wypłaconych przelewów, złożonych wniosków o kolejne transze, wniosków końcowych, sprawozdań;
- weryfikacji przekazywanych przez Partnera dokumentów niezbędnych do podpisania umów o powierzenie grantu;
- weryfikacji wniosków o płatność składanych przez Partnera;
- prowadzeniu zestawienia wydatków i środków rozliczonych w projekcie w celu weryfikacji zaawansowania finansowego Projektu;
- przygotowywaniu we współpracy z Partnerem informacji i instrukcji publikowanych na stronie internetowej Projektu w sekcji „Pytania i Odpowiedzi".

CPPC do dnia zakończenia kontroli, tj. do 5 września 2025 r., nie prowadziło kontroli realizacji Projektu w NASK.

**Kontrole Projektu prowadzone przez IP**

W latach 2023–2025 (do 5 września 2025 r.) CPPC działając jako IP przeprowadziło kontrolę CPPC jako Beneficjenta w zakresie działań podejmowanych w Projekcie i faktycznego postępu rzeczowego prac. Zalecenia pokontrolne zawarte w Informacji Pokontrolnej z 14 marca 2025 r. (FERC.02.02-IP.01-0001/23-003-INF) wskazywały na potrzebę:

- większej staranności przy wypełnianiu wniosku o płatność w zakresie spójności danych. CPPC jako Beneficjent poinformowało, że zwróciło się do Partnera o większą staranność przy składaniu wniosków o płatność i dokładniejsze weryfikowanie przekazywanej dokumentacji;
- powołania Zespołu projektowego, zgodnie z UoP. CPPC jako Beneficjent poinformowało, że powołało zespoły projektowe zgodnie z opisem Beneficjenta i Partnera wskazanymi we WoD, który stanowi załącznik do DoD. W ramach zaleceń pokontrolnych CPPC zobowiązało się opracować zmianę do UoP, które uwzględnią powołanie dwóch odrębnych zespołów projektowych i dołożyć wszelkich starań, aby planowany do podpisania aneks do UoP odzwierciedlał założenia z WoD;
- uzupełniania w kolejnych wnioskach o płatność informacji o nazwę grantobiorcy i numer umowy o powierzenie grantu, aby zapewnić spójność danych i ścieżkę audytu. CPPC jako Beneficjent poinformowało, że jest na etapie konsultacji z administratorem systemu Teta oraz z dostawcą systemu i w sytuacji, gdy taka zmiana będzie możliwa do wprowadzenia wypełni zalecenie pokontrolne lub znajdzie inne rozwiązanie;
- całościowej weryfikacji i aktualizacji listy rankingowej grantobiorców oraz ustalenia przez CPPC sposobu rozliczenia aktualnej wysokości przyznanego grantu w przypadku zmian kwot dofinansowania na liście rankingowej dla wszystkich grantobiorców. CPPC jako Beneficjent poinformowało, że jest na końcowym etapie weryfikacji listy rankingowej i że zamieści poprawną listę rankingową na stronie

internetowej. Ponadto, do każdego wniosku o płatność dołączy odrębne zestawienie wypłaconych grantów z podziałem na środki UE i BP oraz z informacją o numerze transzy, co umożliwi IP dokładną weryfikację wypłat;

– wprowadzenia i stosowania przez Partnera miesięcznych kart czasu pracy dla personelu zaangażowanego w realizację Projektu, które potwierdzą faktyczne zaangażowanie w Projekt w danym miesiącu i będą stanowiły podstawę do wyliczenia kwalifikowanej części wynagrodzenia i jego rozliczania w Projekcie. CPPC jako Beneficjent poinformowało Partnera o konieczności stosowania miesięcznych kart czasu pracy i konsultowało z Partnerem i IP formę prowadzenia ewidencji przez Partnera.

**CPPC jako Beneficjent nie zgłosiło braku możliwości osiągnięcia jednego wskaźnika produktu i jednego wskaźnika rezultatu**

CPPC działając jako Beneficjent we WoD przewidział dla Projektu 11 wskaźników produktu i cztery wskaźniki rezultatu. Do dnia zakończenia czynności kontrolnych CPPC działając jako Beneficjent nie zgłosiło CPPC działającemu jako Instytucja Pośrednicząca faktu braku możliwości osiągnięcia jednego wskaźnika produktu – *Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji* i jednego wskaźnika rezultatu – *Liczba jst wspartych w zakresie cyberbezpieczeństwa* spośród określonych we WoD. Zważywszy na to, że nabór wniosków grantowych zakończył się 14 grudnia 2023 r., mając na względzie postanowienia § 22 ust. 2 pkt 2 DoD, w myśl których IP może uchylić decyzję o dofinansowaniu w przypadku, gdy Beneficjent nie zrealizował wskaźników produktu i rezultatu określonych we wniosku o dofinansowanie, niezgłoszenie do dnia zakończenia czynności kontrolnych faktu nieosiągnięcia ww. wskaźników należy uznać za nierzetelne. Jest to o tyle istotne, że z postanowień § 19 ust. 4 DoD wynika, iż zmiany w obrębie wskaźników zdefiniowanych we WoD wymagają akceptacji Instytucji Pośredniczącej i są wprowadzane aneksem do decyzji.

W toku kontroli ustalono, że dwa ww. wskaźniki, których wartość ustalono na poziomie 2807, na pewno nie zostaną osiągnięte, gdyż w ramach jedynego naboru grantowego w ramach Projektu złożono 2614 wniosków, a obecnie realizowanych jest 2490 umów o powierzeniu grantu, z czego wynika, że możliwe jest osiągnięcie 88,7% zakładanego poziomu wskaźników.

Dyrektor CPPC wyjaśnił, że *wskaźnik odnoszący się do liczby Grantobiorców (2807) nie zostanie osiągnięty. Różnica ta jest trwała i nieodwracalna, ponieważ nabór nie będzie powtórzony (...) Beneficjent podjął działania mające na celu dostosowanie wskaźników projektu do faktycznego poziomu jego realizacji. Trwają robocze rozmowy z Instytucją Pośredniczącą, Instytucją Zarządzającą oraz Ministerstwem Cyfryzacji w zakresie planowanej aktualizacji Decyzji o dofinansowanie, w tym Wniosku o dofinansowanie. Planowana zmiana obejmuje zarówno korektę wskaźnika liczby Grantobiorców, jak i proporcjonalne zmniejszenie pozostałych wskaźników bezpośrednio powiązanych z liczbą jst*. (...) *Obecnie Beneficjent na nowo szacuje wartości wskaźników i aktualizuje treść wniosku o dofinansowanie*.

**CPPC nie sprawozdawało na bieżąco we wnioskach o płatność wartości wskaźników dla Projektu**

CPPC działające jako Beneficjent do 1 lipca 2025 r. nie sprawozdawało na bieżąco we wnioskach o płatność wartości wskaźników, co naruszało postanowienia § 4 ust. 4 pkt 11 UoP oraz pkt 7 i 8 sekcji 2.1.3 „Wytycznych dotyczących monitorowania postępu rzeczowego realizacji programów na lata 2021–2027" Ministra Funduszy i Polityki Regionalnej[23]. Powyższe postanowienia nakładają na Beneficjentów obowiązek bieżącego monitorowania postępu rzeczowego, czemu służą m.in. wartości wskaźników sprawozdawane we wnioskach o płatność.

Dyrektor CPPC poinformował, że: *Beneficjent od początku realizacji projektu raportuje postępy zgodnie z wymaganiami wynikającymi z Decyzji o dofinansowanie oraz zapisów Wniosku o dofinansowanie. Do tej pory raportował do Instytucji Pośredniczącej jedynie wskaźnik „Liczba jst wspartych w zakresie cyberbezpieczeństwa", ponieważ był on bezpośrednio powiązany z wypłatami grantów. Pozostałe wskaźniki Beneficjent będzie mógł raportować na bieżąco po zatwierdzeniu przez Partnera wniosków o rozliczenie grantu złożonych przez jst. Obecnie Partner zatwierdził 15 wniosków rozliczających grant (dane na dzień 18.07.2025 r.), na podstawie których Beneficjent wskaże wartości osiągniętych wskaźników we wniosku o płatność nr 11. Beneficjent zaktualizuje ten wniosek i uzupełni dane wskaźnikowe.*

Należy zauważyć, że dopiero w dwunastym Wniosku o płatność (za okres od 1 do 30 lipca 2025 r.), składanym w trakcie kontroli NIK, Beneficjent uzupełnił dane w zakresie wartości osiągniętych wskaźników, pomimo że przed wskazanym okresem zatwierdził już pierwsze wnioski jst o rozliczenie grantu.

**Terminowa realizacja prac**

Do 31 sierpnia 2025 r. nie wystąpiły opóźnienia w realizacji Projektu. Według wyjaśnień Dyrektora CPPC, dotychczas nie wystąpiły problemy w realizacji Projektu, skutkujące zagrożeniem jego pełnej realizacji. Postępy prac, występujące trudności i ewentualne problemy związane z realizacją Projektu były omawiane na bieżąco w trakcie organizowanych co tydzień spotkań CPPC i NASK.

**Kontrole prowadzone w ramach Projektu**

Do dnia zakończenia kontroli w CPPC działającym jako Beneficjent, CPPC działające jako IP przeprowadziło kontrolę dotyczącą realizacji działań w ramach Projektu (zalecenia IP opisano na str. 31–32). Ponadto, kontrolę w tym zakresie przeprowadziła także Izba Administracji Skarbowej w Warszawie (dalej: IAS). W trakcie audytu projektu FERC.02.02-IP.01-0001/23 „Cyberbezpieczny Samorząd" IAS ustaliła, że CPPC jako Beneficjent wykazało we wnioskach o płatność nr FERC.02.02-IP.01-0001/23-002 i nr FERC.02.02-IP.01-0001/23-003 zawyżone o 18 360,81 zł koszty pośrednie. Zgodnie z DoD, Beneficjent mógł rozliczyć koszty pośrednie według stawki ryczałtowej w wysokości 15% kwalifikowanych bezpośrednich kosztów personelu. W odpowiedzi na wyniki audytu, CPPC zgłosiło zastrzeżenia dotyczące sposobu rozliczania kosztów pośrednich. W odpowiedzi na zastrzeżenia, IAS podtrzymała pierwotne ustalenie. Beneficjent dokonał po tym korekty kosztów pośrednich pomniejszających te koszty o kwotę 18 360,81 zł.

[23] https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/prawo-i-dokumenty/wytyczne/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

## 5.2. Realizacja przez NASK działań na rzecz osiągania rezultatów określonych w projekcie „Cyberbezpieczny Samorząd”

**NASK prowadził zgodne z umową o partnerstwie, działania na rzecz osiągania rezultatów, jednak stwierdzone nieprawidłowości wskazują na potrzebę zwiększenia staranności rozliczania grantów**

W okresie objętym kontrolą NASK, jako partner Centrum Projektów Polska Cyfrowa, prowadził zgodne z umową o partnerstwie, działania na rzecz osiągania rezultatów (zamierzonych skutków) określonych w projekcie Cyberbezpieczny Samorząd, realizowanym w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027.

NASK zapewnił wystarczającą dla sprawnej realizacji Projektu obsadę kadrową oraz ustanowił odpowiednie struktury zarządcze. Pracownicy NASK uczestniczący w realizacji Projektu, w szczególności eksperci merytoryczni oceniający wnioski o udzielenie grantu, posiadali odpowiednie kwalifikacje. Realizacja Projektu przebiegała terminowo, zgodnie z przygotowanym harmonogramem i była na bieżąco monitorowana przez NASK.

NASK zgodnie z § 5 ust. 7 pkt 1 umowy o partnerstwie zorganizował i przeprowadził nabór wniosków o przyznanie grantu. W naborze tym, zgodnie z § 5 ust. 7 pkt 2 umowy o partnerstwie, NASK zapewnił różnego rodzaju wsparcie dla wnioskodawców, m.in. infolinię telefoniczną i webinaria, z którego mogli oni korzystać również na etapie realizacji grantów. Przy ocenie wniosków o przyznanie grantu NASK prawidłowo weryfikował spełnianie przez wnioskodawców kryteriów formalnych i merytorycznych. Następnie NASK gromadził dokumentację do zawarcia umów grantowych i przekazywał ją do CPPC celem podpisania. Zgodnie z przyjętym harmonogramem obecnie trwa etap realizacji powierzonych grantów, a NASK rozpoczął weryfikację pierwszych wniosków o rozliczenie grantu.

Stwierdzone w toku kontroli nieprawidłowości polegały na:

- wydaniu decyzji w przedmiocie powołania nowego Kierownika Projektu po ponad 18 miesiącach od faktycznego powierzenia mu tej funkcji, co było nierzetelne,
- niewyznaczeniu przedstawicieli NASK do Zespołu Projektowego, co było niezgodne z § 2 ust. 8 w zw. z § 1 ust. 17 umowy o partnerstwie,
- nierzetelnej weryfikacji 13 z 15 objętych badaniem wniosków o rozliczenie grantu.

W ocenie NIK, nieprawidłowości te nie miały zasadniczego wpływu na realizację zadań NASK określonych w umowie o partnerstwie, jednak wskazują one na potrzebę zwiększenia staranności przy ich realizacji.

**Zapewnienie przez NASK pracowników do sprawnej realizacji prac**

Przed rozpoczęciem realizacji Projektu w NASK oszacowano liczbę pracowników niezbędnych do jego sprawnej realizacji. Według tych szacunków Projekt miał zostać zrealizowany przez 92 pracowników, zatrudnionych łącznie na 91,5 etatach, a nakład pracy tych osób miał wynieść 1484,35 osobomiesięcy.

Od rozpoczęcia Projektu do 31 lipca 2025 r. w jego realizację było zaangażowanych łącznie 121 pracowników, w tym 98 osób, których wynagrodzenie miesięczne stanowiło (przynajmniej w części) koszty kwalifikowalne w ramach Projektu i które wykonały pracę w łącznym

wymiarze 310,33 osobomiesięcy oraz 21 ekspertów ds. oceny formalnej oraz ds. oceny merytorycznej, których wynagrodzenie za zrealizowane oceny było wypłacane jako dodatek zadaniowy[24]. W realizacji Projektu uczestniczyły także dwie osoby jako członkowie Komitetu Sterującego, które pełniły funkcje zarządcze i których wynagrodzenie nie stanowiło kosztów kwalifikowalnych w ramach Projektu.

Według szacunków liczba osobomiesięcy do 31 lipca 2025 r. miała wynieść 710,25. Dyrektor NASK wyjaśnił, że różnica pomiędzy planem, a jego wykonaniem wynikała m.in. ze zmiany sposobu rozliczania wynagrodzeń za prace ekspertów ds. oceny formalnej i merytorycznej (planowano rozliczanie na bazie alokacji, faktycznie rozliczano na podstawie dodatku zadaniowego) i wyceny zadania, które finalnie nie zostało ujęte w zaakceptowanym wniosku o dofinansowanie, gdyż nastąpiło zmniejszenie zakresu projektu w stosunku do planów. Dyrektor NASK wyjaśnił również, że *przy tak różnorodnym projekcie charakteryzującym się różną pracochłonnością na każdym etapie, w przypadku konieczności zaangażowania dodatkowych pracowników, Kierownik projektu w przypadkach spiętrzenia zadań angażuje dodatkowe zasoby na realizację wszystkich prac zgodnie z harmonogramem i zapisami umowy.*

**Nieprawidłowości w zakresie powoływania kluczowych pracowników w Projekcie**

Dyrektor NASK decyzją z 10 lipca 2023 r.[25] powołał w NASK Komitet Sterujący Projektu[26] i Zespół projektowy realizujący Projekt[27] oraz m.in. określił ich skład i zadania. Decyzją Dyrektora NASK z 3 lutego 2025 r. kolejnym Kierownikiem Projektu została osoba, która faktycznie pełniła tę funkcję już od 17 lipca 2023 r.

Dopiero po ponad 18 miesiącach od rozpoczęcia przez nowego pracownika NASK realizacji zadań Kierownika Projektu i uczestnictwa w pracach Zespołu projektowego, Dyrektor NASK wydał decyzję, którą formalnie powołał tę osobę na tę funkcję, co było nierzetelne.

Dyrektor NASK wyjaśnił, że osoba powołana na funkcję Kierownika Projektu *została zatrudniona 17.07.2023 r. i od tego dnia pełniła funkcję Kierownika projektu FERC JST – Cyberbezpieczny Samorząd, co znalazło swoje odzwierciedlenie w Repozytorium projektów w Jira[28] (...) Brak aktualizacji Decyzji Dyrektora NASK z 10.08.2023 r.[29] nie miał wpływu na realizację projektu*. Ponadto Dyrektor NASK wyjaśnił, że *przed wydaniem decyzji z dnia 3 lutego br. nie nastąpiło pisemne powierzenie pełnienia roli Kierownika Projektu Pani (...) przez Dyrektora NASK. Pani (...) została zatrudniona na stanowisko Kierownika projektu, czego potwierdzeniem jest zakres obowiązków pracownika jak również powierzenie do projektu, które zgodnie z obowiązującymi procedurami podpisywane jest przez pracownika i jego bezpośredniego przełożonego*.

---

[24] Na podstawie decyzji Dyrektora NASK o przyznaniu dodatku zadaniowego.

[25] Decyzja Dyrektora NASK – PIB z dnia 10 lipca 2023 r. w sprawie powołania w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym Komitetu Sterującego Projektu oraz w sprawie powołania zespołu realizującego Projekt Cyberbezpieczny Samorząd w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 w Partnerstwie z Centrum Projektów Polska Cyfrowa.

[26] W skład którego wchodził przewodniczący oraz członkowie.

[27] W skład którego wchodził Kierownik Projektu, Kierownik Biznesowy Projektu, Lider merytoryczny Projektu oraz członkowie – dalej: Zespół projektowy.

[28] System do zarządzania projektami zarządczymi oraz wytwórczymi.

[29] Omyłka pisarska – powinno być: „10.07.2023 r.”.

Zdaniem NIK, powołanie Kierownika Projektu powinno zostać dokonane niezwłocznie decyzją Dyrektora NASK, co miało miejsce, ale dopiero po ponad 18 miesiącach od rozpoczęcia realizacji zadań jako Kierownik Projektu przez tę osobę.

Dyrektor NASK nie zrealizował obowiązków określonych w § 2 ust. 8 umowy o partnerstwie w jej pierwotnym brzmieniu (obowiązującym przed zawarciem aneksu z 12 marca 2025 r.), zgodnie z którym Partner wiodący (CPPC) i Partner (NASK) mieli obowiązek wyznaczyć swoich przedstawicieli do Zespołu Projektowego[30] oraz wzajemnie się o tym poinformować.

Zgodnie z § 2 ust. 8 pierwotnego tekstu umowy o partnerstwie, Partner wiodący (CPPC) i Partner (NASK) mieli obowiązek wyznaczyć swoich przedstawicieli do Zespołu Projektowego oraz wzajemnie się o tym poinformować (w formie pisemnej, elektronicznej lub za pośrednictwem poczty elektronicznej), a w piśmie wyznaczającym przedstawiciela, obok danych osobowych, upoważniający miał umieścić zakres upoważnienia oraz dane do kontaktu z przedstawicielem. Zgodnie z § 1 ust. 17 tej umowy Zespół Projektowy miał być organem wykonawczym i zarządzającym – składającym się z Kierownika Projektu ze strony Partnera wiodącego oraz Koordynatora – Kierownika Projektu ze strony Partnera oraz osób ds. obsługi administracyjno-biurowej, finansowej, kadrowej, informacji i promocji, prawnej, technicznej, nadzoru i innych osób działających w imieniu Partnera wiodącego i Partnera.

Dyrektor NASK wyjaśnił, że *NASK-PIB przekazał w dniu 10.07.2023 roku podpisany Załącznik numer 2 do Umowy Partnerskiej powołujący zespół projektowy po stronie NASK. Dodatkowo w dniu 20.07.2023 roku przekazano mailowo informację o osobach pełniących kluczowe role w projekcie*.

Zdaniem NIK ani powołanie Zespołu projektowego po stronie NASK, ani przekazanie informacji o osobach z NASK pełniących kluczowe role w Projekcie nie stanowiło realizacji obowiązków określonych w § 2 ust. 8 umowy o partnerstwie, w szczególności obowiązku wyznaczenia przedstawicieli do Zespołu Projektowego w rozumieniu § 1 ust. 17 tej umowy.

