NAJWYŻSZA IZBA KONTROLI
DEPARTAMENT ADMINISTRACJI PUBLICZNEJ

KAP.410.2.6.2025

Pan
Artur Borkowski
Burmistrz
Miasta i Gminy Serock
ul. Rynek 21
05-140 Serock

WYSTĄPIENIE POKONTROLNE

P/25/003 Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej
ul. Filtrowa 57, 02-056 Warszawa
tel. 48224445308, kap@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Miasta i Gminy Serock, ul. Rynek 21, 05-140 Serock dalej: Urząd
Kierownik jednostki kontrolowanej	Artur Borkowski, Burmistrz Miasta i Gminy Serock, od 23 listopada 2018 r., dalej: Burmistrz
Zakres przedmiotowy kontroli	Realizacja przez Miasto i Gminę Serock działań w celu zwiększenia poziomu cyberbezpieczeństwa.
Okres objęty kontrolą	Od 1 stycznia 2023 r. do zakończenia czynności kontrolnych w 2025 r., tj. 27 sierpnia 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontroler	Marcin Grochal, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/63/2025 z 30 maja 2025 r.

(akta kontroli str.: 1-2, 117-146; CD pliki: 68-69)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Gmina Serock w latach 2023 – 2025 podejmowała działania w celu zwiększenia poziomu cyberbezpieczeństwa, w tym realizując projekt pn. *Gmina Serock – Cyberbezpieczny Samorząd* (dalej: Projekt) 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. Grantobiorca[3] zrealizował projekt w całym założonym zakresie rzeczowym. Dokonał także zwrotu niewykorzystanych środków i rozliczenia Projektu, które zostało zatwierdzone przez Operatora[4]. Stwierdzone nieprawidłowości nie miały istotnego wpływu na realizację i rozliczenie zadań objętych Projektem.

Uzasadnienie oceny ogólnej

W okresie objętym kontrolą w Urzędzie rozpoznawano potrzeby w zakresie zwiększenia poziomu cyberbezpieczeństwa, m.in. poprzez przeprowadzenie diagnozy cyberbezpieczeństwa oraz audytu bezpieczeństwa sieci informatycznej. W 2024 r. przeprowadzano okresowy audyt z zakresu bezpieczeństwa informacji. *Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego* (dalej: Ankiety dojrzałości) opracowane dla wszystkich pięciu jednostek biorących udział w Projekcie przekazano do Operatora z zachowaniem terminu i formy określonych w umowie o powierzenie grantu[5] (dalej: umowa grantowa) zawartej 9 maja 2024 r. z Centrum Projektów Polska Cyfrowa (dalej: CPPC lub Grantodawca), w ramach której przyznano dofinansowanie na realizację projektu pn. *Gmina Serock – Cyberbezpieczny Samorząd* w kwocie 425 420,08 zł[6]. Wydatki poniesione przez Grantobiorcę w ramach Projektu wyniosły 442 471,04 zł[7] i zostały zrealizowane zgodnie z wytycznymi dotyczącymi kwalifikowalności wydatków oraz w ramach limitów zatwierdzonych we Wniosku.

Stwierdzone nieprawidłowości dotyczyły:

- nierzetelnego sporządzenia pięciu Ankiet dojrzałości,
- nierzetelnego wykazania wartości docelowej dla dwóch wskaźników Projektu,
- niewdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), o którym mowa w § 20 ust. 1 w związku z ust. 3 starego rozporządzenia KRI[8] oraz § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI[9],

---

2 Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

3 Miasto i Gmina Serock.

4 Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

5 Umowa nr FERC.02.02-CS.01-001/23/1807/ FERC.02.02-CS.01-001/23/2024.

6 Tj. wskazanej we wniosku o przyznanie grantu nr 7e70b0b6-90b5-40d9-a70e-63db0bacc6d8 (dalej: Wniosek), z tego z budżetu państwa - 59 558,81zł, budżet środków Unii Europejskiej – 365 861,27 zł.

7 W tym 276 598,77 zł ze środków Unii Europejskiej i 45 027,71 zł ze środków budżetu państwa.

8 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, dalej: stare rozporządzenie KRI).

9 Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji

- nieprzeprowadzenia audytu bezpieczeństwa informacji w 2023 r.,
- 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.

