WOJEWODA MAZOWIECKI

Warszawa, 18 czerwca 2025 r.

WK-I.431.2.1.2025

Pan
Arkadiusz Werelich
Starosta Wołomiński

Starostwo Powiatowe w Wołominie
ul. I. Prądzyńskiego 3
05-200 Wołomin

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 28 ust. 1 pkt 2 ustawy o wojewodzie i administracji rządowej w województwie[1], art. 6 ust. 4 pkt 3 ustawy o kontroli w administracji rządowej[2] oraz art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[3], kontrolerzy: Andrzej Nieszporek – główny specjalista, Katarzyna Możdżyńska oraz Anna Simińska – starsi inspektorzy wojewódzcy w Oddziale Kontroli Jednostek Samorządu Terytorialnego Wydziału Kontroli, a także Krzysztof Sobierski – Dyrektor Biura Informatyki oraz Łukasz Plaskot – kierownik Oddziału Serwisu Informatycznego w Biurze Informatyki Mazowieckiego Urzędu Wojewódzkiego w Warszawie (dalej MUW), przeprowadzili w dniach od 12 marca do 4 kwietnia 2025 r. kontrolę problemową w Starostwie Powiatowym w Wołominie, z siedzibą w Wołominie przy ul. I. Prądzyńskiego 3 (dalej Starostwo).

Przedmiot kontroli obejmował realizację zadań w zakresie działania systemów teleinformatycznych używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów

[1] Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. 2025 poz. 428).
[2] Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224).
[3] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557, ze zm.).

teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej[4] – w okresie od 1 stycznia 2024 r. do 3 marca 2025 r.

Nawiązując do projektu wystąpienia pokontrolnego z 21 maja 2025 r., do którego nie wniesiono zastrzeżeń, przekazuję wystąpienie pokontrolne.

Ocenie poddano dwa główne obszary kontroli, tj. wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami informatycznymi i wspomaganie usług świadczonych drogą elektroniczną oraz zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych.

W Starostwie prowadzono rejestry publiczne, o których mowa w art. 14 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.
W prowadzonych rejestrach publicznych wyróżniono typy obiektów oraz ustalono strukturę ich identyfikatorów, zgodnie z wymogami § 10 ust. 1, 2 i 3 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej rozporządzenie w sprawie KRI).

Kontroli poddano system teleinformatyczny XXXXXXXX używany w Starostwie do realizacji zadań publicznych.

I.A. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami (rejestrami) teleinformatycznymi oraz wspomaganie usług drogą elektroniczną.

Starostwo udostępnia elektroniczną skrzynkę podawczą (dalej ESP) umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Na stronie internetowej Biuletynu Informacji Publicznej (dalej BIP) poinformowano o warunkach organizacyjno-technicznych doręczania dokumentów elektronicznych, zgodnie z § 3 ust. 1 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[6]. Starostwo umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw w formatach danych określonych w załączniku nr 2 rozporządzenia w sprawie KRI.

---

4 Zgodnie z art. 25 ust. 3 przedmiotowej ustawy kontrola dotyczyła wyłącznie systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej.

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 (Dz. U. z 2024 r. poz. 773).

6 Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. z 2018 r. poz. 180).

Na stronie podmiotowej BIP Starostwa[7] umieszczono przekierowania do opisów usług realizowanych przez jednostkę kontrolowaną. Przedmiotowe karty usług pogrupowane są w zakładkach tematycznych określających kategorię spraw. Karty usług sporządzono według jednolitego wzoru. Zawierają one informacje o podstawie prawnej realizacji danej usługi, miejscu i sposobie załatwienia sprawy, wymaganych dokumentach, czasie załatwienia sprawy, przysługujących środkach odwoławczych, a także o komórce organizacyjnej odpowiedzialnej za realizację danego zadania.

Ustalono, że w okresie objętym kontrolą Starostwo nie przekazywało wzorów dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, natomiast korzysta z wzorów zamieszczonych w przedmiotowym repozytorium.