W trakcie kontroli dokonano zmiany uwarunkowań prawnych (w związku z zawarciem przez strony aneksu do umowy o partnerstwie, którym m.in. zmieniono definicję Zespołu Projektowego i uchylono § 2 ust. 8 tej umowy.

**Harmonogram prac**

Przed rozpoczęciem realizacji Projektu NASK we współpracy z CPPC przygotował w czerwcu 2023 r. wstępny harmonogram ramowy. Na etapie rozpoczęcia realizacji Projektu[31] został on zaktualizowany, a następnie trzykrotnie wprowadzano do niego zmiany polegające na wydłużeniu terminu naboru wniosków o przyznanie grantu[32] i w konsekwencji przesunięciu terminów realizacji kolejnych etapów Projektu. Dyrektor NASK wyjaśnił, że *przesunięcia terminów spowodowane były w szczególności*

[30] O którym mowa była w § 1 ust. 17 umowy o partnerstwie.

[31] 12 lipca 2023 r.

[32] Zmiany te zostały dokonane: 11 sierpnia 2023 r. – wydłużono, pierwotnie ustalony na 30 września 2023 r., termin na składanie wniosków konkursowych do 13 października 2023 r., 6 października 2023 r. – wydłużono termin na składanie wniosków konkursowych do 30 listopada 2023 r. oraz 20 listopada 2023 r. – wydłużono termin na składanie wniosków konkursowych do 14 grudnia 2023 r.

*małą liczbą składanych wniosków o granty z Projektu Cyberbezpieczny Samorząd przez podmioty uprawnione. W szczególności NASK, na prośbę CPPC, promował projekt poprzez udział swoich przedstawicieli na konferencjach w okresie wrzesień – październik 2023*. Realizacja Projektu odbywała się zgodnie ze zaktualizowanym harmonogramem.

Dodatkowo, przy wykorzystaniu specjalistycznych narzędzi informatycznych, został opracowany harmonogram szczegółowy prac, który był na bieżąco prowadzony i w razie potrzeby modyfikowany. Dyrektor NASK wyjaśnił, że *zmiany harmonogramu szczegółowego wynikają z bieżących aktywności w projekcie (np. okres urlopowy lub zwolnienia lekarskie personelu, konsultacje prawne), dlatego nie były uzasadniane*.

**Zapewnienie pracowników posiadających niezbędne kompetencje**

Osoby pełniące funkcje Kierownika Projektu, Kierownika Biznesowego Projektu oraz Lidera merytorycznego Projektu posiadały kwalifikacje adekwatne do wykonywanych zadań. Pracownicy, do których zadań należała ocena wniosków o przyznanie grantu pod względem merytorycznym (tj. 25 spośród 121 osób zaangażowanych w realizację Projektu), posiadali wykształcenie i doświadczenie zawodowe w zakresie cyberbezpieczeństwa, co potwierdziła analiza wybranych dokumentów zgromadzonych w aktach osobowych 10 spośród nich.

**Fluktuacja kadr w NASK**

Według stanu na 26 sierpnia 2025 r. w trakcie Projektu udział w nim zakończyło 15 pracowników, natomiast 14 osób dołączyło do jego realizacji. Rotacja pracowników nie wpłynęła na przebieg prac i nie spowodowała konieczności dokonywania zmian w harmonogramie Projektu. Dyrektor NASK wyjaśnił, że *nie zidentyfikowano nadmiarowej rotacji pracowników dla poszczególnych ról w projekcie. W ramach realizacji zadań NASK podejmuje działania utrzymywania zespołu (...) dla projektu zarówno pod kątem ich stałości osobowej, jak i liczbowej.*

**Organizacja przez NASK naboru wniosków o przyznanie grantu**

NASK, zgodnie z § 5 ust. 7 pkt 1 umowy o partnerstwie, zorganizował i zrealizował nabór wniosków o przyznanie grantu. Nabór odbywał się według Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd”[33] z wykorzystaniem narzędzia informatycznego LSI, za pomocą którego wnioskodawcy składali wnioski o przyznanie grantu. Wnioski te podlegały ocenie formalnej, a następnie ocenie merytorycznej przez ekspertów. Ostatecznie wnioski były zatwierdzane przez Komisję Przyznającą Granty[34].

Dyrektor NASK wskazał, że w ramach konkursu został zaplanowany jeden nabór oraz wyjaśnił, że *za opracowanie ram czasowych oraz wszelkich zmian odpowiedzialny był Beneficjent[35]. NASK realizował prace w ramach naboru zgodnie z podpisaną umową Partnerską w oparciu o harmonogram dostępny w Regulaminie konkursu grantowego. Nabór pierwotny realizowany był w okresie od 19.07.2023 do 30.09.2023 roku. Decyzją Beneficjenta z dnia 11.08.2023 roku nabór został wydłużony do 13.10.2023 roku. Następnie*

[33] Dalej: Regulamin Konkursu.

[34] Powołaną decyzją Dyrektora Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego z dnia 13.11.2023 r. w sprawie powołania Komisji Przyznającej Granty dla projektu Cyberbezpieczny Samorząd realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027. Priorytet II – Zaawansowane usługi cyfrowe, Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa.

[35] Tj. CPPC.

*decyzją z dnia 06.10.2023 roku nabór został wydłużony do 30.11.2023 roku. Ostatecznie decyzją z dnia 20.11.2023 roku nabór został wydłużony do 14.12.2023 roku.*

**Wsparcie NASK podczas naboru wniosków o przyznanie grantu**

NASK, zgodnie z § 5 ust. 7 pkt 2 umowy o partnerstwie, zapewnił wparcie dla wnioskodawców (jednostek samorządu terytorialnego) podczas naboru wniosków. Wsparcie to jest również kontynuowane podczas realizacji Projektu i odbywa się poprzez:

- infolinię[36] dostępną w godzinach 8.00–16.00,
- utworzoną dla Projektu skrzynkę poczty elektronicznej, za pomocą której NASK odpowiada na pytania od grantobiorców[37],
- opracowywanie zamieszczanego na stronie internetowej Projektu dokumentu *Pytania i odpowiedzi (Q&A)*, który był aktualizowany wraz z rozwojem Projektu,
- organizowanie webinariów dla grantobiorców.

W wyniku oględzin skrzynki poczty elektronicznej cyberbezpiecznysamorzad@nask.pl[38], podczas których na próbie 10 wiadomości mailowych przesłanych przez grantobiorców zbadano terminowość udzielania przez NASK odpowiedzi, ustalono, że w przypadku większości z nich odpowiedź była udzielana tego samego dnia, którego przesłano zapytanie, a najpóźniej odpowiedzi udzielono po 13 dniach.

**Prawidłowość weryfikacji przez NASK wniosków o przyznanie grantu**

Szczegółowym badaniem objęto 15 grantów, w przypadku których grantobiorcy złożyli końcowe wnioski o rozliczenie grantu, a wnioski te zostały zweryfikowane i zatwierdzone przez NASK[39]. W wyniku badania ustalono, że wnioski o przyznanie grantu spełniały kryteria formalne i merytoryczne określone w Regulaminie Konkursu. NASK po przeprowadzeniu oceny formalnej i merytorycznej wniosków opracowywał zestawienie wniosków zatwierdzonych do dofinansowania i przekazywał informacje o wynikach oceny do wnioskodawców. Następnie NASK gromadził dokumentację do zawarcia umów grantowych i przekazywał przygotowane umowy do CPPC celem ich podpisania.

**Nierzetelna weryfikacja przez NASK wniosków o rozliczenie grantu**

Stwierdzono, że w przypadku części objętych badaniem wniosków o rozliczenie grantu ich weryfikacja była przeprowadzona w NASK nierzetelnie, pomimo ustanowienia 23 maja 2025 r.[40] wewnętrznej procedury (*Procedura weryfikacji wniosku rozliczającego zaliczkę (grant)* – dalej: Procedura weryfikacji).

---

[36] Od 19 lipca 2023 r. do 22 maja 2025 r. odebrano 13 683 połączenia telefoniczne.

[37] Od 19 lipca 2023 r. do 22 lipca 2025 r. odebrano 21 096 wiadomości mailowych i odpowiedziano na 19 541 z nich (różnica wynika z faktu, iż część przesłanych wiadomości nie wymagała odpowiedzi).

[38] Służącej do udzielania odpowiedzi na pytania wysyłane przez grantobiorców na adres cyberbezpiecznysamorzad@cppc.gov.pl, z którego wszystkie wiadomości są przekierowywane na adres cyberbezpiecznysamorzad@nask.pl.

[39] Na 8 czerwca 2025 r. złożonych zostało 18 wniosków o rozliczenie grantu (w ramach 2494 zawartych umów o powierzenie grantu), z których 12 zostało do tego dnia zweryfikowanych i zatwierdzonych przez NASK. Do badania dobrano kolejne trzy wnioski, które zostały zweryfikowane i zatwierdzone w trakcie kontroli.

[40] Zgodnie z pkt 10 tej Procedury zasady określone m.in. w jej pkt 4b – „Wypełnianie listy sprawdzającej" obowiązują również dla wniosków złożonych przed dniem jej podpisania.

NASK nierzetelnie zweryfikował 13 z 15 badanych wniosków o rozliczenie grantu złożonych przez jednostki samorządu terytorialnego[41] i zatwierdził je, pomimo tego, że były sporządzone wadliwie lub nie zawierały wszystkich wymaganych załączników. W szczególności:

1. Ustalono, że zatwierdzono wniosek o rozliczenie grantu złożony przez Gminę Haczów[42], w którym wsparcie otrzymały m.in.: Gminny Ośrodek Kultury i Wypoczynku w Haczowie oraz Gminna Biblioteka Publiczna w Haczowie[43], będące samorządowymi instytucjami kultury posiadającymi osobowość prawną, pomimo, że jak wskazano w § 3 ust. 1 zdanie drugie Regulaminu Konkursu: *Celem Projektu grantowego jest wsparcie jst w zakresie realizacji usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji jednostek samorządu terytorialnego wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia) w kontekście zwiększenia poziomu cyberbezpieczeństwa*.

   W toku realizacji Projektu CPPC, realizując obowiązek określony w § 7 ust. 2 Regulaminu Konkursu, publikowało na stronie internetowej Projektu odpowiedzi na najczęstsze pytania dotyczące konkursu grantowego. W kilku udzielonych tam odpowiedziach wskazano, że użyty w Regulaminie Konkursu zwrot *jednostki podległe (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia)* oznacza *jednostki nieposiadające własnej osobowości prawnej, za których zobowiązania odpowiada jednostka samorządu terytorialnego*.

   Dyrektor NASK wyjaśnił, że *weryfikacja wniosku rozliczającego odbywa się w oparciu o Procedurę nr 4, a w tej nie uwzględniono zagadnienia weryfikacji statusu prawnego jednostek podległych (...) założono, że zagadnienie kwalifikowalności wnioskodawców zostało wystarczająco rozstrzygnięte na etapie oceny formalnej i jst nie będą udzielały wsparcia podmiotom innym niż wymienione w zweryfikowanym przed zawarciem umowy grantowej wniosku. Przykład gminy Haczów pokazuje, że to założenie było błędne i oczywiście omawiana Procedura zostanie skorygowana w przedmiotowym zakresie. Dalsze postępowanie musi zostać ustalone z CPPC, ponieważ umowa o powierzenie grantu nie rozstrzyga jednoznacznie czy taka zmiana była dozwolona bez wcześniejszej autoryzacji/powiadomienia CPPC. 7 sierpnia rozpoczęliśmy pracę nad kolejną procedurą kompleksowo obejmującą zagadnienie zmian w projektach grantowych*.

2. Do wniosków o rozliczenie grantu złożonych w przypadku czterech projektów, nie zostały załączone raporty z przeprowadzonego audytu wdrożonego systemu zarządzania bezpieczeństwem informacji[44],

---

41 FERC.02.02-CS.01-001/23/0130, FERC.02.02-CS.01-001/23/0182, FERC.02.02-CS.01-001/23/0234, FERC.02.02-CS.01-001/23/0245, FERC.02.02-CS.01-001/23/0280, FERC.02.02-CS.01-001/23/0333, FERC.02.02-CS.01-001/23/0384, FERC.02.02-CS.01-001/23/0565, FERC.02.02-CS.01-001/23/0644, FERC.02.02-CS.01-001/23/0686, FERC.02.02-CS.01-001/23/1590, FERC.02.02-CS.01-001/23/1807 oraz FERC.02.02-CS.01-001/23/2015.

42 FERC.02.02-CS.01-001/23/0182.

43 We wniosku o przyznanie grantu złożonym przez gminę Haczów nie została wskazana żadna jednostka podległa. Zostały one wskazane dopiero we wniosku o rozliczenie grantu.

44 FERC.02.02-CS.01-001/23/0182 (do wniosku załączono jedynie niepodpisany raport testu penetracyjnego i nie załączono raportów z audytu w jednostkach podległych uwzględnionych w projekcie), FERC.02.02-CS.01-001/23/0565, FERC.02.02-CS.01-001/23/0644 i FERC.02.02-CS.01-001/23/2015.

a w przypadku dwóch projektów[45] załączone raporty nie zostały podpisane przez sporządzającego je audytora. Pomimo tego wnioski te zostały przez NASK zatwierdzone[46].

Zgodnie z § 3 ust. 3 Regulaminu Konkursu grantobiorca był zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji i przekazania podpisanego przez audytora raportu z tego audytu jako załącznika do wniosku o rozliczenie grantu.

Zastępca Dyrektora NASK wyjaśnił, że *do czasu wprowadzenia Procedury weryfikacji wniosku rozliczającego zaliczkę (grant) eksperci weryfikowali kompletność dokumentacji na podstawie umowy grantowej. Zapisy umowy nie zawierają bezpośrednio wymogu dostarczenia raportu z audytu KRI, a ten wymóg został zdefiniowany w Regulaminie Konkursu Grantowego. 21 lipca pracownicy merytoryczni dokonali przeglądu złożonych raportów z audytu KRI, po czym wysłano wezwania do Grantobiorców.* Następnie Dyrektor NASK poinformował, że trzech grantobiorców dosłało brakujące raporty[47].

NIK zauważa, że wysłanie wezwań do grantobiorców powinno odbyć się na etapie weryfikacji wniosków o rozliczenie grantu, a nie po ich zatwierdzeniu.

3. Do wniosku o rozliczenie grantu w jednym z badanych projektów[48] nie zostały załączone potwierdzenia przelewów za zakupy udokumentowane dwiema fakturami VAT[49].

   Zgodnie z § 3 ust. 2 pkt 3 umowy o powierzenie grantu zawartej w tym projekcie: *Zakończenie realizacji Projektu obejmuje m.in.: przekazanie dokumentacji finansowej potwierdzającej poniesienie wydatku (w tym kopii faktur lub równoważnych dowodów księgowych wraz z potwierdzeniem dowodów zapłaty)*.

   Zastępca Dyrektora NASK wyjaśnił, że *przedmiotowa omyłka nie rodzi skutków finansowych. Grantobiorca został wezwany do uzupełnienia wniosku w powyższym zakresie,* a także przekazał brakujące potwierdzenia przelewów, które w odpowiedzi na to wezwanie dostarczył do NASK grantobiorca.

   Zdaniem NIK przed zatwierdzeniem wniosku o rozliczenie grantu NASK powinien wezwać grantobiorcę do korekty stwierdzonych błędów.

---

45 FERC.02.02-CS.01-001/23/0686 i FERC.02.02-CS.01-001/23/1590.

46 Według ppkt 4 (dot. lit. k) Weryfikacji formalnej w pkt 4b Procedury weryfikacji przy wypełnianiu listy sprawdzającej na pytanie „Czy złożono wszystkie niezbędne załączniki do wniosku?" należało w tym przypadku udzielić odpowiedzi „NIE", co uniemożliwiało zatwierdzenie wniosku o rozliczenie grantu.

47 Dla projektów: FERC.02.02-CS.01-001/23/0565, FERC.02.02-CS.01-001/23/0644 i FERC.02.02-CS.01-001/23/2015.

48 FERC.02.02-CS.01-001/23/0245.

49 Tj. nr FS/1691/11/2023 z 30.11.2023 r. na kwotę 10 947,00 zł brutto i FAS/139/2024 z 17.04.2024 r. na kwotę 9616,13 zł brutto. Według ppkt 4 (dot. lit. e) Weryfikacji formalnej w pkt 4b Procedury weryfikacji na pytanie „Czy złożono wszystkie niezbędne załączniki do wniosku?" należało również w tym przypadku udzielić odpowiedzi „NIE", co uniemożliwiało zatwierdzenie wniosku o rozliczenie grantu.

4. W przypadku dwóch projektów[50] grantobiorcy nie załączyli do wniosków o rozliczenie grantu ani umowy, ani porozumienia, ani żadnego innego dokumentu potwierdzającego wzajemne zobowiązania stron, związanego z realizacją dostaw lub usług, natomiast w przypadku dwóch innych projektów załączyli je, ale były one niekompletne[51].

   W Procedurze weryfikacji ustalono, że ekspert weryfikujący wniosek o rozliczenie grantu powinien m.in. sprawdzić, czy dokumenty te zostały załączone do wniosku[52].

   Zastępca Dyrektora NASK poinformował, że grantobiorcy dosłali w dniach 28–29 lipca 2025 r. przedmiotową dokumentację.

5. W Procedurze weryfikacji ustalono, że ekspert weryfikujący wniosek o rozliczenie grantu powinien m.in. zweryfikować, czy poprawnie wskazano wartość wskaźników osiągniętą w okresie sprawozdawczym i udzielić odpowiedzi „NIE”[53], jeżeli m.in.:

   a) wartość bazowa wskaźników jest różna od „0” (z wyłączeniem wskaźnika „Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych”, o ile w projekcie jest modernizowana istniejąca usługa)[54].

   W siedmiu projektach[55] na to pytanie udzielono odpowiedzi „TAK” (i w konsekwencji zatwierdzono wnioski o rozliczenie grantu), pomimo tego, że grantobiorcy podali wartości przedmiotowych wskaźników inne niż „0”.

   Zastępca Dyrektora NASK wyjaśnił, że *błędnie wypełnione przez Grantobiorcę pole „wartość bazowa” nie niesie za sobą skutków finansowych, w tym nie stanowi podstawy do uznania wydatków za niekwalifikowalne.*

   Zdaniem NIK przed zatwierdzeniem wniosku o rozliczenie grantu NASK powinien wezwać grantobiorcę do korekty stwierdzonych błędów, nawet jeśli nie rodzą one skutków finansowych,

   b) wartość osiągnięta wskaźnika „Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach jst” nie jest równa liczbie podmiotów wynikającej z zestawienia przygotowanego przez Zespół projektowy[56].

---

50 FERC.02.02-CS.01-001/23/1807 oraz FERC.02.02-CS.01-001/23/2015.

51 W przypadku projektu FERC.02.02-CS.01-001/23/0245 grantobiorca nie przekazał kompletnej umowy nr RO.272.8.71.2024.AP (brakowało załącznika nr 2, zawierającego szczegółowy opis przedmiotu zamówienia), a w przypadku projektu FERC.02.02-CS.01-001/23/0384 grantobiorca przekazał jedynie niekompletny projekt (niepodpisany) umowy nr EPAS.272.004.2024.

52 Ppkt 4 lit. c Weryfikacji formalnej w pkt 4b Procedury weryfikacji.

53 Przy wypełnianiu listy sprawdzającej, co w konsekwencji uniemożliwiało zatwierdzenie wniosku o rozliczenie grantu.

54 Ppkt 5 Weryfikacji merytorycznej (Warunek 4 i 4’) w pkt 4b Procedury weryfikacji.

55 FERC.02.02-CS.01-001/23/0182, FERC.02.02-CS.01-001/23/0234, FERC.02.02-CS.01-001/23/0245, FERC.02.02-CS.01-001/23/0280, FERC.02.02-CS.01-001/23/0333, FERC.02.02-CS.01-001/23/0686 i FERC.02.02-CS.01-001/23/2015.

56 Ppkt 5 Weryfikacji merytorycznej (Warunek 3 i 3’) w pkt 4b Procedury weryfikacji. Z tego zestawienia wynikało, że w projekcie FERC.02.02-CS.01-001/23/0130 nie planowano wsparcia jednostek podległych, a zatem przedmiotowy wskaźnik powinien wynieść 1.

