



**WOJEWODA
ŚWIĘTOKRZYSKI**

Kielce, dnia 10 lipca 2025 r.

Znak:OK.V.431.2.2025

**Pani Beata Janiszewska
Wójt Gminy Smyków**

WYSTĄPIENIE POKONTROLNE

Zakres kontroli:	Prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej.
Okres objęty kontrolą:	od 1 stycznia 2022 r. do dnia wszczęcia kontroli tj. 28 maja 2025 r.
Kontrolerzy:	Marek Rak – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 413/2025 z 26 maja 2025 r. Maciej Terek – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 414/2025 z 26 maja 2025 r.
Termin przeprowadzenia kontroli:	Kontrola została przeprowadzona w dniu 28 maja 2025 r. w siedzibie Urzędu Gminy w Smykowie
Podstawa prawna do przeprowadzenia kontroli:	Kontrolę przeprowadzono na podstawie art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. <i>o kontroli w administracji rządowej</i>¹, art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. <i>o Wojewodzie i Administracji rządowej w województwie</i>² oraz art. 25 ust.1 pkt 3 lit. a) ustawy z dnia 17 lutego 2005 r. <i>o informatyzacji działalności podmiotów realizujących zadania publiczne</i>³. Wystąpienie pokontrolne przekazano zgodnie z przepisami art. 47 ustawy o kontroli w administracji rządowej.
Ocena stanu faktycznego wynikająca	Zgodnie z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024r. <i>w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań</i>

¹ Dz. U. z 2020 r. poz. 224, dalej: Ustawa o kontroli w administracji rządowej.

² Dz. U. z 2023 r. poz. 190

³ Dz. U. z 2024 r. poz. 307

z ustaleń kontroli:

dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych⁴ ocenie podlegały czynności podejmowane w trzech obszarach tematycznych:

1. system zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych,
2. realizacja działań z zakresu bezpieczeństwa informacji,

Pozytywnie z nieprawidłowościami ocenia się prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy w Smykowie w okresie objętym kontrolą.

Ocena końcowa ustalona została w oparciu o przedstawione poniżej wnioski i oceny częściowe.

Kontrolą w przedmiotowym zakresie objęto systemy informatyczne używane do realizacji zadań zleconych z zakresu administracji rządowej tj.: SRP Źródło, CEIDG, System ZONE oraz RESPONS. W toku przeprowadzonej kontroli ustalono, że

1. System zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych:

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 1 i 2 Rozporządzenia KRI.

Podstawowym dokumentem z zakresu bezpieczeństwa informacji w Urzędzie Gminy w Smykowie jest Polityka Ochrony Danych (POD) wprowadzona zarządzeniem nr 53/2024 Wójta Gminy Smyków z dnia 11 października 2024 roku. Dokumentacja ta dotyczy ochrony wszystkich danych, ale dla niektórych zagadnień jak analiza ryzyka czy postępowanie z incydentami jest zawężona do danych osobowych. Kontrolowany przedłożył także poprzednią wersję dokumentacji z tego zakresu tj. Politykę Bezpieczeństwa Informacji (PBI) i instrukcję zarządzania systemem informatycznym (IZSI) wprowadzoną zarządzeniem 52/2018 Wójta Gminy Smyków z dnia 1 sierpnia 2018 roku.

W trakcie kontroli przedłożono następujące dokumenty (załączniki) zgodne z POD:

- Załącznik nr 3. Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Załącznik nr 5. Wykaz osób, które zostały zapoznane z POD
- Roczne sprawozdanie z działalności IOD za rok 2024
- Załącznik nr 6. Analiza ryzyka w obszarze ochrony danych na lata 2024-2025
- Załącznik nr 7. Rejestr czynności przetwarzania danych osobowych
- Dokumentacja prowadzona przez ASI: Rejestr testów kopii zapasowych, Rejestr aktualizacji oprogramowania, Rejestr kopii konfiguracji urządzeń
- Załącznik nr 12. Wnioski o nadanie, odebranie, modyfikacje uprawnień w systemach informatycznych