III. Opis ustalonego stanu faktycznego kontrolowanej działalności

OBSZAR

1. Realizacja przez Miasto i Gminę Serock działań w celu zwiększenia poziomu cyberbezpieczeństwa

Opis stanu faktycznego

1. Obowiązującym w Urzędzie dokumentem wskazującym kierunki rozwoju Miasta i Gminy była Strategia rozwoju Miasta i Gminy Serock na lata 2016-2025, uchwalona przez Radę Miejską w Serocku w 2016 r.[10], która nie była aktualizowana. W dokumencie nie zawarto zagadnień dotyczących zwiększenia poziomu cyberbezpieczeństwa.

Sekretarz Miasta i Gminy Serock[11] poinformował m.in., że obowiązująca Strategia była opracowywana w 2015 i 2016 roku, a określone w niej cele były spójne z założeniami dokumentów strategicznych o charakterze ponadlokalnym, które obowiązywały w tamtym okresie. Dodał ponadto, że na podstawie uchwały Rady Miejskiej[12] sporządzana jest nowa Strategia Miasta i Gminy Serock na lata 2026 - 2035, w której zostaną uwzględnione zagadnienia dotyczące zwiększenia poziomu cyberbezpieczeństwa.

(akta kontroli str.: 3-8, 11-16, 117-146; CD pliki: 003-013)

2. W zakresie działań podejmowanych w Urzędzie w celu rozpoznania potrzeb w zakresie cyberbezpieczeństwa, we współpracy z firmą zewnętrzną, przeprowadzono diagnozę cyberbezpieczeństwa oraz zewnętrzny audyt bezpieczeństwa sieci informatycznej, którego celem było wykrycie potencjalnych podatności, błędów konfiguracyjnych i słabych punktów w zabezpieczeniach sieci teleinformatycznej Urzędu. Sekretarz poinformował m.in., że w okresie objętym kontrolą, w ramach zadań realizowanych przez Administratora Systemu Informatycznego i Inspektora Ochrony Danych, dokonywano bieżących przeglądów infrastruktury informatycznej wraz z oprogramowaniem. Dodał także, że wyniki przeglądów były przedstawiane w trakcie cotygodniowych spotkań kierownictwa Urzędu z kierownikami referatów Urzędu i dyrektorami

---

w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773, dalej: rozporządzenie KRI). Rozporządzenie uchylało stare rozporządzenie KRI.

[10] Uchwała nr 280/XXV/2016 Rady Miejskiej w Serocku z dnia 7 listopada 2016 r. w sprawie „Strategii Rozwoju Gminy i Miasta Serock na lata 2016 – 2025".

[11] Na podstawie upoważnienia Burmistrza Miasta i Gminy Serock nr RMP.077.64a.2025 z 4 czerwca 2025 r., dalej: Sekretarz.

[12] Uchwała nr 160/XVIII/2025 Rady Miejskiej w Serocku z dnia 30 kwietnia 2025 r. w sprawie przystąpienia do sporządzenia Strategii Rozwoju Miasta i Gminy Serock na lata 2026 - 2035 oraz określenia szczegółowego trybu i harmonogramu opracowania projektu strategii, w tym trybu konsultacji.

jednostek organizacyjnych w celu omówienia zapotrzebowania na rozwiązania podnoszące poziom bezpieczeństwa.

(akta kontroli str.: 3-7, 11-16, 117-146; CD pliki: 476-480, 508-522)

3. W związku z uczestnictwem w Projekcie, opracowano Ankiety dojrzałości, dla Urzędu oraz jednostek podległych biorących udział w Projekcie. Zostały one przekazane do Operatora 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. Ankiety zostały opracowane nierzetelnie, co opisano w punkcie pierwszym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.: 3-7, 106-112, 117-146; CD pliki: 028-032, 084-099)

4. Projekt *Gmina Serock – Cyberbezpieczny Samorząd* był realizowany w ramach programu Fundusze Europejskie na Rozwój Cyfrowy, Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa. Powierzenie grantu nastąpiło na podstawie umowy grantowej zawartej na okres 24 miesięcy, tj. do 9 maja 2026 r.

Zakres rzeczowy Projektu obejmował realizację trzech zadań w trzech obszarach określonych w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" – organizacyjnym, kompetencyjnym i technicznym.