W projekcie FERC.02.02-CS.01-001/23/0130 na to pytanie udzielono odpowiedzi „TAK" i wniosek o rozliczenie grantu został zatwierdzony, pomimo tego, iż grantobiorca podał, że wartość osiągnięta tego wskaźnika wyniosła 0 (co znaczyłoby, że projekt nie został w ogóle zrealizowany, gdyż wsparcia nie uzyskał żaden podmiot).

Zastępca Dyrektora NASK wyjaśnił, że *podniesione zagadnienie ma charakter jednostkowego błędu ludzkiego.*

**Dokumentacja Projektu nie przewidywała oceny poziomu cyberbezpieczeństwa w jst na etapie składania wniosków o dofinansowanie grantu**

Zgodnie z § 4 ust. 1 pkt 4 zawieranych w ramach Projektu umów o powierzenie grantu grantobiorcy mieli obowiązek przekazania do NASK uzupełnionej *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych)*[57] – po raz pierwszy w terminie 30 dni od dnia zawarcia umowy o powierzenie grantu (pod rygorem wstrzymania wypłaty dofinansowania lub jego części) oraz po raz drugi jako obligatoryjnego załącznika do wniosku o rozliczenie grantu.

Zastępca Dyrektora NASK wyjaśnił, że ankiety złożone w terminie 30 dni od dnia podpisania umowy o powierzenie grantu *nie były weryfikowane merytorycznie, natomiast były przez NASK walidowane pod kątem ich poprawnego wypełnienia oraz że informacje zawarte w Ankiecie nie były porównywane z treścią wniosków o grant*. Natomiast w odniesieniu do ankiet składanych przez grantobiorców jako załącznik do wniosku o rozliczenie grantu Zastępca Dyrektora NASK wyjaśnił, że *są walidowane, pod kątem ich technicznej poprawności* i *zostaną one poddane analizie statystycznej po wpłynięciu wszystkich wniosków rozliczających granty.*

Oświadczył on również, iż *Biorąc pod uwagę dotychczasowe doświadczenie w realizacji projektu Cyberbezpieczny Samorząd, przedmiotowa Ankieta może być wykorzystana do oceny pojedynczego grantobiorcy, jednak trzeba mieć na uwadze, iż tworzona jest ona na bazie samooceny. Ankieta dotyczy wielu działań dotyczących zestawu zagadnień z różnych obszarów cyberbezpieczeństwa. Z kolei zakres zadań grantobiorcy realizowanych z grantu zasadniczo stanowił wycinek tego co obejmowała ankieta.* Według Zastępcy Dyrektora NASK *Ankiet nie weryfikowano pod kątem merytorycznym, ponieważ weryfikacja merytoryczna pojedynczych Ankiet nie mogła mieć wpływu na ocenę wniosków o udzielenie grantu (...) Treść merytoryczna Ankiet nie jest też i nie będzie podstawą oceny wniosków rozliczających Grantobiorców. Podstawą oceny wniosku rozliczającego Grantobiorcy jest zgodność poniesionych wydatków z umową o powierzenie grantu, w tym z wnioskiem o przyznanie grantu (...) ankiety to narzędzie ułatwiające określenie aktualnej pozycji na ścieżce rozwoju jst oraz stanu docelowego jaki jednostka zamierza osiągnąć przy wsparciu z projektu. Ankiety to przede wszystkim szerokie statystyczne badanie sektora jst w zakresie cyberbezpieczeństwa.*

[57] Wzór ankiety został określony w załączniku nr 6 do Regulaminu Konkursu.

**Przeprowadzenie audytów KRI na zakończenie grantu nie miało na celu oceny podniesienia poziomu odporności na cyberzagrożenia w związku z realizacją**

Zgodnie z § 3 ust. 3 Regulaminu Konkursu grantobiorcy mieli obowiązek *przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI*[58] oraz zgodnie z określonymi w Regulaminie Konkursu warunkami[59], a także dostarczyć raport z tego audytu do NASK wraz z wnioskiem o rozliczenie grantu[60]. W dokumentacji konkursowej, za której przygotowanie odpowiadało CPPC[61], audyty nie zostały w żaden inny sposób ustandaryzowane, w szczególności nie sformułowano w niej obowiązku zamieszczenia w raportach z tych audytów oceny podniesienia poziomu odporności na cyberzagrożenia w związku z realizacją Projektu.

Zastępca Dyrektora NASK wyjaśnił, że *Przeprowadzenie audytów KRI u Grantobiorców nie miało na celu oceny podniesienia poziomu odporności na cyberzagrożenia w związku z realizacją projektu Cyberbezpieczny Samorząd (...) Grantodawca*[62] *wymagał jedynie załączenia raportu z audytu KRI wykonanego na zakończenie realizacji grantu*.

Zastępca Dyrektora NASK oświadczył także, że *Grantodawca nie zmienił zakresu audytu KRI (poprzez jego zwiększenie) oraz nie wpływał na treść raportu z audytu poza zapisami wskazanymi w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd", w którym zawęził krąg osób uprawnionych do jego przeprowadzenia (wydatek kwalifikowalny). Grantodawca nie wymagał od Grantobiorcy przeprowadzenia audytu grantu, który miałby określić/potwierdzić podniesienie poziomu cyberbezpieczeństwa przez Grantobiorcę w związku z realizacją grantu (...) Grantodawca wymagał jedynie załączenia jednego raportu z audytu KRI (ew. audytu wg. ISO/IEC 27001) wykonanego na zakończenie realizacji grantu. Tym samym Grantodawca nie planował, na podstawie raportów z audytu, oceniać podniesienie poziomu odporności poszczególnych Grantobiorców na cyberzagrożenia w związku z realizacją projektu Cyberbezpieczny Samorząd.*

Zdaniem Zastępcy Dyrektora NASK *poszerzenie zakresu audytu KRI (przewidzianego prawem) wydaje się możliwe, jednak nie byłoby optymalne*.

Według Zastępcy Dyrektora NASK *Raport z audytu KRI (oprócz wypełnienia obowiązku prawnego) należy traktować jako jeden z elementów budowania cyberbezpieczeństwa, a w szczególności uzyskania świadomości po stronie audytowanego w zakresie aktualnego stanu i kierunku działań.*

**Monitorowanie przez NASK przebiegu realizacji prac**

Dyrektor NASK wyjaśnił, że *nie został opracowany dedykowany dokument opisujący procedury monitoringu wykonania Umowy o partnerstwie*.

W toku kontroli ustalono, że w NASK bieżący monitoring wykonania umowy o partnerstwie odbywał się m.in. poprzez cotygodniowe wewnętrzne spotkania członków Zespołu projektowego, cotygodniowe

---

58 Obowiązującego do 22 maja 2024 r. Odpowiednio § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

59 M.in. zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie jst miał obejmować zgodność z kryteriami zawartymi w § 20 ust. 2 rozporządzenia KRI z 2012 r. lub zgodność z wymaganiami normy PN-ISO/IEC 27001 (§ 3 ust. 3 pkt 1 Regulaminu Konkursu).

60 Zgodnie z § 4 ust. 10 Regulaminu Konkursu.

61 Zgodnie z § 4 ust. 4 pkt 9 umowy o partnerstwie.

62 Tj. CPPC.

spotkania z CPPC oraz spotkania w cyklach dwutygodniowych z przedstawicielami CPPC, Ministerstwa Cyfryzacji oraz Ministerstwa Funduszy i Polityki Regionalnej. Ze spotkań tych NASK sporządzało notatki. Do CPPC, a następnie do przedstawicieli Ministerstwa Cyfryzacji, co tydzień wysyłano również wiadomości mailowe, zawierające informacje o aktualnym stanie realizacji Projektu.

W NASK przyjęto również *Procedurę weryfikacji wniosku sprawozdawczego*[63], do składania którego zobowiązani byli grantobiorcy i w którym m.in. informowali oni o postępie rzeczowym w realizacji umowy o powierzenie grantu zawartej w ramach Projektu. Zgodnie z § 7 ust. 2 umowy o powierzenie grantu wniosek ten powinien być przekazany w terminie 30 dni następujących po upływie 12 miesięcy od podpisania umowy przy wykorzystaniu transzy pierwszej oraz w terminie 30 dni następujących po upływie 18 miesięcy od dnia podpisania umowy przy wykorzystaniu transzy drugiej.

Ponadto ustalono, że w NASK prowadzony był rejestr ryzyk występujących w Projekcie, który był na bieżąco aktualizowany. Zastępca Dyrektora NASK wskazał, że *obecnie najistotniejszym ryzykiem jest czas przeznaczony na weryfikację wniosków rozliczających w spodziewanym piku w okresie grudzień 2025 oraz maj–lipiec 2026. W celu minimalizacji ryzyka realizacji zadania w określonym w umowie czasie, zaplanowano zwiększenie liczby osób odpowiedzialnych za realizację zadania w tych okresach. Dodatkowo została przygotowana szczegółowa procedura oraz nagrania ze szkoleń dla poszczególnych członków zespołu.*

Zastępca Dyrektora NASK odnośnie informowania CPPC o występujących w realizacji Projektu ryzykach i zagrożeniach wskazał, że *informacje przekazywane są Partnerowi Wiodącemu systematycznie na cotygodniowych spotkaniach statusowych, co znajduje swoje odzwierciedlenie w notatkach. Najważniejsze zagadnienia wymagające wiążących decyzji po stronie Partnera Wiodącego kierowane są drogą pisemną (email, pismo drogą ePuap).*

**Kontrole realizacji umów o powierzenie grantów**

Dotychczas nie były przeprowadzone kontrole wynikające z umów o powierzenie grantu. Rozpoczęcie tych kontroli planowane jest w III kwartale 2025 r. W przygotowanej w NASK *Procedurze kontroli grantów* założono, że kontrole w formule zdalnej, na miejscu u grantobiorcy lub hybrydowej, przeprowadzane przez Zespoły Kontrolujące, składające się co najmniej z dwóch osób, obejmą co najmniej 5% wszystkich grantobiorców[64]. Kontrole mają stanowić pogłębioną weryfikację dokumentów w stosunku do weryfikacji prowadzonej na etapie zatwierdzania wniosków o rozliczenie grantu, a ich celem ma być potwierdzenie legalności, celowości, prawidłowości i kwalifikowalności poniesionych wydatków.

[63] Dokument podpisano 23 maja 2025 r.
[64] W tym co najmniej: 1 województwo i 10 powiatów.

## 5.3. Realizacja przez gminy i powiaty działań w ramach projektu „Cyberbezpieczny Samorząd” w celu zwiększenia poziomu cyberbezpieczeństwa

**W jst podejmowano działania dla zwiększenia poziomu cyberbezpieczeństwa, jednak nie zawsze były one wystarczające**

Kontrolowane urzędy w latach 2023–2025 podejmowały działania w celu zwiększenia poziomu cyberbezpieczeństwa, w ramach projektu „Cyberbezpieczny Samorząd”, lecz nie w każdym urzędzie były one skuteczne. W 16 z 17 kontrolowanych jst rozpoznano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, m.in. dokonano analizy stanu zabezpieczeń infrastruktury informatycznej funkcjonującej w urzędach. Łączna wartość przyznanych kontrolowanym urzędom grantów wyniosła 13 105 379,30 zł, a wartość wydatkowana wyniosła 7 741 308,49 zł (z uwzględnieniem wkładu własnego w łącznej kwocie 932 653,00 zł), co stanowiło 59% środków wydatkowanych na realizację projektów grantowych, przy czym zakończenie realizacji i rozliczenie projektów grantowych ma nastąpić do 30 czerwca 2026 r. Zakupione w ramach projektów grantowych urządzenia i oprogramowanie zostały zainstalowane i były użytkowane przez kontrolowane urzędy oraz jednostki organizacyjne lub były na etapie wdrożenia. W związku z uczestnictwem w Projekcie, we wszystkich kontrolowanych jst opracowano Ankiety dojrzałości dla urzędów oraz jednostek podległych biorących udział w Projekcie, jednak w przypadku 23% kontrolowanych jst nie były one sporządzane rzetelnie.

W ponad połowie kontrolowanych urzędów nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, który jest kluczowym elementem zapewnienia cyberbezpieczeństwa. Ponadto, w ośmiu urzędach (47 %) w 2023 r. lub 2024 r. nie przeprowadzono obowiązkowego audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI[65] lub audyt przeprowadzono nierzetelnie, bądź z naruszeniem zasady niezależności i obiektywizmu audytu. W dokumentach strategicznych większości kontrolowanych urzędów (16 spośród 17, tj. 94%) nie uwzględniono zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa, co tłumaczono najczęściej małą istotnością tego zagadnienia w momencie opracowywania strategii, tj. w latach 2014–2020, a także brakiem prowadzenia analiz w tym zakresie oraz brakiem wymogów prawnych. W ocenie NIK wskazuje to na brak systemowego podejścia do kwestii cyberbezpieczeństwa w urzędach jst.

Nieprawidłowości w realizacji grantów stwierdzono w pięciu z 17 kontrolowanych urzędów (29%). Nie miały one jednak zasadniczego wpływu na prawidłowość wykorzystania grantu (poza UG Świerklany, gdzie NIK sformułowała ocenę negatywną). Kontrola wykazała, że zdefiniowane przez CPPC wskaźniki realizacji projektów grantowych, tak produktu, jak i rezultatu, nie były w żaden sposób powiązane z faktycznym wzrostem poziomu cyberbezpieczeństwa u grantobiorców (JST), a jedynie z liczbą dokonanych zakupów i przeszkolonych osób.

[65] Obowiązującego do 22 maja 2024 r. Odpowiednio § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

**W dokumentach strategicznych urzędów jst nie zostały uwzględnione zagadnienia dotyczące zwiększenia poziomu cyberbezpieczeństwa**

W dokumentach strategicznych większości kontrolowanych urzędów[66] (16 spośród 17, tj. 94%) nie uwzględniono zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa. Tłumaczono to najczęściej małą istotnością tego zagadnienia w momencie opracowywania strategii, tj. w latach 2014–2020, a także brakiem prowadzenia analiz w tym zakresie. W kontrolowanych jst podawano również, że prowadzone analizy w ówczesnych uwarunkowaniach społeczno-gospodarczych szczególny nacisk kładły na poprawę dostępności cyfrowej administracji. Tylko w jednym urzędzie (Urząd Gminy w Wilkowicach) uwzględniono zagadnienia w zakresie wzrostu poziomu cyberbezpieczeństwa.

**Przykład**

W *Strategii Rozwoju* ***Gminy Wilkowice*** *do roku 2030 pn. „Gmina Wilkowice 2030"* w ramach celu operacyjnego *Odpowiedzialne zarządzania* (4.3.) uwzględniono zagadnienia dotyczące zwiększenia poziomu bezpieczeństwa.

W Strategii w zakresie celu operacyjnego „Odpowiedzialne zarządzanie" wskazano kierunki, oczekiwane rezultaty, wskaźniki oceny osiągnięcia rezultatów, oczekiwane trendy, podmioty odpowiedzialne (urząd) i zaangażowane i tak, poszczególnym kierunkom działań związanych z cyberbezpieczeństwem przypisano następujące wskaźniki:

- Wzrost poziomu dostępności do usług publicznych oraz rozwój usług publicznych, w tym usług elektronicznych, Zwiększenie dostępności do usług publicznych (oczekiwane rezultaty), którym przypisano wskaźnik „Liczba oferowanych e-usług";
- Podnoszenie kompetencji pracowników samorządowych, Wzrost wykwalifikowania kadry pracowniczej i zarządczej (oczekiwane rezultaty), którym przypisano wskaźnik „Liczba osobodni szkole";
- Monitorowanie jakości usług publicznych, Poznanie ocen i opinii mieszkańców na temat dostępnych, Poznanie ocen i opinii mieszkańców na temat dostępnych usług publicznych, Ewaluacja systemu świadczeń usług publicznych; którym przypisano wskaźniki „Poziom zadowolenia mieszkańców z pracy urzędu".

**W urzędach jst rozpoznawano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa**

W okresie objętym kontrolą w 16 urzędach jst (94 %) rozpoznawano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, m.in. dokonywano analizy stanu zabezpieczeń infrastruktury informatycznej funkcjonującej w urzędach, przeprowadzano testy cyberbezpieczeństwa, którego celem było zidentyfikowanie luk w zabezpieczeniach systemów informatycznych oraz ocena zachowania pracowników.

**Przykład**

W **Starostwie Powiatowym w Gliwicach** w kwestii określania potrzeb dotyczących zwiększenia poziomu cyberbezpieczeństwa, starosta gliwicki podał m.in.: *Powiat Gliwicki nie posiada sformalizowanego planu realizacji zadań z zakresu cyberbezpieczeństwa,* dodał natomiast, że: *Potrzeby sprzętowe oraz związane z zakupem oprogramowania, w tym oprogramowania do zapewnienia cyberbezpieczeństwa, dla Starostwa*

[66] Dotyczy to Starostw Powiatowych w: Białobrzegach, Gliwicach, Legionowie, Kamiennej Górze, Ostrowcu Świętokrzyskim oraz UM/UMiG/UG: Brody, w Bystrzycy Kłodzkiej, w Chęcinach, w Chmielniku, Dąbrowa Zielona, w Górze, Kłodzko, Lelis, Nowe Miasto nad Pilicą, Serock i Świerklany.

*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.*

Tylko w jednym urzędzie (UMiG w Chęcinach) nie rozpoznawano potrzeb w powyższym zakresie. Uniemożliwiało to planowanie, podejmowanie i monitorowanie skutecznych działań w zakresie cyberbezpieczeństwa.

**Ankiety dojrzałości cyberbezpieczeństwa**

W związku z uczestnictwem w Projekcie, we wszystkich kontrolowanych jst opracowano Ankiety dojrzałości, dla urzędów oraz jednostek podległych biorących udział w Projekcie. Zostały one przekazane do NASK za pośrednictwem skrzynki ePUAP w terminie 30 dni od zawarcia umowy o powierzenie grantu oraz jako załącznik do wniosku rozliczającego, zgodnie z § 4 ust. 1 pkt 4 umowy grantowej. W przypadku czterech jst[67] (23%) ankiety zostały opracowane nierzetelnie.

**Przykłady**

W Ankiecie dojrzałości cyberbezpieczeństwa przekazanej przez **Starostwo Powiatowe w Białobrzegach** do NASK 24 lipca 2024 r. podano informacje, które były niezgodne ze stanem faktycznym ustalonym w trakcie kontroli, co było działaniem nierzetelnym. W ww. ankiecie niezgodnie ze stanem faktycznym podano, że:

- kierownik jst wydał zarządzenie o zintegrowanym Systemie Zarządzania Bezpieczeństwa Informacji w jednostce,
- kierownik jst opublikował Politykę Bezpieczeństwa Informacji (PBI) z uwzględnieniem cyberbezpieczeństwa,
- konieczność zapewnienia bezpieczeństwa informacji jest ujęta w strategii informatyzacji Jednostki,
- jednostka opracowała i przyjęła kompleksową Politykę Bezpieczeństwa Informacji (PBI),
- PBI Jednostki jest opracowane w oparciu o właściwe standardy i dobre praktyki,
- Polityka Bezpieczeństwa Informacji w Jednostce jest ogólnie dostępna dla pracowników, a zmiany w niej są im komunikowane w toku okresowych szkoleń stanowiskowych.

Starosta wyjaśnił, że *Dokumentami określającymi Politykę Bezpieczeństwa Informacji oraz system Zarządzania Bezpieczeństwem Informatycznym jest Polityka Ochrony Danych Osobowych oraz Procedura zarządzania incydentami cyberbezpieczeństwa w Starostwie Powiatowym w Białobrzegach.* Wskazał także, że *Omyłkowo zostało zaznaczone znakiem X potwierdzenie posiadania w/w strategii.*

[67] Dotyczy to Starostwa Powiatowego w Białobrzegach oraz UMiG Serock i UG: Lelis i Świerklany.