Starostwo stosuje w prowadzonych rejestrach odwołania do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań, zgodnie z § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI oraz wyposaża posiadane systemy teleinformatyczne w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanawianych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej, zgodnie z § 16 ust. 1 rozporządzenia w sprawie KRI oraz formatach danych określonych w załączniku nr 2 i 3 rozporządzenia w sprawie KRI. Kodowanie znaków w wysyłanych z systemów lub odbieranych przez te systemy dokumentach odbywa się zgodnie z § 17 ust. 1 ww. rozporządzenia.

Ustalono, że w Starostwie obowiązuje jako podstawowy tradycyjny system obiegu dokumentów, natomiast system informatyczny XXXXXX pełni funkcje wspomagające wykonywanie czynności kancelaryjnych w systemie tradycyjnym[8]. Przedmiotowy system, zapewnia zintegrowaną obsługę korespondencji przychodzącej, wychodzącej i wewnętrznej, poprzez rejestrację, dekretację i zarządzanie obiegiem korespondencji.

W wyniku kontroli stwierdzono nieprawidłowość polegającą na XXXXXXXXXXXXXXX XXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXW trakcie trwania

[7] Pod adresem https://samorzad.gov.pl/web/powiat-wolominski/zalatw-sprawe-w-urzedzie4 w zakładce: Jak załatwić sprawę.

[8] Zarządzenie Starosty Wołomińskiego nr 120.197.2023 z 26 lipca 2023 roku.

czynności kontrolnych kontrolującym przedstawiono wykaz 27 usług świadczonych przez Starostwo drogą elektroniczną, zawierający wskazanie poziomu dojrzałości tych usług.

Przedstawiając powyższe informuję, że realizację zadań dotyczących wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami (rejestrami) teleinformatycznymi oraz wspomagania usług drogą elektroniczną **ocenia się pozytywnie pomimo stwierdzonej nieprawidłowości.**

I.B. Systemy zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

Zgodnie z § 19 ust. 1 rozporządzenia w sprawie KRI, w okresie objętym kontrolą funkcjonował system zarządzenia bezpieczeństwem informacji (SZBI), w którego skład wchodziły następujące regulacje wewnętrzne, wprowadzone Zarządzeniem Starosty Wołomińskiego Nr 200.2023[9]:

- Polityka bezpieczeństwa informacji wraz z 2 załącznikami,
- Polityka bezpieczeństwa danych osobowych wraz z 4 załącznikami,
- Instrukcja zarządzania systemem informatycznym,
- Procedura realizacji praw osób, których dane dotyczą wraz z 2 załącznikami,
- Procedura zarządzania incydentami wraz z załącznikiem,
- Procedura zarządzania zmianą, szacowania ryzyka oraz oceny skutków wraz z załącznikiem.

Obowiązujące w okresie kontrolowanym regulacje wewnętrzne opisują m. in. sposoby nadawania, modyfikacji i odbierania uprawnień użytkownikom, zasady pracy w systemach informatycznych Starostwa, zasady wykonywania pracy na odległość, politykę haseł oraz politykę kluczy.

Obowiązujące dokumenty określały stopień zaangażowania kierownictwa urzędu w proces ustanawiania i funkcjonowania systemu zarządzania bezpieczeństwem informacji. W ocenie kontrolowanego organu w okresie objętym kontrolą nie zaistniały istotne zmiany otoczenia, o których mowa w § 19 ust. 2 pkt 1 rozporządzenia w sprawie KRI, wobec czego regulacje wewnętrzne dotyczące bezpieczeństwa informacji nie były w tym czasie aktualizowane[10].