⁴ Dz. U. z 2017 r., poz. 2247, dalej Rozporządzenie KRI

- Załącznik nr 13. Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym. Ewidencja nie jest prowadzona zgodnie z zapisami w POD UG. W dokumentacji brakuje identyfikatorów pracowników którym założono konta i nadano dostęp do danych w systemach informatycznych UG.
- Załącznik nr 15. Inwentaryzacja sprzętu i oprogramowania
ASI przełożył również dokumentację która jest przez niego systematycznie prowadzona a nie została ujęta w POD :
 - Rejestr testów kopii zapasowych
 - Rejestr kopii konfiguracji urządzeń
 - Rejestr aktualizacji oprogramowania

Zespół kontrolny po zapoznaniu się z POD z roku 2024 stwierdził, że część czynności opisanych w POD nie jest realizowana lub realizowana jest w inny sposób niż to opisano w dokumentacji. Kontrolujący nie otrzymali dokumentacji w zakresie:

- Roczego planu przeglądów i konserwacji systemów oraz baz danych. Plan ma opracować ASI (POD §52)
- Sprawdzania logów systemowych (POD §52)
- Wykonywania kopii na nośnikach magnetycznych lub optycznych przez pracowników urzędu (POD §51). Z rozmowy przeprowadzonej z ASI wynika, iż kopie stacji roboczych wykonywane są automatycznie, a same kopie gromadzone są na przygotowanych do tego celu urządzeniach
- wniosków o odebranie uprawnień w systemach informatycznych (załącznik nr 12)
- wniosków o modyfikacje uprawnień w systemach informatycznych (załącznik nr 12)
- Wnioski o nadanie, odebranie, modyfikacje uprawnień w systemach informatycznych nie są kompletnie wypełnione. Brakuje istotnych informacji jak data złożenia wniosku i podpisu osoby wnioskującej. Brakuje również informacji o fizycznym nadaniu uprawnień w systemach informatycznych przez ASI. Brak daty i podpisu ASI. Sam wniosek nie uwzględnia udziału w całym procesie ASI.
- dokumentacji świadczącej o systematycznym przeglądaniu POD (POD §15)

Przedmiotowe dokumenty załączono w formie plików cyfrowych do akt kontroli (pobrane-dokumenty-UG-Smyków.pdf).

Ocena częściowa

Pozytywnie z uchybieniami ocenia się działalność Jednostki

badanego zagadnienia: w przedmiotowym zakresie.

2. Realizacja działań z zakresu bezpieczeństwa informacji:

Zakres kontroli przedmiotowego zagadnienia został podzielony na dwanaście obszarów badawczych:

1. Analiza zagrożeń związanych z przetwarzaniem informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 3 Rozporządzenia KRI.

Przedłożono kopię cyfrową jak również oryginał dokumentu „Analiza ryzyka w obszarze ochrony danych osobowych na lata 2024-2025”. Analiza została wykonana w październiku 2024 roku. Analiza została wykonana przez IOD i zatwierdzona przez Wójta Gminy.

Analiza ryzyka zawiera szereg działań minimalizujących ryzyko. Znaczna część działań minimalizujących ryzyko z analizy ryzyka została wykonana: polityka kluczy (specjalnie przygotowana skrzynka zamykana na klucz gdzie pracownicy po zakończeniu pracy pozostawiają klucze), książki wejść i wyjść pracowników urzędu, instalacja certyfikowanych drzwi w pomieszczeniu serwerowni, przeprowadzone audyty i szkolenia.

Natomiast sam tytuł analizy ryzyka (ryzyka w obszarze danych osobowych) sugeruje, że sama analiza ryzyka dotyczy obszaru związanego ze szczególnymi danymi jakimi są dane osobowe a nie z wszystkimi danymi przetwarzanymi w Urzędzie Gminy w Smykowie.

Kontrolowany nie przedłożył dokumentów analizy ryzyka sprzed roku 2024. W PBI z roku 2018 nie ma nic o analizie ryzyka.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (Analiza ryzyka 2024-2025.pdf).

2. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI.

Ustalono, że inwentaryzacja sprzętu i oprogramowania jest prowadzona przez ASI w oparciu o oprogramowanie IT Manager oraz o plik w formacie xls prowadzony przez ASI. Zespołowi kontrolnemu zostały przedstawione podczas oględzin dane gromadzone w zakresie inwentaryzacji sprzętu i oprogramowania, został udostępniony przykładowy zestaw danych oraz wyświetlone zakładki z danymi gromadzonymi przez IT Manager.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (pobrane-dokumenty-UG-Smyków.pdf).

3. Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 4 oraz

5 Rozporządzenia KRI.

Procedura nadawania, modyfikacji, odbierania uprawnień w systemach informatycznych jest opisana w §42 POD.

Proces nadawania, modyfikacji, odebrania uprawnień w systemach informatycznych rozpoczyna się od złożenia wniosku przez bezpośredniego przełożonego do ADO który następnie przekazuje zaakceptowany wniosek do IOD.

Na przedłożonych wnioskach (załącznik nr 12) nie ma wpisanej daty złożenia wniosku przed bezpośredniego przełożonego jak również nie ma podpisu bezpośredniego przełożonego. Brak jest również na wnioskach numerów porządkowych. Brak jest na wniosku (załącznik numer 12) uwzględnienia udziału ASI w całym procesie nadawania, modyfikacji i odbierania uprawnień w systemach informatycznych. Na wniosku nie ma informacji, czy ASI faktycznie założył konto w systemie informatycznym i nadał odpowiednie uprawnienia. Nie przedłożono wniosków o modyfikację i odebranie uprawnień w systemach informatycznych. (§42 POD, punkt 12,14).

Identyfikatory użytkowników w systemach informatycznych nadane w trybie rejestracji użytkownika powinny zgodnie z POD zostać odnotowane w Rejestrze osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym (załącznik nr 13). Niestety przełożony załącznik numer 13 nie zawiera identyfikatorów użytkowników w systemach informatycznych.

Powyższe ustalenia sugerują, że procedura opisana w POD związana z nadawaniem, modyfikacją, odbiorem uprawnień w systemach informatycznych nie została w pełni wdrożona, co powoduje, że nie ma atrybutów rozliczalności, autentyczności, niezaprzeczalności i niezawodności o których jest mowa w KRI.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (pobrane-dokumenty-UG-Smyków.pdf).

4. Szkolenia pracowników zaangażowanych w proces przetwarzania danych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 6 Rozporządzenia KRI.

Zespołowi kontrolnemu zostały przedłożone listy obecności ze szkoleń z zakresu cyberbezpieczeństwa z lat 2022, 2024 i 2025. Z programów poszczególnych szkoleń wynika, że na przestrzeni lat na szkoleniach nie był poruszany temat POD UG, nie szkolono pracowników w zakresie procedur, instrukcji zawartych w POD, nie omawiano poszczególnych zagadnień dotyczących ochrony danych wdrożonych i obowiązujących w kontrolowanej jednostce.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (pobrane-dokumenty-UG-Smyków.pdf).

5. Praca na odległość i mobilne przetwarzanie danych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 8 Rozporządzenia KRI.

W POD nie ma procedur dotyczących pracy zdalnej, ten temat jest kompletnie pominięty.

Z rozmowy przeprowadzonej z ASI wynika, że firmy zewnętrzne korzystają z możliwości zdalnego dostępu do sieci Urzędu co wynika z podpisanych umów. Brak procedur w tym zakresie.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (pobrane-dokumenty-UG-Smyków.pdf).

6. Serwis sprzętu komputerowego i oprogramowania.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 10 Rozporządzenia KRI.

Z rozmowy przeprowadzonej z ASI wynika, że przeważającą większość prac serwisowych wykonuje sam we własnym zakresie. Niewielka część czynności serwisowych wykonywana jest przez firmy zewnętrzne. Zespół kontrolny nie znalazł w udostępnionej dokumentacji zapisów i procedur związanych z wykonaniem czynności serwisowych przez firmy zewnętrzne.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (pobrane-dokumenty-UG-Smyków.pdf).

7. Procedury zgłaszania incydentów naruszenia Bezpieczeństwa Informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 13 Rozporządzenia KRI.

W POD znajduje się załącznik nr 16 - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

Sam tytuł załącznika nr 16 jak również zawarte w nim definicje, opisy wskazuje, że cała instrukcja dotyczy szczególnych danych jakimi są dane osobowe. W kontrolowanej jednostce gromadzone i przetwarzane są również dane inne niż dane osobowe i definicja incydentu oraz postępowania z incydentem powinna dotyczyć danych w szerszym tego słowa znaczeniu niż tylko danych osobowych.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (pobrane-dokumenty-UG-Smyków.pdf).

8. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 14 Rozporządzenia KRI.

Zespołowi kontrolnemu przedłożono dokumentację z dwóch audytów wewnętrznych z lat 2024-2025.