W Ankietach dojrzałości przekazanych do NASK przez **UMiG Serock** po zawarciu umowy oraz z wnioskiem rozliczającym przedstawiono informacje o obecnym i planowanym w ramach Projektu stanie poszczególnych działań wymienionych we wzorze Ankiety dojrzałości, stanowiącym załącznik nr 6 do Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd". Ustalono, że w przypadku sześciu działań opis stanu obecnego lub planowanego był nierzetelny.
W planowanym zakresie zmian wskazano m.in. opracowanie i wdrożenie SZBI, segmentację sieci i uwierzytelnianie wieloskładnikowe. Kontrola NIK ustaliła, że we wniosku o dofinansowanie stanowiącym załącznik do umowy grantowej, działania we wskazanym zakresie nie były planowane do realizacji w ramach Projektu. Sekretarz wyjaśnił, że *w ankiecie dojrzałości omyłkowo wskazano planowane działania w ramach projektu. Działania zaplanowano do wykonania we własnym zakresie.* Ponadto, w Ankietach dojrzałości wykazano, że Polityka Bezpieczeństwa Informacji (PBI) została opublikowana i jest ogólnie dostępna dla pracowników, a przeglądu dokumentu dokonano nie dawniej niż rok temu.
W toku kontroli ustalono, że w Urzędzie nie została wdrożona PBI. Sekretarz wyjaśnił, że opracowana polityka ochrony danych osobowych szeroko i szczegółowo odnosi się do bezpieczeństwa informacji i danych, nie tylko osobowych.
Zdaniem NIK, obowiązująca w Urzędzie Polityka ochrony danych osobowych nie może być uznana jako tożsama z Polityką Bezpieczeństwa Informacji wynikającą z pkt 5.2 Polskiej Normy PN-ISO/IEC 27001, w myśl przepisu §19 ust. 1, w związku z ust. 3 rozporządzenia KRI, gdyż dotyczy wyłącznie przetwarzania danych osobowych[68] i systemów informatycznych przetwarzających te dane. Nie obejmuje swoim zakresem m.in. informacji dotyczących konfiguracji infrastruktury informatycznej w tym serwerów, zasad bezpieczeństwa fizycznego w obiekcie czy stosowanych zabezpieczeń systemów informatycznych nieprzetwarzających danych osobowych.

**Granty dla jst w ramach projektu „Cyberbezpieczny Samorząd"**

Kontrolowane urzędy jst pozyskały granty przeznaczone na zwiększenie poziomu bezpieczeństwa informacji w ramach projektu „Cyberbezpieczny Samorząd" finansowane z Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027. Badaniem objęto prawidłowość wykorzystania pozyskanych środków. Łącznie kontrolą objęto 17 najwyższych wartościowo grantów, po jednym w każdym z kontrolowanych urzędów. Do badania wybrano urzędy, które najwcześniej otrzymały wszystkie transze grantu. Łączna wartość przyznanych kontrolowanym urzędom grantów wyniosła 13 105 379,30 zł, a wartość wydatkowana wyniosła 7 741 308,49 zł (z uwzględnieniem wkładu własnego jst w łącznej kwocie 932 653,00 zł), co stanowiło 59% środków przyznanych na realizację projektów grantowych. Ponadto, zaangażowanie w umowach jst z wykonawcami w ramach badanych umów grantowych wynosiło 1 546 550,24 zł, co stanowiło 11,8% łącznej kwoty środków przeznaczonych na realizację projektów grantowych w jst.

[68] Na podstawie rozporządzenia Parlamentu Europejskiego i Rady (WE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

**Przykład**

W **Starostwie Powiatowym w Kamiennej Górze** do dnia 21 sierpnia 2025 r. wykorzystano jedynie 3,59%[69] otrzymanego grantu na projekt, mimo otrzymania całości środków na konto starostwa w dniu 20 września 2024 r. Ponadto, przez prawie rok od otrzymania pełnych środków finansowych nie ogłoszono, do dnia zakończenia czynności kontrolnych NIK, postępowania o zamówienie publiczne, obejmującego zakup sprzętu oraz szkoleń przewidzianych we wniosku o przyznaniu grantu. Według wyjaśnień starosty umowa o powierzenie grantu nie określa dokładnej kolejności ani terminu wydatkowania środków, a Projekt trwa do dnia 30 czerwca 2026 r. Starosta wskazał również, że kwota dofinansowania została wypłacona na wniosek starostwa w całości, aby można było przeprowadzić pełne i kompleksowe zakupy i wdrożenie elementów systemu zwiększających cyberbezpieczeństwo.

Infografika nr 5
Wykorzystanie grantów na zwiększenie cyberbezpieczeństwa w kontrolowanych jst


*Źródło: opracowanie własne NIK na podstawie danych z kontroli.*

Warunki dofinansowania określała umowa o powierzenie grantu między grantobiorcą (urzędem) a beneficjentem, określała w szczególności: zadania objęte grantem, kwotę grantu i wkładu własnego, warunki przekazania i rozliczenia grantu, zobowiązanie do zwrotu grantu w przypadku wykorzystania go niezgodnie z celami projektu grantowego, zobowiązanie do poddania się kontroli przeprowadzanej przez beneficjenta lub inne podmioty uprawnione do przeprowadzenia kontroli. Dofinansowanie udzielane w formie grantów przeznaczone było na zadania w ramach trzech obszarów, tj. organizacyjnego, kompetencyjnego i technicznego.

[69] Wydatki kwalifikowalne 30 520,00 zł z 850 000,00 zł otrzymanego grantu.

W obszarze organizacyjnym środki mogły być przeznaczone m.in. na takie działania (usługi) jak:

- opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym między innymi wprowadzenie lub aktualizacja polityk bezpieczeństwa informacji (PBI), na sporządzenie analizy ryzyka (w tym opracowanie i wdrożenie metodyk);
- audyt SZBI, audyt zgodności KRI przez wykwalifikowanych audytorów, (re-)certyfikacja SZBI na zgodność z normami.

W obszarze kompetencyjnym przewidziano finansowanie następujących zadań:

- podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników jst,
- szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry jst, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji,
- szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach projektu grantowego,
- szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

W obszarze technicznym przewidziano finansowanie następujących działań (usług):

- zakup, wdrożenie i utrzymanie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, wykrywanie i reakcję na zagrożenia cyberbezpieczeństwa, z niezbędnym wsparciem producenta,
- zakup, wdrożenie i utrzymanie rozwiązań ciągłego monitorowania bezpieczeństwa, skanery podatności, zarządzanie podatnościami, zarządzanie zasobami IT i aktywami podlegającymi ochronie,
- zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń i oprogramowania z zakresu cyberbezpieczeństwa,
- zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa,
- zakup, wdrożenie i utrzymanie systemów lub usług na potrzeby operacyjnych centrów cyberbezpieczeństwa, także jako element Centrum Usług Wspólnych,
- zakup testów i badań bezpieczeństwa, dostępu do informacji bezpieczeństwa oraz inne usługi integracyjne dotyczące obszaru cyberbezpieczeństwa.

**Przykład**

W **Urzędzie Gminy i Miasta w Chęcinach** w ramach obszaru organizacyjnego określono realizację następujących trzech zadań:
- opracowanie i wdrożenie SZBI;
- wdrożenie w Urzędzie środków zarządzania ryzykiem w cyberbezpieczeństwie,
- przeprowadzenie trzech audytów SZBI (corocznie w okresie realizacji projektu).

W ramach obszaru kompetencyjnego określono realizację następujących zadań:
- przeprowadzenie trzech szkoleń podstawowych z zakresu cyberbezpieczeństwa dla pracowników Urzędu,
- przeprowadzenie trzech szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej Urzędu,
- przeprowadzenie czterech szkoleń z cyberbezpieczeństwa dla administratorów,
- zakup platformy szkoleniowej z zakresu cyberbezpieczeństwa na czas realizacji projektu.

W ramach obszaru technicznego określono realizację następujących zadań:
- zakup usług wsparcia realizowanych przez zewnętrznych ekspertów z zakresu cyberbezpieczeństwa,
- zakup klastra wysokiej wydajności złożonego z dwóch serwerów wraz z oprogramowaniem,
- zakup urządzenia UTM wraz z dwuletnim wsparciem,
- zakup dwóch urządzeń sieciowych switch wraz z dwuletnim wsparciem,
- zakup wsparcia na okres dwóch lat dla urządzeń sieciowych switch,
- zakup czterech urządzeń sieciowych wraz z dwuletnim wsparciem,
- zakup wsparcia technicznego na okres dwóch lat,
- zakup systemu do tworzenia kopii zapasowych,
- wdrożenie oprogramowania do gromadzenia i analizy zapisów działań w systemach – logów wraz ze wsparciem na czas trwania projektu,
- wdrożenie oprogramowania XDR, SIEM wraz ze wsparciem na czas trwania projektu,
- zakup oprogramowania antywirusowego, skaner podatności wraz ze wsparciem na czas trwania projektu,
- zakup i montaż generatora prądu,
- zakup zasilacza awaryjnego,
- zakup dysków do serwerów, serwerów pamięci masowej,
- zakup serwera do backupu wraz z niezbędnym oprogramowaniem,
- zakup macierzy dyskowej,
- zakup wirtualnej platformy udostępniającej zaawansowane funkcje ochrony poczty elektronicznej.

**Nieprawidłowości w realizacji projektów grantowych**

Nieprawidłowości w realizacji grantów stwierdzono w sześciu urzędach[70] z 17 kontrolowanych (36%). Nie miały one jednak zasadniczego wpływu na prawidłowość wykorzystania grantu (poza UG Świerklany). Dotyczyły one m.in.:

[70] Starostwo Powiatowe w: Białobrzegach i Legionowie oraz UMiG/UG: w Górze, Kłodzko, Serock, Świerklany.

- braku zabezpieczenia interesów zamawiającego, co było działaniem nierzetelnym (UMiG w Górze, UG Kłodzko);
- zakupu komponentów serwera w postaci 14 pamięci RAM o wartości 23 800,00 zł[71], które nie mieściły się bezpośrednio w katalogu działań (usług) na jakie można przeznaczyć środki projektu, określonego w § 3 ust. 2 pkt 3 Regulaminu Projektu. Zakup ten ponadto nie był ujęty we wniosku o przyznanie grantu (UMiG w Górze);
- wskazania we wniosku o dofinansowanie projektu *Poprawa cyberbezpieczeństwa Powiatu Białobrzeskiego* informacji niezgodnej ze stanem faktycznym, że starostwo posiada wdrożony i audytowany system SZBI, a jego dokumentacja wymagać będzie jednak dalszej aktualizacji/poprawy i rozbudowy z uwzględnieniem planowanych rozwiązań, co było działaniem nierzetelnym (Starostwo Powiatowe w Białobrzegach);
- nie zaksięgowania do dnia 18 czerwca 2025 r. w ewidencji księgowej wydatku dla projektu grantowego w kwocie 11 070 zł, poniesionego w grudniu 2023 r., na usługi doradcze w zakresie przygotowania koncepcji projektu oraz przygotowania dokumentacji finansowej – budżetu projektu, co było niezgodne z postanowieniami § 4 ust. 1 pkt 6 umowy grantowej (Starostwo Powiatowe w Białobrzegach);
- opóźnienia w realizacji obowiązków sprawozdawczych projektu grantowego, co stanowiło naruszenie § 7 ust. 2 umowy grantowej (Starostwo Powiatowe w Legionowie);
- nieprawidłowego określenia wartości dwóch wskaźników realizacji projektu grantowego we wniosku rozliczającym grant (UMiG Serock).

W przypadku **UG Świerklany** NIK negatywnie oceniła działalność Urzędu w zakresie realizacji projektu grantowego. Wartość wydatków w ramach projektu przewidziano na 849 700 zł, w tym dofinasowanie ze środków budżetu państwa i UE w łącznej wysokości 781 724,01 zł. Stwierdzono m.in. następujące nieprawidłowości:

- nieprzekazanie do NASK Ankiety Dojrzałości Cyberbezpieczeństwa dotyczącej jednej z gminnych jednostek przewidzianych jako korzystające z grantu oraz przekazanie jednej ankiety 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 grantu;
- udzielenie w dniu 31 października 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*[72] oraz nierzetelna realizacja i odbiór przedmiotu tego zamówienia;
- naruszenie postanowień *Wytycznych dotyczących kwalifikowalności wydatków na lata 2021–2027* Ministra Funduszy i Polityki Regionalnej

[71] Ogółem wydatkowano 29 274,00 zł, z czego 5 474,00 zł stanowiły wydatki niekwalifikowalne (podatek VAT).
[72] Dz. U. z 2024, poz. 1320, ze zm.

z 18 listopada 2022 r.[73] i obowiązującego w Urzędzie *Regulaminu udzielania zamówień publicznych o wartości szacunkowej nieprzekraczającej kwoty 130 000 zł*[74] 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 KRI oraz nierzetelne postanowienia i zapisy;
- niezapewnienie przeprowadzenia w 2024 r. w urzędzie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, do czego zobowiązywał § 20 ust. 2 pkt 14 rozporządzenia KRI[75];
- nierzetelną, niezgodną z postanowieniami § 11 umowy grantowej realizację obowiązków w zakresie informowania i promowania dofinansowania uzyskanego na realizację grantu.

W związku ze stwierdzonymi nieprawidłowościami, NIK wnioskowała o zwrot środków grantu pobranych przez urząd w nadmiernej wysokości z tytułu niespełniania przez wskazane wydatki warunków kwalifikowalności (poniesionych bez zastosowania przepisów ustawy *Prawo zamówień publicznych* lub z naruszeniem procedur i wytycznych dotyczących Programu FERC) wraz z odsetkami, w wysokości określonej jak dla zaległości podatkowych, stosownie do postanowień § 10 ust. 16 w związku z ust. 1 umowy grantowej.

**Jednostki organizacyjne jst biorące udział w projekcie grantowym**

W działaniach dotyczących realizacji projektu grantowego, poza wnioskodawcą (jst), w przypadku 10 kontrolowanych urzędów[76] (59%) brały również udział jednostki organizacyjne jst nieposiadające osobowości prawnej, takie jak m.in. placówki pomocy społecznej, placówki oświatowe, centra usług wspólnych (jednostki organizacyjne gmin powołane do obsługi placówek oświatowych), zakłady gospodarki komunalnej, zakłady wodociągowe, ośrodki kultury.

**Wskaźniki produktu i rezultatu w ramach grantu**

Zgodnie z § 4 ust. 10 Regulaminu Konkursu, jst w ramach realizacji projektów grantowych były zobowiązane do realizacji wskaźników określonych w załączniku nr 9 do ww. Regulaminu. W załączniku tym wskazano Opis wskaźników Projektu „Cyberbezpieczny Samorząd" oraz cele Projektu, które należało wyrazić adekwatnymi, mierzalnymi wskaźnikami:

---

[73] 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.).

[74] Wprowadzonego zarządzeniem nr W.0050.235.2020 Wójta Gminy z dnia 28 grudnia 2020 r.

[75] Obowiązującego do 22 maja 2024 r. Odpowiednio § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

[76] Starostwa Powiatowe w: Gliwicach, Kamiennej Górze, Legionowie i Ostrowcu Świętokrzyskim oraz UMiG/UG: Brody, Bystrzyca Kłodzka, Chmielnik, Kłodzko, Serock, Świerklany.

- produktu (powiązanymi bezpośrednio z wydatkami ponoszonymi w projekcie grantowym, zrealizowanymi w okresie od rozpoczęcia do ukończenia projektu. Osiągnięte wartości powinny zostać wykazane najpóźniej we wniosku rozliczającym, o którym mowa w § 3 ust. 2 pkt 2 Umowy o powierzenie grantu);
- rezultatu (odnoszącymi się do bezpośrednich efektów realizowanego projektu grantowego, osiągniętymi w wyniku realizacji projektu zdefiniowanymi we Wniosku o powierzenie grantu).

Kontrola wykazała, że zdefiniowane przez CPPC wskaźniki realizacji projektów grantowych, tak produktu, jak i rezultatu, nie były w żaden sposób powiązane z faktycznym wzrostem poziomu cyberbezpieczeństwa u grantobiorców (jst), a jedynie z liczbą dokonanych zakupów i przeszkolonych osób. Co więcej w kontrolowanych urzędach występowały sytuacje gdzie wartości wskaźników zostały wyznaczone na najniższym możliwym poziomie, tj. jeden projekt grantowy to jedna jednostka danego wskaźnika. Na przykład, wartość wskaźnika „Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym" określono w ten sposób, że przyjęto, iż każdy dofinansowany podmiot przeszkoli tylko jedną osobę, podobnie określono wartość wskaźnika „Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji" – jeden grantobiorca (jst) to jeden system.

Zdaniem NIK przyjęcie tak niskich wartości wskaźników zapewnia duże prawdopodobieństwo ich osiągnięcia, ale nie prowadzi do optymalnego wykorzystania pozyskanych funduszy i nie gwarantuje zasadniczej poprawy poziomu bezpieczeństwa. W takiej sytuacji wystarczy formalnie poprawne wydatkowanie środków przez grantobiorcę, aby CPPC mogło uznać, że osiągnięto poprawę poziomu bezpieczeństwa.

**Przykład**

**Urząd Gminy Lelis** we wniosku o przyznanie grantu wskazał pięć planowanych do osiągnięcia wskaźników wyrażających cele projektu grantowego:
- Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji – 2 szt.;
- Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach jst – 1 szt.;
- Liczba jst wspartych w zakresie cyberbezpieczeństwa – 1 szt.;
- Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa – 1 szt.;
- Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych – 1 szt.

W sześciu objętych kontrolą urzędach[77] (35%) na etapie zawierania umowy o powierzenie grantu nie wskazano wskaźników produktu i rezultatu lub nie podano ich wartości.

[77] Dotyczy to Starostw Powiatowych w: Gliwicach i Ostrowcu Świętokrzyskim oraz UMiG/UG: w Górze, Nowe Miasto nad Pilicą, Świerklany, w Wilkowicach.

**Przykład**

Starosta **Powiatu Gliwickiego** podał, że *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*[78] 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.

**Wykorzystanie przez jst zakupionych urządzeń i dostarczonych usług**

Z wyjątkiem UG Świerklany, zakupione w ramach projektów grantowych urządzenia i oprogramowanie zostały zainstalowane i były użytkowane przez kontrolowane urzędy oraz jednostki organizacyjne lub były na etapie wdrożenia. Zlecone usługi, tj. m.in. szkolenia zostały przeprowadzone lub były zaplanowane do realizacji. Zamówione w ramach grantu audyty bezpieczeństwa informacji zostały wykonane i sformułowano w nich wnioski/rekomendacje, z których część została wdrożona, a część była w trakcie realizacji lub została zaplanowana do realizacji.

[78] *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.*

**Realizacja przez jst obowiązków w zakresie informacji i promocji w ramach grantu**

Na podstawie § 11 ust. 3 umowy grantowej, w zakresie informacji i promocji projektu grantowego, grantobiorca (jst) zobowiązany był do stosowania zasad określonych w *Podręczniku wnioskodawcy i beneficjenta programów polityki spójności na lata 2021–2027 w zakresie informacji i promocji*. Obowiązek obejmował w szczególności:

- oznaczenie miejsca realizacji projektu grantowego poprzez umieszczenie plakatu;
- zamieszczenie znaków Funduszy Europejskich, barw Rzeczypospolitej Polskiej i Unii Europejskiej na dokumentach związanych z projektem grantowym, w tym na dokumentacji przetargowej, umowach, stronach internetowych, e-publikacjach;
- umieszczenie opisu projektu grantowego na stronie internetowej oraz w mediach społecznościowych grantobiorcy;
- umieszczenie na zakupionym sprzęcie trwałych naklejek.

W większości kontrolowanych urzędów[79] (11 z 17, tj. 65%) informowano opinię publiczną o fakcie otrzymania dofinansowania, m.in. poprzez umieszczenie plakatu na głównej tablicy informacyjnej oraz na tablicy multimedialnej w głównej hali obsługi obywateli w budynku urzędu. Na stronach internetowych tych urzędów oraz w ich mediach społecznościowych zamieszczano informacje dotyczące realizacji projektu grantowego oraz jego dofinansowania ze środków Unii Europejskiej.

W pozostałych sześciu urzędach[80] wystąpiły nieprawidłowości w zakresie informacji i promocji projektu grantowego i dotyczyły m.in.:

- braku umieszczenia plakatu informującego o grancie;
- niezamieszczeniu na stronach internetowych i w mediach społecznościowych urzędu informacji o uczestnictwie w projekcie grantowym;
- niewłaściwego oznakowania logotypami grantu dokumentacji przetargowej.

**Systemy Zarządzania Bezpieczeństwem Informacji w kontrolowanych urzędach jst**

Pomimo przystąpienia do projektu „Cyberbezpieczny Samorząd" w ponad połowie kontrolowanych urzędów nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji, który jest kluczowym elementem zapewnienia cyberbezpieczeństwa.