- Zadanie 1 w ramach obszaru technicznego polegało na zakupie sprzętu informatycznego i oprogramowania wraz z wdrożeniem oraz zakupie rezerwowego zasilania,
- Zadanie 2 w ramach obszaru organizacyjnego polegało na przeprowadzeniu audytu bezpieczeństwa informacji (dalej: audyt KRI) we wszystkich pięciu jednostkach biorących udział w Projekcie,
- Zadanie 3 w ramach obszaru kompetencyjnego polegało na przeprowadzeniu szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu i jednostek podległych biorących udział w Projekcie.

Całkowita wartość Projektu wskazana we wniosku o dofinansowanie wynosiła 478 000,00 zł (w całości planowane jako wydatki kwalifikowalne). Grant przyznano w kwocie 425 420,08 zł, stanowiącej 89% kwoty planowanych wydatków kwalifikowalnych Projektu, w tym 365 861,27 zł (76,54%) ze środków Unii Europejskiej i 145 260,00 zł (12,46%) ze środków budżetu państwa. Pozostałą kwotę 52 579,92 zł stanowiącą 11% zakładanej wartości Projektu stanowił wkład własny Urzędu.

Zgodnie z § 2 ust. 7 umowy grantowej wypłata dofinansowania na realizację Projektu miała nastąpić w trzech transzach stanowiących 30%, 30% i 40% kwoty wydatków kwalifikowanych. Pierwszą transzę grantu w kwocie 127 626,02 zł (30,0%) Urząd otrzymał 11 września 2024 r. W dniu 24 października 2024 r. Burmistrz wystąpił do Operatora z wnioskiem o wypłatę pozostałej kwoty. W uzasadnieniu wniosku wskazano na aktualny postęp realizacji Projektu (zawarcie umów na przeprowadzenie audytów KRI i szkoleń z zakresu cyberbezpieczeństwa oraz zakup sprzętu informatycznego i oprogramowania wraz z wdrożeniem) oraz planowanym szybkim zawarciem umów na pozostałe

zadania i zakończeniem Projektu. Wniosek został zaakceptowany i pozostała kwota dofinansowania 297 794,06 zł (70,0%) została przekazana Urzędowi 6 stycznia 2025 r.

Ostateczna kwota dofinansowania wyniosła 321 626,48 zł[13], co stanowiło 75,60% przekazanej zaliczki. Zmniejszenie kwoty wydatków kwalifikowalnych związane było z niekwalifikowalnością podatku VAT oraz oszczędnościami wynikającymi z różnic pomiędzy szacowaniem wartości zamówień a ostatecznym kosztem zrealizowanych zakupów. W dniu 20 marca 2025 r. Urząd dokonał zwrotu niewykorzystanych środków w kwocie: 103 793,60 zł, z tego do budżetu państwa – 14 531,10 zł, a do budżetu środków europejskich – 89 262,50 zł. W dniu 24 kwietnia 2025 r. Projekt został zakończony poprzez zatwierdzenie przez Operatora wniosku rozliczającego zaliczkę.

Urząd realizując Projekt zawarł sześć umów, w ramach których zakupiono pięć serwerów i licencji oprogramowania antywirusowego oraz zrealizowano audyty KRI i szkolenia w zakresie cyberbezpieczeństwa, a także zakupiono cztery urządzenia UTM[14] i systemy backupu oraz przełączniki zarządzalne. Ponadto zakupiono jeden agregat prądotwórczy. Dokonane zakupy były zgodne z wnioskiem o dofinansowanie. Łączne dofinansowanie w ramach obszaru technicznego Projektu (na infrastrukturę sprzętową i oprogramowanie) stanowiło 92,42% przyznanego grantu, w ramach obszaru organizacyjnego (audyty KRI) 5,15%, a w ramach obszaru kompetencyjnego (szkolenia) 2,44%.

(akta kontroli str.: 3-7, 106-112, 117-146;
CD pliki: 067-522, 566-588, 630-664)

5. W realizacji Projektu, poza Urzędem, uczestniczyły cztery jednostki organizacyjne Gminy, tj. Ośrodek Pomocy Społecznej, Zespół Obsługi Szkół i Przedszkoli, Miejsko-Gminny Zakład Gospodarki Komunalnej oraz Miejsko-Gminny Zakład Wodociągowy. Dla podległych jednostek dokonano zakupu serwerów, systemów do tworzenia kopii zapasowych i archiwizacji danych, urządzeń UTM, Switchy zarządzalnych oraz oprogramowania antywirusowego. Ponadto pracownicy jednostek odbyli w ramach Projektu szkolenie z zakresu cyberbezpieczeństwa. Zakład Wodociągowy został dodatkowo wyposażony w agregat prądotwórczy.