W raporcie z audytu z roku 2025 w części dotyczącej przeglądania polityki w zaplanowanych odstępach czasu oraz przy wprowadzanych zmianach w otoczeniu wewnętrznym lub zewnętrznym Organizacji napisano, że przeglądy są dokonywane okresowo, ponadto są wykonywane przy większych zmianach. Tymczasem zespołowi kontrolnemu nie przedłożono żadnej dokumentacji świadczącej o tym, że dokonywany jest systematyczny przegląd dokumentacji związanej z POD (patrz §15 POD).

Zalecenia po audytowe w miarę swoich możliwości są realizowane.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (audyt wewnętrzny 2024 RODO.pdf, Audyt Teleinformatyczny wewnętrzny KRI 2025.pdf).

9. Kopie zapasowe.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 12 Rozporządzenia KRI.

Kopie zapasowe zasobów stacji roboczych, zasobów sieciowych, baz danych, aplikacji i systemów wykonywane są codziennie według harmonogramu opracowanego przez ASI. Kopie przechowywane są na urządzeniu zamontowanym w szafie dystrybucyjnej w serwerowni jak również na dwóch dyskach zewnętrznych przechowywanych w metalowym sejfie umieszczonym w zwykłej szafie. Zespołowi kontrolnemu zostały udostępnione zrzuty ekranu z harmonogramu wykonywania kopii poszczególnych zasobów. ASI prowadzi rejestr testów kopii zapasowych oraz rejestr kopii konfiguracji urządzeń.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt (pobrane-dokumenty-UG-Smyków.pdf).

10. Bezpieczeństwo techniczno-organizacyjne dostępu do informacji.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 7, 9 oraz 11 Rozporządzenia KRI.

Urząd Gminy w Smykowie posiada dwa wejścia do budynku. Oba wejścia zabezpieczone są oszklonymi drzwiami z podwójnymi zamkami. Wejście główne zabezpieczone jest dodatkowo metalowa kratą zamykaną na kłódkę. Budynek wyposażony jest w system antywłamaniowy którego

urządzenia znajdują się na terenie budynku. Na terenie budynku rozmieszczone są urządzenia systemu przeciwpożarowego. Budynek wewnątrz i na zewnątrz uzbrojony jest w kamery monitoringu wizyjnego. Obraz monitoringu przechowywany jest przez 2 tygodnie. Pomieszczenia na terenie budynku zabezpieczone są drzwiami z zamkiem. Klucze po zakończeniu pracy pracownicy pozostawiają w metalowej zamykanej na klucz skrzynce zamontowanej wewnątrz pomieszczenia sekretariatu. Prowadzone są książki wejść i wyjść pracowników urzędu. Prowadzona jest ewidencja wejść do pomieszczenia serwerowni. Samo pomieszczenie serwerowni jest wyposażone w urządzenie systemu klimatyzacji, systemu przeciwpożarowego, w szafy dystrybucyjne oraz urządzenia UPS. Urząd bierze udział w projekcie „Cyberbezpieczny samorząd”. W ramach projektu zostało zaplanowane pozyskanie dwóch urządzeń UTM, switchy zarządzalnych, nadmiarowego serwera, który będzie pełnił funkcję serwera zapasowego strategicznego w procesie zapewnienia ciągłości pracy oraz zakup agregatu prądotwórczego.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (protokół oględzin pomieszczeń.pdf).

11. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.

Oceny stanu faktycznego dokonano zgodnie z §19 ust. 2 pkt 12, oraz ust. 4 Rozporządzenia KRI.

W dniu kontroli w szafie dystrybucyjnej zamontowane były między innymi dwa skonfigurowane i pracujące urządzenia UTM oraz urządzenia UPS zapewniające utrzymanie napięcia na około 15 minut. Wprowadzona jest polityka haseł dostępu do sieci informatycznej, określono złożoność haseł dostępu jak również częstotliwość zmian haseł. Hasła administracyjne do systemów informatycznych przechowywane są w specjalnie przygotowanym miejscu w metalowym sejfie. Są pewne nieścisłości odnośnie sposobu przechowywania haseł administracyjnych fizycznie a tym co zostało zapisane w POD. Należy dokonać przeglądu tych zapisów i ujednolicić zapisy w POD ze stanem faktycznym. Stacje robocze w razie bezczynności zabezpieczone są wygaszaczami ekranu, pracownicy Urzędu są przeszkoleni w zakresie klawiaturowej blokady stacji roboczej.