Jednostka, aby zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji. System Zarządzania Bezpieczeństwem Informacji określa wymagania oraz zasady inicjowania, wdrażania, utrzymania i poprawy zarządzania bezpieczeństwem informacji w jednostce, oraz zawiera najlepsze praktyki celów stosowania zabezpieczeń.

[79] Starostwo Powiatowe w: Białobrzegach, Gliwicach, Kamiennej Górze, Legionowie i Ostrowcu Świętokrzyskim oraz UMiG/UG: w Bystrzycy Kłodzkiej, Chęcinach, w Chmielniku, w Górze, Kłodzko, w Wilkowicach.

[80] UMiG/UG: Brody, Dąbrowa Zielona, Lelis, Nowe Miasto nad Pilicą, Serock, Świerklany.

W dziewięciu objętych kontrolą urzędach[81] (53 %) nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), o którym mowa w § 20 ust. 1 w zw. z ust. 3 wcześniejszego rozporządzenia KRI oraz § 19 ust. 1 w związku z ust. 3 obowiązującego rozporządzenia KRI, w szczególności nie ustanowiono polityki bezpieczeństwa informacji. W myśl tych przepisów podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ponadto, § 20 ust. 3 wcześniejszego rozporządzenia KRI oraz § 19 ust. 3 obwiązującego rozporządzenia KRI wskazuje, że wymagania określone w ww. ust. 1 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-EN ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą[82].

Kontrolowani wskazywali m.in., że planowane są, bądź zostały podjęte prace dla przygotowania SZBI, w tym polityki bezpieczeństwa informacji.

W pozostałych ośmiu urzędach opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji.

Spośród dziewięciu urzędów, w których nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z rozporządzeniem KRI, w siedmiu z nich (77%) przewidziano opracowanie SZBI w ramach grantu w zakresie obszaru organizacyjnego. W pozostałych dwóch urzędach (23%) działania takie jednak nie były planowane.

**Okresowy audyt z zakresu bezpieczeństwa informacji**

W ośmiu urzędach[83] (47 %) w 2023 r. lub 2024 r. nie przeprowadzono obowiązkowego audytu z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI[84] lub audyt przeprowadzono nierzetelnie, bądź z naruszeniem zasady niezależności i obiektywizmu audytu. Powyższe nieprawidłowości tłumaczono m.in. brakiem pracowników posiadających niezbędną wiedzę i doświadczenie dla przeprowadzenia takiego audytu.

---

81 Dotyczy to Starostw Powiatowych w: Białobrzegach, Kamiennej Górze i Ostrowcu Świętokrzyskim oraz UMiG/UG: Brody, w Chęcinach, Lelis, Nowe Miasto nad Pilicą, Serock, w Wilkowicach.

82 W tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

83 Dotyczy: Starostw Powiatowych w: Legionowie i Ostrowcu Świętokrzyskim oraz UMiG/UG: Brody, w Bystrzycy Kłodzkiej, w Chęcinach, w Chmielniku, Świerklany, w Wilkowicach.

84 Obowiązującego do 22 maja 2024 r. Odpowiednio § 19 ust. 2 pkt 14 rozporządzenia KRI obowiązującego od 23 maja 2024 r.

**Przykład**

W **Starostwie Powiatowym w Legionowie** i trzech jednostkach podległych m.in. audyty SZBI oraz inne audyty związane z bezpieczeństwem informacji zostały przeprowadzone przez osobę, która pełniła w tych jednostkach jednocześnie funkcję IOD, co naruszało art. 38 ust. 6 RODO.
Zgodnie z art. 38 ust. 6 RODO, osoba wyznaczona na IOD może wykonywać inne zadania i obowiązki, jednak administrator danych (tj. starosta) musi zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów.
Zdaniem NIK wykonywanie obowiązków IOD w starostwie, jak i w jednostkach podległych, oraz przeprowadzenie ww. audytów, stanowi konflikt interesów i tym samym narusza art. 38 ust. 6 RODO. Powyższe wynika z faktu, iż zadaniem audytora było sprawdzenie przestrzegania zgodności działań starostwa (jego pracowników) z przepisami prawa (w tym z RODO), natomiast jednym z zadań IOD jest decydowanie o stosowaniu przepisów RODO w starostwie (art. 39 ust. 1 RODO). Pomimo, iż starosta ostatecznie zatwierdzał zmiany w SZBI, to merytoryczne opracowanie zmian leżało po stronie IOD – osoby, która sama dokonywała przeglądów zgodności, audytowała wdrożone procedury i kontrolowała obszar działań, m.in. postępowania z incydentami naruszenia danych osobowych, które sama współtworzyła i za które odpowiadała, tym samym oceniając poprawność tych działań, oraz przygotowując propozycje zmian. Biorąc pod uwagę fakt, że audyt wewnętrzny SZBI powinien być przeprowadzany przez osoby zapewniające obiektywność i bezstronność procesu audytu, w tym przypadku ocena SZBI przez IOD stwarza ryzyko dla procesu weryfikacji zapewnienia stanu bezpieczeństwa informacji stosowanego w starostwie.

**Inne stwierdzone nieprawidłowości związane z bezpieczeństwem informacji**

W siedmiu jednostkach[85] z 17 s41%) stwierdzono także inne nieprawidłowości w zakresie bezpieczeństwa informacji, które dotyczyły m.in.:

- niewłaściwego zabezpieczenia serwerowni, w tym przechowywania w nich materiałów łatwopalnych;
- niewłaściwego sporządzania kopii zapasowych;
- nieodebrania uprawnień do systemów informatycznych osobom, które zakończyły zatrudnienie;
- niestosowania procedury przyznawania uprawnień w systemach informatycznych;
- ustawienia monitorów w sposób umożliwiający wgląd osobom postronnym w dane osobowe;
- ustanowienia Polityki Bezpieczeństwa Informacji zawierającej wewnętrznie sprzeczne, niezgodne z prawem postanowienia i zapisy.

[85] Dotyczy to Starostwa Powiatowego w Kamiennej Górze oraz UMiG/UG: Dąbrowa Zielona, w Górze, w Kłodzku, Nowe Miasto nad Pilicą, Świerklany, w Wilkowicach.

**Przykłady**

W **Urzędzie Miasta i Gminy w Górze** badanie wykazało, że wszystkie trzy osoby, które zakończyły zatrudnienie w Urzędzie po 1 stycznia 2025 r. nadal miały aktywne konta użytkowników w domenie Active Directory, umożliwiające jednocześnie logowanie (i dostęp) do innych systemów dziedzinowych Urzędu. Było to niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI. Sekretarz miasta i gminy wyjaśnił, że sytuacja ta miała miejsce z powodu nieuwagi informatyków, a konta tych osób nie były używane i zostały zablokowane w trakcie oględzin.

W **Starostwie Powiatowym w Kamiennej Górze** nie sporządzano wniosków o odebranie uprawnień w systemach informatycznych, osobom, które zakończyły pracę w Urzędzie, co było niezgodne z art. 20 ust. 2 Polityki Ochrony Danych Osobowych[86] (PODO). Oględziny wykazały brak wniosków o wyrejestrowanie uprawnień dla wszystkich ośmiu sprawdzanych pracowników, którzy zakończyli zatrudnienie po 1 stycznia 2023 r. Starosta wyjaśniła, że odbieranie uprawnień pracownikom, którzy kończą zatrudnienie, realizowane było na podstawie aktualnej karty rozliczenia pracownika. Przyznała jednak, że praktyka ta nie znalazła odzwierciedlenia w PODO i zadeklarowała, że stosowny zapis zostanie zamieszczony w kolejnej wersji SZBI.

W **Starostwie w Kamiennej Górze** sporządzano kopie zapasowe danych niezgodnie z art. 23 ust. 4 PODO, tj. znajdowały się one w tym samym pomieszczeniu co dane źródłowe. Oględziny wykazały, że kopie zapasowe wykonane automatycznie na zasobach dyskowych (macierzy) znajdowały się w pomieszczeniu serwerowni głównej wraz z podstawowym serwerem produkcyjnym. Natomiast kopie zapasowe wykonywane ręcznie na serwerze NAS[87] zlokalizowanym w serwerowni pomocniczej, były sporządzane z niewystarczającą[88] częstotliwością, przez co nie spełniały one wymogów w zakresie sporządzania i przechowywania kopii zapasowych w innym miejscu niż podstawowy serwer produkcyjny.
Starosta poinformowała, że został już uruchomiony skrypt, który automatyzuje proces wykonania kopii zapasowej na serwerze NAS, eliminując problemy związane z częstotliwością ich tworzenia. Pozwala to przechowywać prawidłowo sporządzone kopie w innym pomieszczeniu niż serwer produkcyjny. Przeprowadzone ponowne oględziny wykazały, że rozwiązanie to zostało wprowadzone i funkcjonuje poprawnie.

[86] Załącznik nr 1 do Zarządzenia Nr 19/2023 Starosty Kamiennogórskiego z 27 czerwca 2023 r.

[87] Network Attached Storage, to urządzenie do przechowywania i udostępniania danych w sieci lokalnej i przez Internet.

[88] Kopia sporządzona około miesiąc przed oględzinami, zamiast codzienne/raz w tygodniu.

# 6. ZAŁĄCZNIKI

## 6.1. METODYKA KONTROLI I INFORMACJE DODATKOWE

**Cel główny kontroli**

Czy projekt „Cyberbezpieczny Samorząd" był realizowany zgodnie z założeniami oraz skutecznie?

**Cele szczegółowe**

1. Czy CPPC prawidłowo, terminowo i zgodnie z założeniami realizuje projekt „Cyberbezpieczny Samorząd"?
2. Czy NASK prowadzi skuteczne i zgodne z umową o partnerstwie działania na rzecz osiągania rezultatów określonych w projekcie „Cyberbezpieczny Samorząd"?
3. Czy gminy i powiaty w ramach projektu „Cyberbezpieczny Samorząd" podejmują skuteczne działania w celu zwiększenia poziomu bezpieczeństwa informacji, w szczególności czy skutecznie osiągają założone rezultaty?

**Podstawa podjęcia kontroli**

Inicjatywa własna NIK.

**Zakres podmiotowy**

Kontrolą objęto 19 jednostek: 12 urzędów miast i gmin i 5 starostw powiatowych oraz CPPC i NASK.

**Kryteria kontroli**

Kontrolę w CPPC i NASK przeprowadzono na podstawie art. 2 ust. 1 ustawy o NIK z uwzględnieniem kryteriów: legalności, gospodarności, rzetelności i celowości, a w urzędach jst na podstawie art. 2 ust. 2 ustawy o NIK z uwzględnieniem kryteriów: legalności, gospodarności i rzetelności.

**Okres objęty kontrolą**

Kontrolą objęto okres od 1 stycznia 2023 r. do dnia zakończenia kontroli. Czynności kontrolne w jednostkach przeprowadzono w okresie od 28 kwietnia 2025 r. do 5 września 2025 r. Ostatnie wystąpienie pokontrolne zostało podpisane 26 września 2025 r.

Zgłoszono dwa zastrzeżenia do wystąpienia pokontrolnego skierowanego do Dyrektora Centrum Projektów Polska Cyfrowa. Zastrzeżenia dotyczyły:

- nieprawidłowości polegającej na tym, że w dokumentacji konkursu grantowego nie przewidziano oceny poziomu cyberbezpieczeństwa u grantobiorców na etapie składania przez nich wniosków o grant oraz nie przyjęto zasady, aby powiązać osiągnięty poziom cyberbezpieczeństwa po zakończeniu prac w ramach grantu z kwalifikowalnością wydatków i związanego z tą nieprawidłowością wniosku;
- nieprawidłowości polegającej na tym, że w Projekcie, w ramach projektów grantowych, dopuszczono możliwość jednoczesnego funkcjonowania na serwerach zarówno systemów dziedzinowych jak i systemów bezpieczeństwa oraz związanego z tą nieprawidłowością wniosku.

Uchwałą Zespołu Orzekającego Komisji Rozstrzygającej NIK z dnia 1 grudnia 2025 r. zastrzeżenia oddalono.

Wójt Gminy Świerklany zgłosił dziewięć zastrzeżeń do wystąpienia pokontrolnego z dnia 9 września 2025 r. (LKA.410.12.2.2025). Uchwałą Zespołu Orzekającego Komisji Rozstrzygającej NIK z dnia 1 grudnia 2025 r. zastrzeżenia oddalono.

**Stan realizacji wniosków pokontrolnych**

Do kierowników jednostek kontrolowanych zostało skierowanych 19 wystąpień pokontrolnych. NIK sformułowała 46 wniosków pokontrolnych. Według stanu na dzień 4 lutego 2026 r. zrealizowano 10 wniosków, a 36 było w trakcie realizacji.

Kierownicy kontrolowanych urzędów poinformowali NIK o podjęciu działań na rzecz realizacji wniosków pokontrolnych.

Wnioski NIK skierowane do kierowników jednostek kontrolowanych dotyczyły m.in.:

- opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji,
- zapewnienia odpowiedniego poziomu zabezpieczenia fizycznego serwerowni,
- dokonania korekty wniosku rozliczającego w zakresie wartości wskaźników realizacji Projektu i przekazanie skorygowanego wniosku do NASK,
- zapewnienia wypełniania obowiązku w zakresie informacji i promocji zgodnie z określonymi wymogami,
- zapewnienia rzetelnego sporządzania dokumentów związanych z realizacją Projektu,
- zapewnienia prowadzenia audytu w zakresie bezpieczeństwa informacji nie rzadziej niż raz w roku.

**Finansowe rezultaty kontroli NIK**

Finansowe rezultaty kontroli NIK wyniosły łącznie 304 338,50 zł, w tym: kwota wydatkowana z naruszeniem prawa w wysokości 254 548,50 zł oraz kwota wydatkowana z naruszeniem zasad należytego zarządzania finansami w wysokości 49 790 zł.

**Wykaz jednostek kontrolowanych**

| Lp. | Jednostka organizacyjna NIK przeprowadzająca kontrolę | Nazwa jednostki kontrolowanej | Imię i nazwisko kierownika jednostki kontrolowanej |
|---|---|---|---|
| 1. | Departament Administracji Publicznej | Centrum Projektów Polska Cyfrowa | Wojciech Szajnar |
| 2. | | Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy | Radosław Nielek<br>od 28 grudnia 2023 r.<br>wcześniej<br>Wojciech Pawlak jako pełniący obowiązki Dyrektora<br>od 23 listopada 2022 r.<br>do 26 września 2023 r.<br>oraz jako Dyrektor<br>od 27 września 2023 r.<br>do 28 grudnia 2023 r. |
| 3. | | Starostwo Powiatowe w Białobrzegach | Sylwester Korgul |
| 4. | | Starostwo Powiatowe w Legionowie | Roman Smogorzewski<br>od 6 maja 2024 r.<br>wcześniej Sylwester Sokolnicki<br>od 27 kwietnia 2020 r.<br>do 5 maja 2024 r. |
| 5. | | Urząd Gminy Lelis | Stefan Prusik |
| 6. | | Urząd Miasta i Gminy Nowe Miasto nad Pilicą | Barbara Gąsiorowska<br>od 7 maja 2024 r.<br>wcześniej Mariusz Dziuba<br>od 22 listopada 2018 r.<br>do 6 maja 2024 r. |

| Lp. | Jednostka organizacyjna NIK przeprowadzająca kontrolę | Nazwa jednostki kontrolowanej | Imię i nazwisko kierownika jednostki kontrolowanej |
|---|---|---|---|
| 7. | | Urząd Miasta i Gminy Serock | Artur Borkowski |
| 8. | Delegatura NIK w Katowicach | Starostwo Powiatowe w Gliwicach | Dawid Rams<br>od 7 maja 2024 r.<br>wcześniej Włodzimierz Gwiżdż<br>od 27 października 2022 r. |
| 9. | | Urząd Gminy Dąbrowa Zielona | Joanna Sokolińska<br>od 6 maja 2024 r.<br>wcześniej Maria Włodarczyk<br>od 19 listopada 2018 r.<br>do 6 maja 2024 r. |
| 10. | | Urząd Gminy Świerklany | Tomasz Pieczka |
| 11. | | Urząd Gminy w Wilkowicach | Maciej Mrówka<br>od 14 maja 2024 r.<br>wcześniej Janusz Zemanek<br>od 20 listopada 2018 r.<br>do 14 maja 2024 r. |
| 12. | Delegatura NIK w Kielcach | Starostwo Powiatowe w Ostrowcu Świętokrzyskim | Agnieszka Rogalińska<br>od 15 maja 2024 r.<br>wcześniej Marzena Dębnika<br>od 22 listopada 2018 r.<br>do 14 maja 2024 r. |
| 13. | | Urząd Gminy Brody | Ernest Kumek<br>od 7 kwietnia 2024 r.<br>wcześniej Agata Bernat<br>od 21 października 2018 r.<br>do 6 kwietnia 2024 r. |
| 14. | | Urząd Gminy i Miasta w Chęcinach | Robert Jaworski |
| 15. | | Urząd Miasta i Gminy w Chmielniku | Paweł Wójcik |
| 16. | Delegatura NIK we Wrocławiu | Starostwo Powiatowe w Kamiennej Górze | Małgorzata Krzyszkowska<br>od 7 maja 2024 r.<br>wcześniej Jarosław Gęborys<br>od 20 listopada 2018 r.<br>do 7 maja 2024 r. |
| 17. | | Urząd Miasta i Gminy w Bystrzycy Kłodzkiej | Renata Surma |
| 18. | | Urząd Miasta i Gminy w Górze | Tadeusz Juska<br>od 17 lipca 2024 r.<br>wcześniej Irena Krzyszkiewicz<br>od 6 marca 2008 r.<br>do 17 lipca 2024 r. |
| 19. | | Urząd Gminy Kłodzko | Zbigniew Tur |