(akta kontroli str.: 3-7, 27-72, 117-146; CD pliki: 026-050, 100-475)

---

[13] Łączne całkowite wydatki w ramach Projektu wyniosły 442 471,04 zł, z tego 361 378,08 zł stanowiły wydatki kwalifikowalne i 81 092,96 zł podatek VAT, który był wydatkiem niekwalifikowalnym.

[14] Unified Threat Management - to zintegrowany system ochrony sieci komputerowej, który łączy w sobie kilka funkcjonalności, takich jak zapory sieciowe, systemy wykrywania i zapobiegania atakom, serwery poczty elektronicznej, VPN, antywirusy i filtry treści internetowych.

6. W celu zapewnienia odpowiedniej realizacji Projektu wprowadzono procedurę zarządzania Projektem[15], w ramach której powołano zespół ds. realizacji Projektu. W skład zespołu wchodziło dziesięciu pracowników Urzędu, z tego:

- trzy osoby z referatu Administracyjno-Gospodarczego, w tym informatyk – realizujące zadania w zakresie m.in. koordynacji działań w Projekcie, sporządzenia opisu przedmiotu zamówienia dla poszczególnych elementów kupowanych w ramach Projektu oraz monitorowania kwalifikowalności wydatków;
- cztery osoby z Referatu Finansowo-Budżetowego realizujące zadania w zakresie obsługi finansowo-księgowej Projektu;
- jedna osoba z Referatu Pozyskiwania Funduszy Zewnętrznych – w zakresie współpracy z instytucją przyznającą grant, rozliczenia projektu oraz wypełnienia obowiązków informacji i promocji projektu;
- jedna osoba z Referatu Przygotowania i Realizacji Inwestycji – w zakresie kompleksowej obsługi prowadzonych w ramach projektu postępowań zakupowych;
- Inspektor Ochrony Danych – w zakresie opracowania ankiet dojrzałości, współpracy z audytorem oraz ochroną danych osobowych w projekcie.

Pracownicy wchodzący w skład Zespołu posiadali niezbędne kwalifikacje i doświadczenie.

(akta kontroli str.: 3-10, 117-146; CD pliki: 014-025)

7. W okresie objętym kontrolą w Urzędzie nie wystąpiła fluktuacja kadr mogąca wpłynąć na realizację Projektu.

(akta kontroli str.: 3-10, 117-146; CD pliki: 014-025)

8. We wniosku rozliczającym zaliczkę w ramach Programu „Cyberbezpieczny Samorząd”[16] wskazano pięć wskaźników wyrażających cele Projektu:

- Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (mężczyźni) – 1 szt.;
- Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym (kobiety) – 104 szt.;
- Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym (mężczyźni) – 37 szt.;
- Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji – 18 szt.;
- Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych – 1 szt.
- Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST – 5 szt.;

Były one zgodne ze wskaźnikami zdefiniowanymi dla całego konkursu grantowego określonymi w załączniku nr 9 do Regulaminu Konkursu

---

[15] Stanowiącą załącznik do zarządzenia nr 34a/2024 Burmistrz Miasta i Gminy Serock z dnia 14 maja 2024 r. w sprawie procedury zarządzania projektem „Gmina Serock – Cyberbezpieczny Samorząd”.

[16] Nr dokumentu: FERC.02.02-CS.01-001/23/1807/WRZ/WRZ/1.

Grantowego i były adekwatne do zakresu działań w ramach grantu. W przypadku dwóch wskaźników nierzetelnie została ustalona ich *wartość osiągnięta*, co opisano w punkcie drugim w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.: 3-10, 117-146; CD pliki: 014-049)

9. Zakupione w ramach Projektu urządzenia i oprogramowanie zostały zainstalowane i były użytkowane przez Urząd oraz jednostki organizacyjne Gminy, a zlecone audyty KRI zostały wykonane. Zlecone audyty zostały wykonane i sformułowano w nich wnioski/rekomendacje, z których część została wdrożona, a część jest w trakcie realizacji lub została zaplanowana do realizacji.