Od roku 2022 czyli od trzech lat obowiązuje trzeci stopień alarmowy CHARLIE-CRP. Należałoby opracować, wdrożyć i przetestować plany ciągłości działania.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (pobrane-dokumenty-UG-Smyków.pdf).

12. Rozliczalność działań w systemach teleinformatycznych.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2, 3 oraz 4 Rozporządzenia KRI. Ustalono, że oprogramowanie wspomagające oraz systemy operacyjne używane w kontrolowanej jednostce posiadają funkcjonalności monitorujące prace użytkowników. Nie ma jednak procedury do systematycznego przeglądania logów systemowych, co w efekcie końcowym skutkuje brakiem przeglądania logów a tym samym brakiem monitorowania zdarzeń.

Przedmiotowe regulacje załączono w formie plików cyfrowych do akt kontroli (pobrane-dokumenty-UG-Smyków.pdf).

**Ocena częściowa
badanego zagadnienia:**

Pozytywnie z nieprawidłowościami ocenia się działalność Jednostki w przedmiotowym zakresie.

**3. Zapewnienie
dostępności cyfrowej
informacji zawartych na
stronach internetowych
urzędów dla osób
z niepełnosprawnościami
zgodnie z ustawą z dnia 4
kwietnia 2019 r.
o dostępności cyfrowej
stron internetowych i
aplikacji mobilnych
podmiotów publicznych:**

Czy sporządzono i opublikowano deklarację dostępności oraz zawarto w deklaracji dostępności elementy wskazane w art. 10 ust. 3-5 ustawy dla stron internetowych podmiotu.

Oceny stanu faktycznego dokonano zgodnie z §10 ust. 3, 4 i 5 ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych⁵.

Zespół kontrolny zapoznał się ze stroną internetową Urzędu Gminy w Smykowie. Deklaracja dostępności dla strony internetowej Urzędu nie zawiera informacji na temat skrótów klawiszowych służących przemieszczaniu się po elementach strony internetowej.

**Ocena częściowa
badanego zagadnienia:**

Pozytywnie z uchybieniami ocenia się działalność Jednostki w przedmiotowym zakresie.

**Wnioski, zalecenia oraz
dodatkowe informacje:**

Reasumując powyższe ustalenia, zwracam się z prośbą do Pana Burmistrza o niedopuszczenie do powstania nieprawidłowości wykazanych w toku kontroli w przyszłej działalności w podległej Panu Jednostce. Wobec powyższego sformułowano następujące zalecenia:

- 1) Zapewnić, aby dokumentacja z zakresu bezpieczeństwa informacji obejmowała wszystkie dane przetwarzane w jednostce.
- 2) W dokumentacji z zakresu bezpieczeństwa informacji opisywać zasady, procesy i czynności w sposób w jaki są faktycznie realizowane w jednostce.

⁵ Dz. U. z 2023 r. poz. 1440

- ~~3)~~ Systematycznie wykonywać analizę ryzyka dla wszystkich danych przetwarzanych w jednostce a nie tylko danych osobowych.
- ~~4)~~ W ramach szkoleń omawiać również tematy związane z dokumentacją z zakresu bezpieczeństwa informacji.
- ~~5)~~ Ustanowić podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
- ~~6)~~ Zapewnić, aby zarządzanie incydentami obejmowało wszystkie dane przetwarzane w jednostce.
- ~~7)~~ Systematycznie dokonywać przeglądu dokumentacji związanej z POD i dokumentować te czynności.
- ~~8)~~ W miarę możliwości opracować, wdrożyć i przetestować plan ciągłości działania.
- 9) W miarę możliwości opracować i wdrożyć procedurę systematycznego przeglądania logów systemowych.
- 10) Uzupełnić deklarację dostępności cyfrowej strony internetowej Urzędu o informacje na temat skrótów klawiszowych służących przemieszczaniu się po elementach strony internetowej.

Jednocześnie na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę poinformować Wojewodę Świętokrzyskiego w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz o wykonaniu zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Ponadto informuję, iż zgodnie z art. 48 ustawy o kontroli w administracji rządowej od niniejszego wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Józef Bryk
Wojewoda Świętokrzyski