## 6.1.1. WYKAZ OCEN KONTROLOWANYCH JEDNOSTEK

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| 1. | Centrum Projektów Polska Cyfrowa | w formie opisowej | • CPPC prawidłowo zorganizowało nabór wniosków do Konkursu Grantowego pn. „Cyberbezpieczny Samorząd", określiło kryteria wyboru projektów i zapewniło jst równy dostęp do środków grantowych.<br>• Ustanowiono struktury zarządcze, w tym wyznaczono pracowników odpowiedzialnych za realizację Projektu.<br>• Określono system monitorowania wskaźników produktu i rezultatu dla Projektu.<br>• W ramach systemu monitorowania organizowano cotygodniowe spotkania z przedstawicielami NASK, podczas których omawiano bieżące tematy związane z realizacją Projektu, postępy prac, trudności i ryzyka.<br>• Analizowano raporty Partnera z realizacji Projektu w zakresie liczby podpisanych umów, zleconych i wypłaconych przelewów, złożonych wniosków o kolejne transze, wniosków końcowych i sprawozdań. | • W dokumentacji konkursu grantowego nie przewidziano oceny poziomu cyberbezpieczeństwa jst na etapie składania wniosków o grant oraz nie powiązano kwalifikowalności wydatków ponoszonych w ramach umów o powierzeniu grantów ze wzrostem poziomu cyberbezpieczeństwa jst po wykorzystaniu grantu.<br>• W związku z realizacją Projektu przewidziano zarządzanie ryzykiem i zidentyfikowano 11 ryzyk, jednak w analizie ryzyka zamiast wymaganych mechanizmów kontrolnych opisano mechanizmy zapobiegania, które, zdaniem NIK, nie zapewniały bezzwłocznego podjęcia działań zaradczych w przypadku wystąpienia ryzyka, co było działaniem nierzetelnym i ogranicza skuteczność systemu zarządzania Projektem.<br>• Przyjęty w Projekcie system monitorowania wskaźników nie dostarczał informacji na temat postępu rzeczowego, ponieważ CPPC dotychczas dokumentowało i sprawozdawało monitorowanie tylko jednego wskaźnika dotyczącego liczby podmiotów wspartych w zakresie cyberbezpieczeństwa, co było działaniem nierzetelnym.<br>• W ramach Projektu CPPC dopuściło możliwość jednoczesnego funkcjonowania systemów dziedzinowych i bezpieczeństwa na serwerach nabywanych przez jst w ramach grantów na zwiększenie bezpieczeństwa informacji, co było niezgodne z wymogami § 15 ust. 1 rozporządzenia KRI.<br>Ponadto stwierdzono nieprawidłowości polegające m.in. na:<br>• poniesieniu przez CPPC jako Beneficjenta w ramach zadania nr 5 „Ewaluacja, rozliczenie projektu" wydatków w wysokości 828,3 tys. zł przed planowanym terminem jego rozpoczęcia, co było niezgodne z postanowieniami § 5 ust. 8 Decyzji o dofinansowaniu projektu „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, a także z § 4 ust. 3 Umowy o partnerstwie w celu wspólnej realizacji projektu pn. „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 z 14 lipca 2023 r.;<br>• niewystąpieniu Beneficjenta do Instytucji Pośredniczącej w sprawie potrzeby zmiany wskaźników w związku z brakiem możliwości osiągnięcia dwóch zaplanowanych wskaźników w ramach Projektu, co było nierzetelne. |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| 2. | Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy | w formie opisowej | • W okresie objętym kontrolą NASK, jako partner CPPC prowadził na ogół skuteczne i zgodne z umową o partnerstwie, działania na rzecz osiągania rezultatów określonych w Projekcie.<br>• NASK zapewnił wystarczającą dla sprawnej realizacji Projektu obsadę kadrową oraz ustanowił odpowiednie struktury zarządcze.<br>• Pracownicy NASK uczestniczący w realizacji Projektu, w szczególności eksperci merytoryczni oceniający wnioski o udzielenie grantu, posiadali odpowiednie kwalifikacje.<br>• Realizacja Projektu przebiegała terminowo, zgodnie z przygotowanym harmonogramem i była na bieżąco monitorowana przez NASK.<br>• NASK zgodnie z § 5 ust. 7 pkt 1 umowy o partnerstwie zorganizował i przeprowadził nabór wniosków o przyznanie grantu. W naborze tym, zgodnie z § 5 ust. 7 pkt 2 umowy o partnerstwie, NASK zapewnił różnego rodzaju wsparcie dla wnioskodawców, m.in. infolinię telefoniczną i webinaria, z którego mogli oni korzystać również na etapie realizacji grantów.<br>• Przy ocenie wniosków o przyznanie grantu NASK prawidłowo weryfikował spełnianie przez wnioskodawców kryteriów formalnych i merytorycznych. Następnie NASK gromadził dokumentację do zawarcia umów grantowych i przekazywał ją do CPPC celem podpisania. Zgodnie z przyjętym harmonogramem obecnie trwa etap realizacji powierzonych grantów, a NASK rozpoczął weryfikację pierwszych wniosków o rozliczenie grantu. | Stwierdzone w toku kontroli nieprawidłowości polegały na:<br>• wydaniu decyzji w przedmiocie powołania nowego Kierownika Projektu po ponad 18 miesiącach od faktycznego powierzenia mu tej funkcji, co było nierzetelne,<br>• niewyznaczeniu przedstawicieli NASK do Zespołu Projektowego, co było niezgodne z § 2 ust. 8 w zw. z § 1 ust. 17 umowy o partnerstwie,<br>• nierzetelnej weryfikacji 13 z 15 objętych badaniem wniosków o rozliczenie grantu.<br>W ocenie NIK, nieprawidłowości te nie miały zasadniczego wpływu na realizację zadań NASK określonych w umowie o partnerstwie, jednak wskazują one na potrzebę zwiększenia staranności przy ich realizacji. |
| 3. | Starostwo Powiatowe w Białobrzegach | w formie opisowej | • Starosta białobrzeski w latach 2023–2025 podejmował działania w celu zwiększenia poziomu cyberbezpieczeństwa, realizując projekt pn. Poprawa cyberbezpieczeństwa powiatu białobrzeskiego.<br>• W ramach Projektu m.in. przeprowadzono postępowania przetargowe i zawarto umowy, w szczególności dotyczące świadczenia usług Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji oraz wdrożenia SZBI i przygotowania/aktualizacji dokumentów SZBI.<br>• Informowano opinię publiczną o otrzymaniu dofinansowania na realizację Projektu.<br>• W okresie objętym kontrolą w starostwie rozpoznano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, m.in. poprzez przeprowadzenie analiz, które wykazały niski poziom świadomości pracowników w zakresie zagrożeń cybernetycznych oraz niską skuteczność procedur reagowania na incydenty bezpieczeństwa. | • Na dzień zakończenia kontroli Projekt był w trakcie realizacji i nie osiągnięto jeszcze docelowych poziomów wskaźników określonych we wniosku o dofinansowanie Projektu.<br>Stwierdzone w trakcie kontroli nieprawidłowości nie miały istotnego wpływu na realizację Projektu i dotyczyły:<br>• niewdrożenia SZBI, o którym mowa w §19 ust. 1 w związku z ust. 3 rozporządzenia KRI,<br>• nierzetelnego sporządzenia Ankiety Dojrzałości Cyberbezpieczeństwa w ramach Projektu,<br>• nierzetelnego sporządzenia wniosku o dofinansowanie projektu Poprawa cyberbezpieczeństwa powiatu białobrzeskiego,<br>• niezaksięgowania w wyodrębnionej ewidencji księgowej wydatków prowadzonej przez starostwo dla Projektu, wydatku kwalifikowanego w kwocie 11 070 zł, co było niezgodne z postanowieniami §4 ust. 1 pkt 6 umowy grantowej,<br>• nierzetelnego sporządzenia umowy Nr 48/AR/2025 z 26 maja 2025 r. dotyczącej świadczenia usług |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| | | | • W związku z przystąpieniem do Projektu terminowo wypełniono Ankietę Dojrzałości Cyberbezpieczeństwa i przekazano ją do NASK.<br>• W starostwie w 2024 r. zgodnie z §19 ust. 2 pkt 14 rozporządzenia KRI, przeprowadzono okresowy audyt z zakresu bezpieczeństwa informacji, z którego część zaleceń planowana jest do realizacji w ramach ww. Projektu. | Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),<br>• nierzetelnego sporządzenia protokołu z przeprowadzonego postępowania, w ramach którego zawarto umowę Nr 49/AR/2025 z 27 maja 2025 r. |
| 4. | Starostwo Powiatowe w Legionowie | w formie opisowej | • Powiat legionowski w latach 2023–2025 podejmował działania na rzecz zwiększenia poziomu cyberbezpieczeństwa realizując projekt pn. *Cyberbezpieczny samorząd w Powiecie Legionowskim* na potrzeby starostwa oraz jednostek podległych. W ramach Projektu m.in. przeprowadzono postępowania przetargowe oraz dokonano zakupu urządzeń i oprogramowania zwiększających odporność na cyberataki, a także prowadzono audyty z zakresu diagnozy cyberbezpieczeństwa.<br>• W okresie objętym kontrolą w starostwie rozpoznawano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa oraz wdrożono w tym zakresie rozwiązania organizacyjne i techniczne.<br>• W starostwie w 2021 r. ustanowiono System Zarządzania Bezpieczeństwem Informacji, który podlegał regularnym przeglądom.<br>• Informowano opinię publiczną o otrzymaniu dofinansowania na realizację Projektu.<br>• Grantobiorca zrealizował wszystkie zadania dotyczące Projektu i osiągnął założone wskaźniki produktu. | Stwierdzone w trakcie kontroli nieprawidłowości nie miały istotnego wpływu na realizację Projektu i polegały na:<br>• nieterminowym przekazaniu NASK informacji o postępie rzeczowym realizacji Projektu, co było niezgodne z § 7 ust. 2 umowy grantowej;<br>• przeprowadzeniu w Urzędzie zadania audytowego pn.: *Audyt wewnętrzny bezpieczeństwa informacji i ochrony danych osobowych w oparciu o wymagania PN ISO/IEC 27001 i RODO*, a także audytów SZBI oraz audytów zgodności z wymaganiami prawnymi – Diagnoza cyberbezpieczeństwa w Urzędzie oraz trzech jednostkach podległych przez osobę, która pełniła jednocześnie funkcję Inspektora Ochrony Danych w tych jednostkach, i tym samym wystąpił konflikt interesów co naruszało art. 38 ust. 6 RODO;<br>• nieprzestrzeganiu niektórych obowiązków informacyjnych i promocyjnych określonych w § 11 ust. 3 umowy grantowej w zakresie stosowania oznaczania znakiem Unii Europejskiej i Funduszy Europejskich i barw Rzeczypospolitej Polskiej w publikowanych informacjach na stronie internetowej oraz oficjalnym profilu mediów społecznościowych, a także części dokumentacji projektowej. |
| 5. | Urząd Gminy Lelis | w formie opisowej | • Gmina Lelis w latach 2023–2025 podejmowała działania w celu zwiększenia poziomu cyberbezpieczeństwa, w tym w ramach realizacji projektu pn. *Dostosowanie struktury informatycznej Gminy Lelis w zakresie cyberbezpieczeństwa* m.in. przeprowadzono postępowanie przetargowe oraz zawarto umowy na dostawę, instalację i konfigurację sprzętu i oprogramowania. Ponadto, uruchomiono usługi SaaS multiportalu gminy wraz z ochroną AntyDDos.<br>• W urzędzie rozpoznano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa.<br>• Przeprowadzono okresowy audyt z zakresu bezpieczeństwa informacji.<br>• Ustalono adekwatne wskaźniki produktu i rezultatu. | Stwierdzone w trakcie kontroli nieprawidłowości nie miały zasadniczego wpływu na realizację Projektu i dotyczyły:<br>• niewdrożenia SZBI, o którym mowa w §19 ust. 1 w związku z ust. 3 rozporządzenia KRI;<br>• niewypełnienia niektórych obowiązków z zakresu informacji i promocji Projektu określonych na podstawie § 11 ust. 3 umowy grantowej, w zakresie oznaczenia dokumentów znakami Funduszy Europejskich i Unii Europejskiej oraz barwami Rzeczypospolitej Polskiej, a także nie zawarcia wymaganych informacji dotyczących opisu Projektu na stronie internetowej i mediach społecznościowych Urzędu;<br>• nierzetelnego sporządzenia Ankiety Dojrzałości. |
| 6. | Urząd Miasta i Gminy Nowe Miasto nad Pilicą | w formie opisowej | • Gmina Nowe Miasto nad Pilicą w latach 2023–2025 podejmowała działania na rzecz zwiększenia poziomu cyberbezpieczeństwa realizując projekt | W toku kontroli stwierdzono nieprawidłowości polegające na:<br>• niewdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji, o którym |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| | | | pn. *Wzmocnienie cyberbezpieczeństwa w Urzędzie Miasta i Gminy Nowe Miasto nad Pilicą* na potrzeby urzędu. W ramach Projektu m.in. przeprowadzono postępowanie przetargowe oraz zawarto umowę na zakup urządzeń i oprogramowania zwiększających odporność na cyberataki, a także zawarto umowy na przeprowadzenie audytów z zakresu diagnozy cyberbezpieczeństwa oraz przygotowania dokumentacji SZBI.<br>• Podjęto działania informacyjne dotyczące otrzymania dofinansowania i realizacji Projektu. | mowa w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI,<br>• nieoznaczeniu miejsca realizacji Projektu plakatem informującym o dofinansowaniu, a także niezamieszczeniu opisu Projektu w mediach społecznościowych oraz nieprzestrzeganiu niektórych obowiązków informacyjnych i promocyjnych w zakresie stosowania oznaczeń: znakiem Unii Europejskiej i Funduszy Europejskich, i barw Rzeczypospolitej Polskiej – w publikowanych informacjach na stronie internetowej i części dokumentacji projektowej, co było niezgodne z postanowieniami § 11 ust. 3 umowy grantowej,<br>• przechowywaniu w serwerowni, tj. pomieszczeniu podlegającemu szczególnej ochronie materiałów łatwopalnych, tj. kartonów i wyeksploatowanego sprzętu komputerowego, co zwiększało ryzyko utraty danych bądź zakłócenia ciągłości działania urzędu na skutek pożaru i było niezgodne z § 19 ust. 2 pkt 9 rozporządzenia KRI. |
| 7. | Urząd Miasta i Gminy Serock | w formie opisowej | • Gmina Serock w latach 2023–2025 podejmowała działania w celu zwiększenia poziomu cyberbezpieczeństwa, w tym realizując projekt pn. *Gmina Serock – Cyberbezpieczny Samorząd* w urzędzie oraz czterech jednostkach podległych. W ramach Projektu m.in. przeprowadzono postępowanie przetargowe oraz dokonano zakupu urządzeń i oprogramowania zwiększającego poziom zabezpieczeń przed cyberatakami, a także przeszkolono pracowników z zakresu cyberbezpieczeństwa. Zrealizowano projekt w całym założonym zakresie rzeczowym. Dokonano także zwrotu niewykorzystanych środków i rozliczenia Projektu, które zostało zatwierdzone przez NASK. | Stwierdzone nieprawidłowości nie miały istotnego wpływu na realizację i rozliczenie zadań objętych Projektem i dotyczyły:<br>• nierzetelnego sporządzenia pięciu Ankiet dojrzałości,<br>• nierzetelnego wykazania wartości docelowej dla dwóch wskaźników Projektu,<br>• niewdrożenia SZBI, o którym mowa w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI,<br>• nieprzeprowadzenia audytu bezpieczeństwa informacji w 2023 r.,<br>• niewypełnienia niektórych obowiązków z zakresu informacji i promocji Projektu określonych na podstawie § 11 umowy grantowej, w zakresie oznaczenia dokumentów znakami Funduszy Europejskich i Unii Europejskiej oraz barwami Rzeczypospolitej Polskiej, a także nie umieszczenia niektórych wymaganych informacji dotyczących Projektu na stronie internetowej urzędu. |
| 8. | Starostwo Powiatowe w Gliwicach | pozytywna | • W dokumentach strategicznych starostwa nie uwzględniono wprost zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa w jednostce, jednakże zawarto w nich zapisy pośrednio odnoszące się tego zagadnienia.<br>• 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.<br>• Starostwo powiatowe przekazywało do NASK Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach | |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| | | | Samorządu Terytorialnego zgodnie z wymogami umowy o powierzenie grantu oraz Regulaminu Konkursu Grantowego Cyberbezpieczny Samorząd.<br>• Środki z dofinansowania Projektu Cyberbezpieczny Powiat Gliwicki 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.<br>• W realizacji Projektu brały udział dwie jednostki organizacyjne starostwa w zakresie umieszczenia ich zasobów na serwerach starostwa sraz 12 jednostek w zakresie przekazania zakupionego oprogramowania antywirusowego.<br>• W związku z realizacją Projektu wyznaczono pracowników odpowiedzialnych za jego realizację. Ich liczba nie ulegała zmianie w okresie od rozpoczęcia realizacji Projektu.<br>• 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.<br>• W starostwie powiatowym opracowano, ustanowiono i wdrożono SZBI, na który składała się Polityka Bezpieczeństwa Informacji oraz Instrukcja zarządzania systemem informatycznym. Podlegały one corocznym przeglądom, zgodnie z wewnętrznymi regulacjami jednostki kontrolowanej.<br>• W badanym okresie w starostwie przeprowadzane były okresowe audyty wewnętrzne z zakresu bezpieczeństwa informacji, realizowane przez osoby posiadające wymagane kompetencje.<br>• Starostwo powiatowe realizowało obowiązki informacyjne wynikające z Umowy w związku z dofinansowaniem na realizację Projektu. | |
| 9. | Urząd Gminy Dąbrowa Zielona | w formie opisowej | • W okresie objętym kontrolą gmina Dąbrowa Zielona na podstawie umowy o powierzenie grantu zawartej z CPPC 22 kwietnia 2024 r. zrealizowała projekt pod nazwą *Wzmocnienie odporności na zagrożenia płynące z Cyberbezpieczeństwa*.<br>• Środki finansowe zostały przez gminę wykorzystane zgodnie z przeznaczeniem, wszystkie wydatki spełniały warunki kwalifikowalności, a niewykorzystaną kwotę grantu zwrócono w przewidzianym umową terminie. CPPC oraz NASK także uznały poniesione przez gminę wydatki | • W trakcie realizacji Projektu urząd nie informował na bieżąco i w sposób ciągły o uzyskanym jego dofinasowaniu ze środków Unii Europejskiej i budżetu państwa oraz niezrealizowanie prac zabezpieczających dostęp do pomieszczenia serwerowni urzędu. |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| | | | za kwalifikowalne, prawidłowo udokumentowane i poniesione terminowo co potwierdziła przyjmując i zatwierdzając wniosek rozliczeniowy.<br>• W ramach projektu zmodernizowano infrastrukturę informatyczną, stworzono system zasilania awaryjnego oraz wprowadzono SZBI urzędu.<br>• Audyt zgodności z wymaganiami rozporządzenia KRI zakończył się wynikiem pozytywnym. | |
| 10. | Urząd Gminy Świerklany | negatywna | • Podniesiony został poziom ogólnej wiedzy z zakresu bezpieczeństwa informacji kierownictwa, kadry urzędu oraz podległych jednostek,<br>• Urząd opracował i przekazał do NASK 10 Ankiet Dojrzałości Cyberbezpieczeństwa dotyczących Urzędu i dziewięciu podległych jednostek objętych projektem.<br>Stwierdzone stany prawidłowe nie miały decydującego wpływu na ocenę. | • Dotychczas nie zakupiono lub nie oddano w pełni do użytku wszystkich zaplanowanych z punktu widzenia zarządzania ryzykiem cyberbezpieczeństwa rozwiązań informatycznych, środków technicznych (serwerów , 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.<br>• Nie udało się przeszkolić pracowników IT Urzędu, kluczowych z punktu widzenia systemu zarządzania bezpieczeństwem informacji oraz wdrażanych rozwiązań technicznych i informatycznych, przeprowadzić edukacji phishingowej pracowników urzędu i wdrożyć rozwiązania do weryfikacji dwuetapowej.<br>• 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 niepowodzenia realizacji celu Projektu jakim jest kompleksowe zwiększenie poziomu bezpieczeństwa informacji jednostki samorządu terytorialnego.<br>Ponadto zidentyfikowano nieprawidłowości, takie jak:<br>• nieprzekazanie do NASK 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;<br>• nieuzasadnione opóźnienie odbioru I etapu przedmiotu umowy z 15 grudnia 2023 r. na wykonanie usługi doradczej w ramach Projektu;<br>• udzielenie w dniu 31 października 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 oraz nierzetelna realizacja i odbiór przedmiotu tego zamówienia; |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| | | | | • naruszenie postanowień Wytycznych dotyczących kwalifikowalności wydatków na lata 2021–2027 Ministra Funduszy i Polityki Regionalnej z 18 listopada 2022 r. i obowiązującego w Urzędzie Regulaminu udzielania zamówień publicznych o wartości szacunkowej nieprzekraczającej kwoty 130 000 zł podczas ustalania wartości szacunkowej zamówienia publicznego na przeprowadzenie szkolenia pracowników Urzędu i jednostek podległych w zakresie bezpieczeństwa informacji oraz w trakcie prowadzenia tego postępowania;<br>• wdrożenie w dniu 24 lipca 2023 r. Polityki Bezpieczeństwa Teleinformatycznego w urzędzie, która zawierała postanowienia niezgodne z przepisami rozporządzenia KRI oraz nierzetelne postanowienia i zapisy;<br>• 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;<br>• nierzetelną, niezgodną z postanowieniami §11 umowy grantowej realizację obowiązków w zakresie informowania i promowania dofinansowania uzyskanego na realizację Projektu. |
| 11. | Urząd Gminy w Wilkowicach | w formie opisowej | • W Urzędzie rozpoznawano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, które ujęto w: *Strategii Rozwoju Gminy Wilkowice do roku 2030,* audycie wewnętrznym *Bezpieczeństwo informacji w 2023 r.*, oraz w analizie ryzka przeprowadzonej w 2023 r. na poziomie zidentyfikowanych ryzyk w obszarze przetwarzania i ochrony danych osobowych.<br>• Gmina we wniosku o przyznanie grantu nie określiła wskaźników produktu i rezultatu, wniosek ten został zaakceptowany przez CPPC. W trakcie kontroli urząd wskazał jakie wskaźniki rezultatu planuje rozliczyć.<br>• Gmina przekazała *Ankietę Dojrzałości Cyberbezpieczeństwa* do NASK z zachowaniem terminu i formy określonej w umowie o powierzenie grantu, w ramach której przyznano dofinansowanie na realizację projektu pn. *Cyberbezpieczny Urząd Gminy w Wilkowicach*.<br>• Poniesione wydatki zostały zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o przyznanie grantu. | Stwierdzone nieprawidłowości dotyczyły:<br>• nieustanowienia i niewdrożenia kompletnego SZBI, o którym mowa w §19 ust. 1 w związku z ust. 3 rozporządzenia KRI;<br>• niewypełnienia obowiązku określonego w § 19 ust. 2 pkt 14 rozporządzenia KRI tj. zapewnienia okresowego audytu wewnętrznego;<br>• braku analizy ryzyka w 2024 r. wymaganej zarządzeniem wewnętrznym urzędu;<br>• niestosowania procedury przyznawania uprawnień w systemach informatycznych w zakresie ich przydziału do korzystania z zasobów sprzętowych, co było niezgodne z § 15 ust. 1 rozporządzenia KRI;<br>• zainstalowania na serwerze przeznaczonym do zapewnienia bezpieczeństwa informatycznego innej aplikacji dziedzinowej, co było niezgodne z § 15 ust. 1 rozporządzenia KRI. |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| 12. | Starostwo Powiatowe w Ostrowcu Świętokrzyskim | w formie opisowej | • Starostwo realizowało Projekt zgodnie z zapisami umowy o powierzenie grantu.<br>• Starostwo terminowo przekazało, za pośrednictwem ePUAP uzupełnione Ankiety Dojrzałości Cyberbezpieczeństwa.<br>• Zrealizowane w ramach Projektu zakupy zostały dokonane zgodnie z §4 ust. 1 pkt 5 umowy o udzielenie grantu. | • W Starostwie nie było opracowanego i wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji, w rozumieniu § 19 ust. 1 rozporządzenia KRI.<br>• W 2023 r. nie przeprowadzono audytu z zakresu bezpieczeństwa informacji, pomimo wymogu z § 20 ust. 2 pkt 14 rozporządzenia KRI. |
| 13. | Urząd Gminy Brody | w formie opisowej | • W Gminie podejmowano działania informacyjne dotyczące Projektu, tj. oznaczano znakiem Unii Europejskiej, barwami Rzeczypospolitej Polskiej i znakiem Funduszy Europejskich. | • Pomimo, że obowiązek opracowania, ustanowienia i wdrożenia SZBI wynikał z §20 ust. 1 rozporządzenia KRI z 12 kwietnia 2012 r., system ten został wprowadzony w gminie dopiero w dniu 18 lutego 2025 r.<br>• W okresie objętym kontrolą Wójt nie przeprowadził obowiązkowego corocznego audytu w zakresie bezpieczeństwa informacji. |
| 14. | Urząd Gminy i Miasta w Chęcinach | w formie opisowej | • Podczas realizacji grantu zapewniono stabilną i kompetentną obsadę kadrową. Terminowo przekazano do NASK Ankietę Dojrzałości Cyberbezpieczeństwa.<br>• Zapewniono poinformowanie opinii publicznej o fakcie otrzymania dofinansowania na realizację projektu.<br>• Poniesione wydatki zostały. zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o przyznanie grantu. | • Nie opracowano i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji.<br>• Nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. |
| 15. | Urząd Miasta i Gminy w Chmielniku | w formie opisowej | • Terminowo przekazano do NASK Ankietę Dojrzałości Cyberbezpieczeństwa.<br>• Poniesione wydatki zostały. zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o przyznanie grantu.<br>• Urząd prowadził wyodrębnioną ewidencję księgową oraz posiadał wyodrębniony rachunek bankowy umożliwiający identyfikację wszystkich transakcji oraz poszczególnych operacji bankowych związanych z Projektem. | • Urząd nie przeprowadził w 2024 r. obowiązkowego, corocznego audytu z zakresu bezpieczeństwa informacji. |
| 16. | Starostwo Powiatowe w Kamiennej Górze | w formie opisowej | • Zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu.<br>• Przeprowadzano wymagane okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji. | • System Zarządzania Bezpieczeństwem Informacji nie spełniał wymogów § 19 ust. 1 rozporządzenia KRI.<br>• Nie sporządzano wniosków o odebranie pracownikom uprawnień w systemach informatycznych.<br>• Nie zapewniono aktualności „Planu postępowań o udzielenie zamówień na 2025 r.”, co było niezgodne z art. 23 ust. 4 ustawy z 11 września 2019 r. – Prawo zamówień publicznych. |
| 17. | Urząd Miasta i Gminy w Bystrzycy Kłodzkiej | w formie opisowej | • Zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu.<br>• Terminowo przekazano do NASK Ankietę Dojrzałości Cyberbezpieczeństwa.<br>• Wydatki te zrealizowano zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we wniosku o przyznanie grantu. | • W 2023 r. nie przeprowadzono w urzędzie okresowego audytu z zakresu bezpieczeństwa informacji. |