(akta kontroli str.: 27-72, 93-112, 117-146; CD pliki: 524-551)

10. Zgodnie z § 13 ust. 1 umowy grantowej, w Urzędzie wprowadzono procedurę, której celem było monitorowanie utrzymania efektów Projektu, tj. utrzymanie nabytych środków trwałych i usług po zakończeniu Projektu. Sekretarz poinformował, że w celu utrzymania poziomu cyberbezpieczeństwa po zakończeniu okresu trwałości Projektu planowane jest zabezpieczenie środków w budżecie Miasta i Gminy Serock na aktualizację wdrożonego oprogramowania i przedłużanie okresu ważności licencji oraz naprawy serwisowe w przypadku awarii zakupionych urządzeń. Dodał także, że część zakupionego sprzętu została objęta pięcioletnim okresem ochrony gwarancyjnej.

(akta kontroli str.: 3-10, 82-146; CD pliki: 27-50)

11. W Urzędzie nie został opracowany, ustanowiony i wdrożony System Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 w związku z ust. 3 starego rozporządzenia KRI oraz w § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI, co opisano w punkcie trzecim w sekcji *Stwierdzone nieprawidłowości.*

Wprowadzone w 2018 r.[17] Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym dotyczyły bezpieczeństwa danych osobowych.

(akta kontroli str.: 3-10, 117-146; CD pliki: 051-060)

12. W okresie objętym kontrolą w Urzędzie wykonano jeden audyt z zakresu bezpieczeństwa informacji, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI[18]. Audyt został przeprowadzony przez podmiot zewnętrzny, którego personel posiadał odpowiednie kwalifikacje oraz doświadczenie w realizacji tego typu zadań, zgodnie z obowiązującymi standardami i przepisami. W wyniku audytu sformułowano 12 zaleceń dotyczących m.in. wdrożenia kompleksowego SZBI, wdrożenia fizycznych zabezpieczeń danych na urządzeniach, wykonywania i dokumentowania działań w zakresie bezpieczeństwa informacji oraz corocznego przeprowadzania audytów bezpieczeństwa informacji. Według

---

[17] Zarządzeniem nr 20a/2018 Burmistrza Miasta i Gminy Serock z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych Urzędu Miasta i Gminy Serock.

[18] Audyt przeprowadzono w ramach Projektu okresie 4-20 grudnia 2024 r. we wszystkich pięciu jednostkach biorących udział w Projekcie.

stanu na dzień 21 sierpnia 2025 r. trzy rekomendacje zostały wdrożone, a pozostałe dziewięć jest w trakcie realizacji.

Nie przeprowadzono audytu bezpieczeństwa informacji w 2023 r., co opisano w punkcie czwartym w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str.: 3-8, 82-91, 117-146;
CD pliki: 041-045, 064-066, 542-545)

13. Na podstawie § 11 ust. 3 umowy grantowej, w zakresie informacji i promocji Projektu Grantobiorca zobowiązany był do stosowania zasad określonych w Podręczniku wnioskodawcy i beneficjenta programów polityki spójności na lata 2021 -2027 w zakresie informacji i promocji (dalej: Podręcznik). Obowiązek obejmował w szczególności:

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

Urząd informował opinię publiczną o fakcie otrzymania dofinansowania poprzez umieszczenie plakatu na głównej tablicy informacyjnej oraz na tablicy multimedialnej w głównej hali obsługi obywateli w budynku Urzędu. Plakaty zawierały wszystkie wymagane oznaczenia, tj. znaki Funduszy Europejskich oraz Unii Europejskiej, nazwę beneficjenta oraz tytuł Projektu, a także wysokość dofinansowania i adres portalu mapadotacji.gov.pl. Na stronie internetowej Urzędu oraz w mediach społecznościowych umieszczono informacje dotyczące realizacji Projektu oraz jego dofinansowania ze środków Unii Europejskiej. Wypełniono także obowiązek w zakresie dokumentowania realizacji działań informacyjnych i promocyjnych poprzez utworzenie segregatora, w którym przechowywano m.in. zrzuty ekranu ze strony internetowej oraz mediów społecznościowych, a także zdjęcia plakatów informujących o Projekcie, umieszczonych w Urzędzie.