| Lp. | Nazwa jednostki kontrolowanej | Ocena kontrolowanej działalności*/ | Stany mające wpływ na wydaną ocenę: | |
|---|---|---|---|---|
| | | | prawidłowe | nieprawidłowe |
| 18. | Urząd Miasta i Gminy w Górze | w formie opisowej | • Zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu.<br>• Terminowo przekazano do NASK Ankietę Dojrzałości Cyberbezpieczeństwa.<br>• Urząd posiadał ustanowiony System Zarządzania Bezpieczeństwem Informacji. | • Urząd nie zabezpieczył właściwie interesów zamawiającego w jednym z prowadzonych postępowań o zamówienie publiczne, nie formułując wymogu posiadania przez wykonawców/oferentów dwuletniego doświadczenia w przygotowaniu i przeprowadzeniu szkoleń.<br>• Brak było adekwatnych zabezpieczeń pomieszczenia serwerowni.<br>• Nie odebrano uprawnień do systemów informatycznych osobom, które zakończyły pracę w urzędzie. |
| 19. | Urząd Gminy Kłodzko | w formie opisowej | • Zapewniono stabilną i kompetentną obsadę kadrową zaangażowaną w nadzór i realizację Projektu.<br>• Terminowo przekazano do NASK Ankietę Dojrzałości Cyberbezpieczeństwa.<br>• Urząd zaktualizował SZBI, który spełnił wymogi § 19 ust. 1 rozporządzenia KRI.<br>• Prowadzono okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji. | • Urząd nie zabezpieczył właściwie swoich interesów w jednym z prowadzonych postępowań, nie formułując wymogu posiadania przez wykonawców/oferentów dwuletniego doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących oraz wzmacniających świadomość cyberzagrożeń, tj. wymogu dla uznania wydatków za kwalifikowalne wynikającego z § 4 pkt 7 ppkt d Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” , co było działaniem nierzetelnym.<br>• Brak było adekwatnych zabezpieczeń pomieszczenia serwerowni.<br>• Nieprawidłowe ustawienie monitorów w Biurze Obsługi Mieszkańców, co naruszało § 19 ust. 2 pkt 7 rozporządzenia KRI |

*/ pozytywna/negatywna/w formie opisowej

## 6.2. ANALIZA STANU PRAWNEGO I UWARUNKOWAŃ ORGANIZACYJNO-EKONOMICZNYCH

**Zasady realizacji projektów grantowych**

Zasady realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2021–2027, podmioty uczestniczące w realizacji tych programów i tej polityki oraz tryb współpracy między nimi, reguluje ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (dalej: ustawa wdrożeniowa)[89].

Art. 38 ustawy wdrożeniowej stanowi, że cele programu są osiągane przez realizację projektów objętych dofinansowaniem. Projekt to przedsięwzięcie zmierzające do osiągnięcia założonego celu określonego wskaźnikami, z określonym początkiem i końcem realizacji, zgłoszone do objęcia albo objęte finansowaniem UE jednego z funduszy strukturalnych, Funduszu Spójności albo Funduszu na rzecz Sprawiedliwej Transformacji w ramach programu (art. 2 pkt 22 ustawy wdrożeniowej).

Zgodnie z art. 41 ust. 1 ustawy wdrożeniowej w ramach programów mogą być realizowane projekty grantowe. Projektem grantowym jest projekt, którego beneficjent udziela grantów na realizację zadań służących osiągnięciu celu tego projektu przez grantobiorców. grantobiorcą jest podmiot publiczny albo prywatny, inny niż beneficjent projektu grantowego albo partner projektu partnerskiego, wybrany w drodze otwartego naboru ogłoszonego przez beneficjenta projektu grantowego w ramach realizacji projektu grantowego. Grantobiorcą nie może być podmiot wykluczony z możliwości otrzymania dofinansowania na podstawie przepisów odrębnych (art. 41 ust. 3–4). Zgodnie z art. 41 ust. 5 ustawy wdrożeniowej, grantem są środki finansowe programu, które beneficjent projektu grantowego przekazał grantobiorcy na realizację zadań, o których mowa w ust. 2. Wartość grantu przekazanego grantobiorcy nie może przekroczyć równowartości w złotych 200 000 euro (art. 41 ust. 6).

Stosownie do art. 41 ust. 7 ustawy wdrożeniowej, umowa o powierzenie grantu zawierana między beneficjentem projektu grantowego a grantobiorcą określa w szczególności:

1) cel projektu grantowego i zadania grantobiorcy objęte grantem;
2) kwotę grantu i wkładu własnego grantobiorcy;
3) warunki przekazania i rozliczenia grantu, w tym warunki rozliczania wydatków przez grantobiorcę;
4) zobowiązanie do zwrotu grantu w przypadku wykorzystania go niezgodnie z celami projektu grantowego;
5) zobowiązanie do poddania się kontrolom lub audytom prowadzonym przez beneficjenta projektu grantowego lub uprawnione podmioty, o których mowa w art. 25 ust. 1 i 2.

Beneficjent projektu grantowego odpowiada w szczególności za (art. 41 ust. 8):

1) realizację projektu grantowego zgodnie z założonym celem;
2) przygotowanie i przekazanie właściwej instytucji propozycji kryteriów wyboru grantobiorców;

[89] Dz.U. poz. 1079, ze zm.

3) dokonywanie wyboru grantobiorców w oparciu o określone kryteria, z uwzględnieniem zasady przejrzystości, rzetelności, bezstronności i równego traktowania podmiotów;
4) zawieranie z grantobiorcami umów o powierzenie grantu;
5) rozliczanie wydatków poniesionych przez grantobiorców;
6) monitorowanie realizacji zadań przez grantobiorców;
7) kontrolę realizacji zadań przez grantobiorców;
8) odzyskiwanie grantów w przypadku ich wykorzystania niezgodnie z umową o powierzenie grantu.

W przypadku gdy projekt grantowy jest jednocześnie projektem partnerskim, beneficjent może powierzyć partnerom realizację części zadań związanych z wyborem grantobiorców (art. 41 ust. 9).

Projekt partnerski został określony w art. 39 ust. 1 ustawy wdrożeniowej. Stanowi on, że w celu wspólnej realizacji projektu, w zakresie określonym przez instytucję zarządzającą krajowym programem albo instytucję zarządzającą regionalnym programem, może zostać utworzone partnerstwo przez podmioty wnoszące do projektu zasoby ludzkie, organizacyjne, techniczne lub finansowe, realizujące wspólnie projekt, zwany dalej projektem partnerskim, na warunkach określonych w porozumieniu albo umowie o partnerstwie.

Zgodnie z art. 41 ust. 10 ustawy wdrożeniowej, właściwa instytucja zatwierdza procedury dotyczące realizacji projektu grantowego opracowane przez beneficjenta projektu grantowego.

**Bezpieczeństwo informacji**

Podstawowe wymagania w zakresie bezpieczeństwa informacji w jednostkach samorządu terytorialnego określają:

1) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[90],
2) obowiązujące od 23 maja 2024 r. 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[91]. Wcześniejsze rozporządzenie 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[92] obowiązywało do 22 maja 2024 r.
3) ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa[93].

Wymagania dodatkowe znajdują się także w przepisach szczególnych, dotyczących danej dziedziny, np. rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia

[90] Dz. U. z 2024 r. poz. 1557, ze zm.
[91] Dz. U. poz. 773.
[92] Dz. U. z 2017 r. poz. 2247.
[93] Dz. U. z 2024 r. poz. 1077, ze zm.

dyrektyw 95/46/WE[94], tzw. RODO, a także ustawie z dnia 29 września 1994 r. o rachunkowości[95], ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[96], ustawie z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej[97], ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[98] (itp.), można znaleźć przepisy odnoszące się do bezpieczeństwa informacji w danym obszarze.

Zgodnie z art. 13 ust. 1 ustawy o informatyzacji, podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności.

Na podstawie upoważnienia zawartego w art. 18 ustawy o informatyzacji zostało wydane, obowiązujące od 23 maja 2024 r., 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.

W myśl § 15 ust. 1 rozporządzenia KRI, systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Zgodnie z § 19 ust. 1 rozporządzenia KRI, podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań wymienionych w § 19 ust. 2 obowiązującego rozporządzenia KRI w zakresie:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

---

94 Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.
95 Dz. U. z 2023 r. poz. 120, ze zm.
96 Dz. U. z 2022 r. poz. 902.
97 Dz. U. z 2024 r. poz. 152, ze zm.
98 Dz. U. z 2024 r. poz. 1513, ze zm.

4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;

6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

   a. zagrożenia bezpieczeństwa informacji,
   b. skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

   a. monitorowanie dostępu do informacji,
   b. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c. zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

   a. dbałości o aktualizację oprogramowania,
   b. minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c. ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d. stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e. zapewnieniu bezpieczeństwa plików systemowych,
   f. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Zgodnie z § 19 ust. 3 obowiązującego rozporządzenia KRI, obowiązki, o których mowa w § 19 ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem.

Do 22 maja 2024 r. obowiązywało rozporządzenie 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[99], w którym obowiązki dotyczące opracowania, ustanowienia i wdrożenia SZBI były określone w § 20 w sposób tożsamy jak w § 19 obowiązującego rozporządzenia KRI.

**Ochrona danych osobowych w kontekście zapewnienia cyberbezpieczeństwa**

Od 25 maja 2018 r. obowiązuje unijne ogólne rozporządzenie o ochronie danych RODO.

W pkt 49 preambuły do RODO określono, iż przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy. Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu "odmowa usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej.

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

Bezpieczeństwo przetwarzania danych osobowych zostało uregulowane w art. 32 RODO. Zgodnie z ust. 1 niniejszego artykułu, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający mają obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 ust. 1 RODO).

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 32 ust. 2 RODO).

Zgodnie z art. 37 ust. 1 lit. a RODO, w przypadku gdy przetwarzania dokonują organ lub podmiot publiczny, administrator i podmiot przetwarzający wyznaczają zawsze inspektora ochrony danych. Status inspektora ochrony danych określa art. 38 RODO. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Zgodnie z art. 38 ust. 6 RODO inspektor ochrony danych może wykonywać inne obowiązki, jednak najwyższe kierownictwo zapewnia by takie zadania i obowiązki nie powodowały konfliktu interesów.

**Ustawa o samorządzie gminnym**

W myśl art. 6 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym[100] (dalej: u.s.g.), do zakresu działania gminy należą wszystkie sprawy publiczne o znaczeniu lokalnym, niezastrzeżone ustawami na rzecz innych podmiotów. Art. 7 ust. 1 u.s.g. wymienia zadania własne gminy, wskazując, że zaspokajanie zbiorowych potrzeb wspólnoty należy do zadań własnych gminy. Organem wykonawczym gminy jest wójt/burmistrz/prezydent (art. 26 u.s.g.). Zadania wójta/burmistrza/prezydenta określa art. 30 u.s.g. Zgodnie z tym przepisem, wójt/burmistrz/prezydent wykonuje uchwały rady gminy i zadania gminy określone przepisami prawa. Do jego zadań należy w szczególności:

1) przygotowywanie projektów uchwał rady gminy;
2) opracowywanie programów rozwoju w trybie określonym w przepisach o zasadach prowadzenia polityki rozwoju;
3) określanie sposobu wykonywania uchwał;
4) gospodarowanie mieniem komunalnym;
5) wykonywanie budżetu;
6) zatrudnianie i zwalnianie kierowników gminnych jednostek organizacyjnych.

Wójt/burmistrz/prezydent kieruje bieżącymi sprawami gminy oraz reprezentuje ją na zewnątrz. Zadania wykonuje przy pomocy urzędu gminy, którego jest kierownikiem (art. 33 ust. 1 i 3 u.s.g.).

**Ustawa o samorządzie powiatowym**

W art. 4 ust. 1 w pkt 1–23 ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym[101] (dalej: u.s.p.) wymienione zostały zadania publiczne o charakterze ponadgminnym wykonywane przez powiat. Ustawy mogą określać inne zadania powiatu (art. 4 ust. 3 u.s.p.), a także mogą określać niektóre sprawy należące do zakresu działania powiatu jako zadania z zakresu administracji rządowej wykonywane przez powiat (art. 4 ust. 4 u.s.p.).

Organem wykonawczym powiatu jest zarząd powiatu (art. 26 ust. 1 u.s.p.). Zgodnie z art. 33 u.s.p., zarząd wykonuje zadania powiatu przy pomocy starostwa powiatowego oraz jednostek organizacyjnych powiatu, w tym powiatowego urzędu pracy. Starosta organizuje pracę zarządu powiatu i starostwa powiatowego, kieruje bieżącymi sprawami powiatu oraz reprezentuje powiat na zewnątrz (art. 34 ust. 1 u.s.p.). Stosownie do art. 35 ust. 1 u.s.p., organizację i zasady funkcjonowania starostwa powiatowego określa regulamin organizacyjny. Starosta jest kierownikiem starostwa powiatowego oraz zwierzchnikiem służbowym pracowników starostwa i kierowników jednostek organizacyjnych powiatu oraz zwierzchnikiem powiatowych służb, inspekcji i straży (art. 35 ust. 2 u.s.p.).

Zgodnie z art. 92 ust. 1 u.s.p., funkcje organów powiatu w miastach na prawach powiatu sprawuje rada miasta i prezydent miasta. Stosownie do art. 92 ust. 2 u.s.p., miasto na prawach powiatu jest gminą wykonującą zadania powiatu na zasadach określonych w ustawie o powiatach. Ustrój i działania organów miasta na prawach powiatu, w tym nazwę, skład, liczebność oraz ich powoływanie i odwoływanie, a także zasady sprawowania nadzoru określa ustawa o samorządzie gminnym (art. 92 ust. 3 u.s.p.).

---

[100] Dz. U. z 2025 r. poz. 1153.
[101] Dz. U. z 2024 r. poz. 107, ze zm.

**Podstawowe zadania i status prawny CPPC i NASK**

**Centrum Projektów Polska Cyfrowa** jest państwową jednostką budżetową podległą ministrowi właściwemu do spraw informatyzacji, pełniącą funkcję Instytucji Pośredniczącej Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027. Realizuje zadania związane z wdrażaniem programów i projektów współfinansowanych ze środków pochodzących z budżetu Unii Europejskiej zapewniających między innymi wsparcie w ramach polityki spójności, środków pochodzących z bezzwrotnej pomocy zagranicznej, środków pochodzących z budżetu państwa i funduszy celowych. Dodatkowo CPPC zajmuje się profesjonalnym poradnictwem wspomagającym beneficjentów w procesie zarządzania projektami Unii Europejskiej. Umożliwia organizacjom, instytucjom i firmom realizację projektów finansowanych z funduszy Unii Europejskiej, które koncentrują się przede wszystkim na rozwoju e-usług, wsparciu kompetencji cyfrowych i ułatwieniu dostępu do internetu dla każdego obywatela. CPPC jest beneficjentem projektu grantowego w rozumieniu art. 41 ust. 8 pkt 1 ustawy wdrożeniowej.

CPPC jest partnerem wiodącym w ramach *Umowy o partnerstwie w celu wspólnej realizacji projektu pn. „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027*. Zgodnie z § 4 ww. umowy:

1. Partner wiodący ma prawo do dofinansowania odpowiadającego jego wkładowi do Projektu i realizowanej części Projektu na zasadach i w wysokości wynikających z Decyzji o dofinansowanie.

2. Partner wiodący zobowiązuje się do złożenia Wniosku o dofinansowanie Projektu.

3. Partner wiodący odpowiada za prawidłową, rzetelną i terminową realizację uprawnień i obowiązków wynikających z Decyzji o dofinansowaniu Projektu w relacji z Instytucją Pośredniczącą FERC.