Ustalono, że nie wszystkie dokumenty oraz zakupione urządzenia posiadały wymagane oznaczenia w postaci znaków Funduszy Europejskich, barw Rzeczypospolitej Polskiej i Unii Europejskiej, a na stronie internetowej nie zawarto niektórych elementów określonych w *Podręczniku wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji*. Szczegółowy opis w punkcie piątym w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str.: 26-72, 95-107)

Stwierdzone nieprawidłowości

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

1. Nierzetelne sporządzenie Ankiet dojrzałości dla pięciu jednostek uczestniczących w Projekcie.

W Ankietach dojrzałości przekazanych do Operatora 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 Urzędu.*

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, stanowiąca podstawowy element niewdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (szczegółowo opisane w punkcie trzecim w sekcji *Stwierdzone nieprawidłowości)*. Sekretarz wyjaśnił, że opracowana polityka ochrony danych osobowych szeroko i szczegółowo odnosi się do bezpieczeństwa informacji i danych, nie tylko osobowych. Dodał także, że dokument jest dostępny dla pracowników Urzędu i na bieżąco weryfikowany przez IOD. 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[19] 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.

W związku z zakończeniem i rozliczeniem prac w ramach Projektu, NIK odstępuje od sformułowania wniosku pokontrolnego w zakresie rzetelnego sporządzania Ankiet dojrzałości.

(akta kontroli str.: 3-5, 17-25, 117-146;
CD pliki: 028-032, 051-060, 084-099)

2. Nieprawidłowe określenie wartości dwóch wskaźników realizacji Projektu we wniosku rozliczającym.

Wykazana we wniosku rozliczającym wartość wskaźnika *Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji* wynosiła 18 i obejmowała wszystkie pojedyncze systemy zakupione dla pięciu jednostek uczestniczących w Projekcie. Zgodnie z definicją wskazaną w załączniku do

[19] Na podstawie rozporządzenia Parlamentu Europejskiego i Rady (HE) 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).

Regulaminu Projektu (...) *w przypadku, gdy ten sam system wdrażany jest w kilku podmiotach, jest on liczony 1 raz, a nie tyle razy, ile jest podmiotów. (...).*

Sekretarz poinformował, że w związku z kontrolą NIK dokonano weryfikacji wartości wskaźnika. Po konsultacji z NASK ustalono, *(...) że wartość wskaźnika powinna wynosić 5 (...).*
Do zakończenia czynności kontrolnych nie dokonano korekty i nie przekazano skorygowanego wniosku rozliczającego do Operatora.
Wartość wskaźnika *Użytkownicy nowych i zmodernizowanych usług, produktów i procesów cyfrowych* wykazana we wniosku rozliczającym wynosiła jeden. Sekretarz wyjaśnił, że wykazana wartość wskaźnika odnosiła się do pracownika IT Urzędu odpowiedzialnego za sprzęt zakupiony w ramach Projektu, który monitoruje nabyte środki trwałe.

Kontrola NIK ustaliła, że uczestniczące w Projekcie jednostki podległe we własnym zakresie organizują bieżącą obsługę informatyczną w ramach swojej działalności. W związku z tym, zdaniem NIK pracownik IT Urzędu nie sprawował nadzoru nad sprzętem wdrożonym w jednostkach podległych, gdyż zgodnie z protokołami przekazania sprzętu osobami odpowiedzialnymi za ich prawidłowe wykorzystanie byli dyrektorzy jednostek przyjmujący sprzęt. Zatem wskaźnik ten powinien wynosić 5.

(akta kontroli str.: 3-10, 27-54, 82-94, 117-146;
CD pliki: 014-049, 589-629)

3. Nieopracowanie Systemu Zarządzania Bezpieczeństwem Informacji.

W okresie objętym kontrolą w Urzędzie Miasta i Gminy Serock nie został opracowany, ustanowiony i wdrożony Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym nie opracowano PBI, co było niezgodne z § 20 ust. 1 w związku z ust. 3 starego rozporządzenia KRI oraz z § 19 ust. 1 w związku z ust. 3 rozporządzenia KRI. Stosownie do ww. przepisów Urząd zobowiązany był m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i doskonalenia SZBI, zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak rozliczalność, autentyczność, niezaprzeczalność i niezawodność.

Sekretarz wyjaśnił, że brak wdrożenia SZBI wynikał z przekonania, iż wdrożona w Urzędzie Polityka Bezpieczeństwa Danych Osobowych była dokumentem wystarczającym. Dodał także, że obecnie Urząd przygotowuje się do opracowania kompleksowej Polityki Bezpieczeństwa Informacji.

(akta kontroli str.: 3-7, 17-25, 27-54, 82-94, 117-146;
CD pliki: 051-060, 523-551)

4. Nieprzeprowadzenie audytu bezpieczeństwa informacji w 2023 r.

W 2023 r. nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 starego rozporządzenia KRI.

W 2023 r. Inspektor Ochrony Danych (IOD) przeprowadził ocenę technicznych i organizacyjnych środków bezpieczeństwa stosowanych u Administratora dla ochrony danych osobowych, ze szczególnym uwzględnieniem wymogów rozporządzenia KRI. Ponadto IOD we współpracy z pracownikiem

odpowiedzialnym za infrastrukturę informatyczną (Administratorem Systemów Informatycznych urzędu – ASI) przeprowadzili przegląd bezpieczeństwa informacji oraz cyberbezpieczeństwa Urzędzie.
Sekretarz wyjaśnił, że w 2023 r. uznano sporządzone przez IOD dokumenty za wystarczające do spełnienia obowiązku wynikającego z rozporządzenia KRI.
Zgodnie z wytycznymi Normy PN-ISO/IEC 27001:2017 punkt 9.2 *Audyt wewnętrzny Organizacja powinna: wybierać audytorów i prowadzić audyty w sposób zapewniający obiektywność i bezstronność procesu audytu*. Audyty nie mogą więc być przeprowadzane przez osoby realizujące zadania poddawane ocenie.
Zdaniem NIK, dokumenty opracowane przez IOD i ASI stanowiły jedynie przegląd zadań realizowanych przez nich w ramach powierzonych obowiązków i nie stanowiły okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.
W związku z przeprowadzeniem w 2024 r. audytu bezpieczeństwa informacji przez zewnętrzny, niezależny podmiot, NIK odstępuje od sformułowania wniosku pokontrolnego w tym zakresie.

(akta kontroli str.: 3-10, 17-72, 82-93, 117-146; CD pliki: 014-049,17-23, 061-066, 552-565)

5. Niepełna realizacja obowiązków w zakresie informacji i promocji.

Zgodnie z pkt 3 Podręcznika obowiązek w zakresie informacji i promocji powstał od momentu podpisania umowy grantowej. Ustalono, że na stronie internetowej Urzędu (www.serock.pl) nie zostały umieszczone hasztagi #FunduszeUE lub #FunduszeEuropejskie, wskazane w punkcie 11 Podręcznika. Ponadto ustalono, że część dokumentów dotyczących postępowania przetargowego przeprowadzonego w ramach Projektu[20], a także sprzęt zainstalowany w serwerowni Ośrodka Pomocy Społecznej nie posiadały oznaczeń wskazanych w punkcie 7 Podręcznika, tj. znaku Unii Europejskiej, barw Rzeczypospolitej Polskiej i znaku Funduszy Europejskich.

Sekretarz wyjaśnił, że hasztagi nie zostały umieszczone na stronie internetowej ze względu na brak możliwości ich zastosowania zgodnie z przeznaczeniem, gdyż funkcjonalność ta nie została zaimplementowana na stronie Urzędu. W zakresie braku oznaczeń na dokumentach wyjaśnił, że wynikało to z omyłki podczas drukowania dokumentów.

W trakcie kontroli hasztagi zostały umieszczone na stronie Urzędu, a na urządzeniach zamieszczono naklejki informujące o uzyskanym dofinansowaniu z Funduszy Europejskich, zgodnie z pkt 7 i 11 Podręcznika.

(akta kontroli str.: 26-72, 95-107, 117-146; CD pliki: 552-560)

[20] M.in.: informacja z otwarcia ofert, informacja o kwocie przeznaczonej na sfinansowanie zamówienia, zawiadomienie o wyborze najkorzystniejszej oferty.

IV. Wnioski

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

Wnioski

1. Dokonanie korekty wniosku rozliczającego w zakresie wartości wskaźników realizacji Projektu i przekazanie skorygowanego wniosku do Operatora.
2. Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.
3. Zapewnienie wypełniania obowiązku w zakresie informacji i promocji zgodnie z wymogami określonymi w Podręczniku.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne sporządzono w postaci elektronicznej z użyciem kwalifikowanych podpisów elektronicznych.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Dyrektora Departamentu Administracji Publicznej NIK. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, 5 września 2025 r.

Kontroler

Marcin Grochal

Główny specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Departament Administracji Publicznej

p.o. Dyrektor

Bogdan Skwarka

/podpisano elektronicznie/