4. W zakresie niezbędnym do realizacji Umowy oraz Decyzji o dofinansowaniu Projektu, Partner wiodący w szczególności:

1) informuje Partnera o wszelkich zdarzeniach istotnych, w tym stanowiskach Instytucji Pośredniczącej FERC, zagrożeniach i nieprawidłowościach, mogących wpłynąć na prawidłowe wykonanie Umowy i Decyzji o dofinansowaniu;
2) koordynuje i zapewnia spójność działań Stron w trakcie realizacji Projektu;
3) gromadzi informacje o realizacji Projektu przez Partnera;
4) jest zobowiązany do poinformowania Partnera o każdej zmianie w Decyzji o dofinansowaniu;
5) informuje Partnera o planowanych zmianach zakresu Projektu i uzgadnia te zmiany z Partnerem;
6) reprezentuje Partnera w trakcie realizacji Projektu przed Instytucją Pośredniczącą FERC, składając oświadczenia po wcześniejszym uzyskaniu zgody Partnera;
7) koordynuje (w tym monitoruje i nadzoruje) prawidłowość działań Partnera przy realizacji zadań zawartych w Projekcie oraz wspiera Partnera w realizacji powierzonych zadań;

8) zapewnia niezbędne know-how do realizacji zadań zaplanowanych w Projekcie oraz umożliwia efektywne rozwiązywanie problemów związanych z koordynacją Projektu;
9) przygotowuje niezbędną dokumentację aplikacyjną oraz konkursową;
10) przedkłada wnioski o płatność do Instytucji Pośredniczącej FERC celem rozliczenia wydatków w Projekcie oraz otrzymania środków na dofinansowanie zadań własnych i Partnera;
11) monitoruje wskaźniki zadeklarowane we Wniosku o dofinansowanie;
12) informuje Instytucję Pośredniczącą FERC o problemach w realizacji Projektu, w tym o zamiarze zaprzestania jego realizacji lub o zagrożeniu nieosiągnięcia zaplanowanych wskaźników określonych w zatwierdzonym Wniosku o dofinansowanie;
13) zapewnia zachowanie zasady równości szans i płci w ramach partnerstwa zgodnie z Wytycznymi dotyczącymi realizacji zasad równościowych w ramach funduszy unijnych na lata 2021–2027;
14) współpracuje z podmiotami zewnętrznymi, realizującymi badania ewaluacyjne na zlecenie Instytucji Zarządzającej FERC lub Instytucji Pośredniczącej FERC poprzez udzielanie każdorazowo na wniosek tych podmiotów dokumentów i informacji na temat realizacji Projektu, niezbędnych do przeprowadzenia badania ewaluacyjnego;
15) zawiera Umowy o powierzenie grantu;
16) realizuje zadania związane z promocją Projektu w sposób uzgodniony z Partnerem.

**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy** posiada osobowość prawną. NASK działa na podstawie:

1) ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2024 r. poz. 534);
2) rozporządzenia Rady Ministrów z dnia 7 czerwca 2017 r. w sprawie nadania Naukowej i Akademickiej Sieci Komputerowej statusu państwowego instytutu badawczego (Dz. U. poz. 1193);
3) rozporządzenia Rady Ministrów z dnia 26 stycznia 2018 r. w sprawie połączenia Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego i Instytutu Maszyn Matematycznych (Dz. U. poz. 271);
4) Statutu NASK, stanowiącym załącznik do uchwały nr 2/2025 Rady Naukowej NASK – PIB z dnia 9 stycznia 2025 r. w sprawie zmiany statutu NASK – PIB oraz wprowadzenia tekstu jednolitego, zatwierdzonej decyzją nr 1 Ministra Cyfryzacji z dnia 21 stycznia 2025 r. w sprawie zatwierdzenia zmian w statucie Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (Dz. Urz. Ministra Cyfryzacji, poz. 4).

Przedmiotem działania Instytutu jest prowadzenie badań naukowych i prac rozwojowych w zakresie telekomunikacji, teleinformatyki, informatyki, cyberbezpieczeństwa, funkcjonowania polskiego rejestru domen internetowych, społeczeństwa informacyjnego; przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki oraz wdrażanie wyników badań naukowych i prac rozwojowych w usługach świadczonych między innymi na potrzeby organów bezpieczeństwa i porządku publicznego, bezpieczeństwa państwa oraz bezpieczeństwa jednostek infrastruktury krytycznej.

NASK jest partnerem w ramach *Umowy o partnerstwie w celu wspólnej realizacji projektu pn. „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027*. Partner, w odniesieniu do realizowanej części Projektu, w myśl § 5 pkt 7 ww. umowy, zgodnie z postanowieniami Decyzji o dofinansowaniu, zobowiązany jest do:

1) organizacji naboru wniosków grantowych, w tym z wykorzystaniem narzędzi do składania wniosków aplikacyjnych przez podmioty aplikujące o grant;
2) udzielania odpowiedzi na pytania wnioskodawców podczas naboru wniosków grantowych;
3) przeprowadzenia oceny braków formalnych oraz oceny formalnej i merytorycznej wniosków złożonych przez grantobiorców, opracowania zestawienia wniosków zatwierdzonych do dofinansowania;
4) przekazania informacji o wynikach oceny do wnioskodawców, w tym listy dokumentów niezbędnych do podpisania umowy o powierzenie grantu dla podmiotów, których projekty zostały wybrane do dofinansowania;
5) przeprowadzenia procesu zebrania i analizy poprawności dokumentacji niezbędnej do zawarcia Umów o powierzenie grantu oraz realizacji zadań związanych z zawarciem Umów o powierzenie grantów;
6) przekazania przygotowanych i kompletnych Umów o powierzenie grantu do zawarcia przez Partnera wiodącego Projektu;
7) rozliczania Umów o powierzenie grantu, bieżący kontakt z grantobiorcami, w tym monitoring i sprawozdawczość z wykorzystaniem narzędzi do raportowania i rozliczania grantów;
8) współpracy przy organizacji działań informacyjno-promocyjnych;
9) wypłaty grantów grantobiorcom;
10) współpracy z Partnerem wiodącym Projektu w przypadku wykorzystania grantów niezgodnie z celami Projektu;
11) raportowania do Partnera wiodącego o stanie realizacji prac w zakresie realizowanych zadań w Projekcie;
12) systematycznego monitorowania przebiegu realizacji powierzonej mu części Projektu oraz niezwłoczne informowanie Partnera wiodącego Projektu o zaistniałych nieprawidłowościach, przewidywanych opóźnieniach i innych ryzykach w realizacji;

13) przeprowadzania kontroli realizacji Umów o powierzenie grantu;

14) osiągnięcia i utrzymania celów powierzonej mu części Projektu po zakończeniu jej realizacji w całym okresie trwałości Projektu, zgodnie z Umową, o ile będzie to miało zastosowanie;

15) przechowywania i archiwizowania Dokumentacji Projektu powierzonej mu części Projektu;

16) udostępniania Dokumentacji Projektu upoważnionym do jej otrzymania lub analizy organom i instytucjom;

17) udzielania wyczerpujących, pisemnych odpowiedzi i wyjaśnień Partnerowi wiodącemu Projektu w razie jakichkolwiek pytań, wątpliwości lub zastrzeżeń dotyczących powierzonej mu części Projektu, w terminie wskazanym przez Partnera wiodącego Projektu, umożliwiającym przygotowanie dokumentów przez Partnera;

18) poddania się kontroli w zakresie prawidłowej realizacji powierzonej mu części Projektu prowadzonej przez Partnera wiodącego Projektu, Instytucję Pośredniczącą FERC, Instytucję Zarządzającą FERC, Instytucję Audytową, Komisję Europejską, Europejski Trybunał Obrachunkowy oraz inne podmioty uprawnione do przeprowadzania kontroli na podstawie odrębnych przepisów lub upoważnień, w tym:

    a) umożliwienia wglądu do Dokumentacji Projektu, w tym wglądu do dokumentów księgowych, związanych z realizacją zadań bezpośrednio przez niego lub jego Wykonawców,

    b) umożliwienia przeprowadzenia czynności kontrolnych, w tym dostępu do swojej siedziby i miejsca realizacji zadań bezpośrednio przez niego lub jego Wykonawców,

    c) zobowiązania podmiotów realizujących powierzoną mu część Projektu o obowiązku do poddania się czynnościom kontrolnym;

19) wdrożenia zaleceń oraz działań naprawczych wskazanych przez Partnera wiodącego Projektu zakresie i w odpowiednich terminach przez Partnera wiodącego wskazanych;

20) nienaruszania zasady zakazu podwójnego finansowania, oznaczającej niedozwolone ponowne zrefundowanie całkowite lub częściowe danego wydatku ze środków publicznych (wspólnotowych lub krajowych);

21) powstrzymania się od zawierania jakichkolwiek umów czy porozumień, które w sposób bezpośredni uniemożliwiałyby lub istotnie utrudniły realizację Umowy i Decyzji o dofinansowaniu;

22) osiągnięcia wartości docelowych wskaźników produktu i rezultatu powierzonej mu części Projektu, zgodnie z Wnioskiem o dofinansowanie Projektu i Decyzją o dofinansowaniu oraz Wytycznymi;

23) pozostawania w gotowości do realizacji powierzonej mu części Projektu pod względem zgodności z przepisami prawa przed dniem podpisania przez Partnera wiodącego Projektu Decyzji o dofinansowanie Projektu.

**Analiza uwarunkowań ekonomicznych i organizacyjnych**

W ostatnich latach obserwowana jest bardzo duża dynamika wzrostu liczby ataków i incydentów w obszarze cyberbezpieczeństwa. Badanie bezpieczeństwa stron internetowych samorządów przeprowadzone przez zespół w NASK w 2020 r. w ponad połowie zbadanych witryn ujawniło podatności na ataki, w tym poważne błędy. Są one coraz częściej zauważane i wykorzystywane przez cyberprzestępców. W drugiej połowie 2022 r. odnotowano wyraźny trend wzrostowy w liczbie zarejestrowanych przez NASK zgłoszeń. Najwyższą wartość odnotowano w grudniu 2022 r. – niemal 85,2 tys., co w porównaniu z analogicznym miesiącem 2021 r. oznacza ponad czterokrotny wzrost. Pokazuje to, jak pilne jest wzmocnienie odporności systemów IT wykorzystywanych w jst, a także stworzenie systemowego wsparcia w reagowaniu na incydenty.

Projekt Cyberbezpieczny Samorząd jest realizowany w ramach Funduszy Europejskich na rozwój cyfrowy 2021–2027 Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Projekt realizowany jest przez Centrum Projektów Polska Cyfrowa (Beneficjent Projektu) w Partnerstwie z NASK Państwowym Instytutem Badawczym. Zakres zadań NASK został określony w umowie o partnerstwie.

Celem kontrolowanego projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Realizacja Projektu poprzez wsparcie grantowe jednostek samorządowych, ma przyczynić się do:

- wdrożenia lub aktualizacji w jst polityk bezpieczeństwa informacji (SZBI),
- wdrożenia w jst środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w jst mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu jst kluczowego z punktu widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w jst audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

W ramach Projektu przewidziano dla jst wsparcie w formie grantu. Dla gmin przewidziano dofinansowanie w przedziale od 200 000 zł do 850 000 zł, a dla powiatów przewidziano środki do 850 000 zł.

Wnioski o granty złożone przez samorządy zakładają realizację działań w 3 kluczowych obszarach mających wpływ na cyberbezpieczeństwo: techniczny (ok. 1,2 mld zł) – infrastruktura sprzętowa i oprogramowanie oraz usługi wdrożeniowe; organizacyjny (ok. 183 mln zł) – procedury, audyty, certyfikaty, System Zarządzania Bezpieczeństwem Informacji itp. I kompetencyjny (ok. 105 mln zł) – szkolenia pracowników. Czas realizacji grantu wynosi 24 miesiące od dnia wejścia w życie umowy na realizację grantu, jednak nie dłużej niż do 30 czerwca 2026 r. Dofinansowanie będzie wypłacane w 3 transzach: 30 proc. – 30 proc. – 40 proc.

Szczegółowe zasady powierzania grantów w ramach Projektu określono w regulaminie Konkursu Grantowego. Regulamin określa m.in.: nabór wniosków o przyznanie grantów oraz sposób i zasady oceny wniosków o przyznanie grantu (§5); zawarcie umowy o powierzenie grantu (§6);

zasady finansowania, w szczególności jakie wydatki zalicza się do wydatków kwalifikowanych w ramach grantu, a jakie do wydatków niekwalifikowalnych (§4).

Zgodnie z § 4 ust. 7 Regulaminu, do wydatków kwalifikowanych w ramach grantu zalicza się w szczególności:

1) środki trwałe/dostawy:

sprzęt informatyczny i urządzenia bezpieczeństwa:

- Firewall sieciowy;
- WAF (Web Application Firewall);
- SIEM (Security Information and Event Management);
- UTM (Unified Threat Management);
- IPS (Intrusion Prevention System);
- IDS (Intrusion Detection System);
- VPN (Virtual Private Network);
- NAC (Network Access Control);
- proxy sprzętowe;
- serwer;
- serwer do wykonywania kopii zapasowych;
- macierz dyskowa;
- dyski twarde do macierzy dyskowej;
- Network Attached Storage (NAS);
- Storage Area Network (SAN);
- Web Secure Gateway;
- Email Secure Gateway;
- generator prądu;
- UPS;
- ochrona AntyDDoS;
- zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X;

2) wartości niematerialne i prawne, w szczególności:

wartości niematerialne i prawne, takie jak: autorskie prawa majątkowe lub licencje, w tym subskrypcyjne, na korzystanie z oprogramowania, w tym systemowego o przewidywanym okresie używania dłuższym niż rok; prawa do dokumentacji, raportów, opracowań. Koszty kwalifikowane będą tylko w okresie realizacji Projektu:

- oprogramowanie antywirusowe;
- oprogramowanie typu EDR (Endpoint Detection and Response);
- oprogramowanie typu XDR (Extended Detection and Response);
- oprogramowanie do wykonywania kopii zapasowych;
- oprogramowanie antyspamowe;
- oprogramowanie WAF (Web Application Firewall);
- oprogramowanie SIEM (Security Information and Event Management);
- oprogramowanie Menadżera logów;
- oprogramowanie do zarządzania podatnościami;
- programowanie przeciwdziałającemu wyciekowi danych (DLP – Data Leak Prevention);
- oprogramowanie do zarządzania uprzywilejowanemu dostępowi (PAM – Privileged Access Management);

- oprogramowanie Web Secure Gateway;
- oprogramowanie Email Secure Gateway;
- oprogramowanie do zarządzania tożsamością i dostępem;
- oprogramowanie centralnego menadżera haseł;
- oprogramowanie do monitorowania infrastruktury informatycznej;
- oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych;
- oprogramowanie do badania podatności systemów informatycznych;
- oprogramowanie do badania podatności serwisów WWW;
- oprogramowanie do badania podatności w kodzie aplikacji;
- oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików;
- oprogramowanie do analizy po włamaniowej;
- oprogramowanie do ochrony przed ransomware;

3) usługi zewnętrzne, w szczególności:
   a) przygotowanie Projektu: sfinansowanie przygotowania Projektu opracowanego przez specjalistów/organizacje, w których osoba odpowiedzialna za przygotowania Projektu posiada stosowną wiedzę i m.in. 2 letnie doświadczenie we wnioskowanym zakresie oraz co najmniej 1 (jeden) certyfikat świadczący o posiadanej wiedzy w danym zakresie. Koszty będą kwalifikowane tylko w okresie realizacji projektu;
   b) usługi informatyczne. Pokrycie kosztów zwiększających poziom bezpieczeństwa informacji, tj. wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych tylko w okresie realizacji Projektu:
      - usługa poczty elektronicznej w chmurze obliczeniowej typu IaaS, SaaS, PaaS z elementami bezpieczeństwa;
      - usługa testowania bezpieczeństwa infrastruktury sieciowej;
      - usługa testowania bezpieczeństwa serwisów internetowych;
      - usługa testowania bezpieczeństwa aplikacji;
      - usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS w zakresie sandbox do badania bezpieczeństwa aplikacji oraz plików;
      - usługa w chmurze obliczeniowej typu IaaS, SaaS, PaaS dotycząca bezpieczeństwa sieciowego;
   c) usługi wspomagające realizację Projektu, w szczególności usługi doradcze podmiotów posiadających stosowne kwalifikacje i min. 2 letnim doświadczeniem w prowadzeniu projektów z obszaru cyberbezpieczeństwa oraz stosowne certyfikaty lub równoważne poświadczenia (np. Kwalifikację zawodową) potwierdzające możliwość wykonania zlecenia. Kwalifikowalność kosztów tylko w okresie realizacji Projektu;
   d) szkolenia: zakup i organizacja 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 szkoleń budujących i wzmacniających świadomość cyberzagrożeń.

Kwalifikowalność kosztów tylko w okresie realizacji Projektu; informacja i promocja: pokrycie kosztów przygotowania i wyprodukowania (drukowanych i elektronicznych) materiałów promocyjnych

i informacyjnych upowszechniających świadomość o zagrożeniach cybernetycznych, np.: sfinansowanie przygotowania newslettera dla pracowników; przygotowanie periodyku o cyberhigienie dla pracowników; materiałów budujących i wzmacniających świadomość o zagrożeniach cybernetycznych.

Zgodnie z § 4 ust. 7 Regulaminu, do wydatków niekwalifikowalnych w ramach Grantu zaliczają się:

1) do współfinansowania nie kwalifikują się wszelkie wydatki określone w podrozdziale 3.3. Katalogu wydatków kwalifikowanych II priorytetu programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027;
2) do współfinansowania nie kwalifikują się wszelkie wydatki na zakup, dostawę lub usługi, które nie służą bezpośrednio wsparciu cyberbezpieczeństwa w jst, w szczególności:
   a) komputery stacjonarne i przenośne;
   b) urządzenia mobilne tj. smartfony lub tablety;
   c) akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki, klawiatury, myszy);
   d) materiały eksploatacyjne;
   e) oprogramowanie biurowe, z wyłączeniem systemów operacyjnych niezbędnych do instalacji i utrzymania systemów bezpieczeństwa;
   f) szkolenia informatyczne niezwiązane z cyberbezpieczeństwem, np. szkolenia z obsługi oprogramowania biurowego;
   g) usługi dostępu do internetu, abonamenty telefoniczne.

Regulamin przewiduje, że okres realizacji wynosi maksymalnie 24 miesiące od dnia wejścia w życie umowy o powierzenie grantu, jednak nie później niż do 30 czerwca 2026 r. Dopuszcza się kwalifikowalność wydatków poniesionych w okresie od 1 czerwca 2023 r. do dnia zakończenia realizacji określonego w umowie o powierzenie grantu.

## 6.3. WYKAZ AKTÓW PRAWNYCH DOTYCZĄCYCH KONTROLOWANEJ DZIAŁALNOŚCI

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[102].
2. Ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027[103].
3. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym[104].
4. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym[105].
5. 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[106].
6. Rozporządzenie 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[107].
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektyw 95/46/WE[108].

[102] Dz. U. z 2024 r. poz. 1557, ze zm.
[103] Dz.U. poz. 1079, ze zm.
[104] Dz. U. z 2025 r. poz. 1153.
[105] Dz. U. z 2024 r. poz. 107, ze zm.
[106] Dz.U. poz. 773.
[107] Dz. U. z 2017 r. poz. 2247.
[108] Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.

## 6.4. WYKAZ PODMIOTÓW, KTÓRYM PRZEKAZANO INFORMACJĘ O WYNIKACH KONTROLI

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Przewodniczący Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
6. Przewodniczący Sejmowej Komisji do Spraw Kontroli Państwowej
7. Przewodniczący Sejmowej Komisji Samorządu Terytorialnego i Polityki Regionalnej
8. Przewodniczący Sejmowej Komisji do Spraw Unii Europejskiej
9. Przewodniczący Senackiej Komisji Samorządu Terytorialnego i Administracji Państwowej
10. Minister Cyfryzacji
11. Minister Funduszy i Polityki Regionalnej
12. Minister Spraw Wewnętrznych i Administracji
13. Szef Krajowej Administracji Skarbowej (Instytucja Audytowa)
14. Zarządy Województw
15. Prezydenci/Burmistrzowie/Wójtowie
16. Starostowie
17. Dyrektor Centrum Projektów Polska Cyfrowa