W okresie poddanym kontroli Starostwo utrzymywało aktualność inwentaryzacji posiadanego sprzętu i oprogramowania służącego do przetwarzania informacji, poprzez prowadzenie w systemie teleinformatycznym[11] rejestru zasobów teleinformatycznych (tj. bazy konfiguracji CMDB[12]) zawierającego informację o wszystkich aktywach informatycznych oraz jego

---

9 Zarządzenie Starosty Wołomińskiego nr 200.2023 z 3 sierpnia 2023 roku w sprawie wprowadzenia w Starostwie Powiatowym w Wołominie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
10 Wyjaśnienia pisemne z 31 marca 2025 roku.
11 Przy pomocy oprogramowania XXXXXXXXXX.
12 Configuration Management Database.

aktualizację, stosownie do wymogów określonych w § 19 ust. 2 pkt 2 rozporządzenia w sprawie KRI.

W Starostwie obowiązywały procedury zarządzania ryzykiem uregulowane w Procedurze zarządzania zmianą, ryzykiem i oceną skutków. Przedmiotowa regulacja stanowi część składową SZBI funkcjonującego w Starostwie i określa sposób identyfikacji ryzyka oraz zasady szacowania ryzyka w obszarze bezpieczeństwa informacji oraz przetwarzania danych osobowych. W przedmiotowej procedurze określono poziom akceptowalnego ryzyka, jak również plan postępowania dla pozostałych ryzyk. Kontrolującym przedłożono arkusz analizy ryzyka przeprowadzonej w roku 2024. Powyższej analizy dokonano zgodnie z zasadami określonymi w obowiązującej procedurze, spełniając tym samym wymóg określony w § 19 ust. 2 pkt 3 rozporządzenia w sprawie KRI.

W jednostce kontrolowanej w okresie objętym kontrolą funkcjonowała procedura określająca sposób nadawania uprawnień do systemów teleinformatycznych spełniająca wymogi określone w § 19 ust. 2 pkt 4 oraz 5 powyższego rozporządzenia. W Starostwie działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych podejmowane są przez Naczelników Wydziałów. W trakcie trwania czynności kontrolnych analizie poddano historię nadawania i odbierania uprawnień do systemu XXXXXXXXXXXX funkcjonującego w Starostwie. Kontrolą objęto wnioski dotyczące 14[13] osób zatrudnionych w Wydziale Geodezji i Kartografii, Wydziale Ochrony Środowiska, Wydziale Budownictwa oraz Wydziale Inwestycji i Remontów, stwierdzając nadanie oraz odebranie uprawnień do pracy w badanym systemie teleinformatycznych zgodnie z obowiązującą procedurą uregulowaną w Instrukcji Zarządzania System Informatycznym[14].

W kontrolowanej jednostce zapewniono szkolenie osób zaangażowanych w proces przetwarzania informacji, stosownie do § 19 ust. 2 pkt 6 rozporządzenia w sprawie KRI. Kontrolującym przedłożono dokumentację dotyczącą przeprowadzonych w okresie kontrolowanym szkoleń z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji w postaci wydruku treści prezentacji wykorzystywanej w trakcie szkolenia oraz list uczestników.

W Starostwie ustanowiono zasady gwarantujące bezpieczną pracę przy przetwarzaniu informacji z wykorzystaniem urządzeń przenośnych i pracy na odległość, stosownie do wymogów zawartych w § 19 ust. 2 pkt 8 powyższego rozporządzenia. Analizie poddano regulację określającą zasady wykonywania pracy zdalnej[15] obowiązującą w okresie objętym

[13] Dotyczy wniosków o nadanie uprawnień dostępu do systemu e-property 10 pracownikom oraz 4 przypadki odebrania uprawnień dostępu osobom, które zakończyły zatrudnienie w Starostwie Powiatowym w Wołominie.
[14] W każdym z badanych przypadków o nadanie uprawnień drogą elektroniczną (e-mail) występował bezpośredni przełożony osoby (naczelnik wydziału), której nadawano uprawnienia.
[15] Regulamin pracy zdalnej w Starostwie Powiatowym w Wołominie wprowadzano Zarządzeniem Starosty Wołomińskiego nr 300 z 21 października 2024 roku.

kontrolą, jak również wszystkie złożone w tym okresie wnioski o wyrażenie zgody na świadczenie pracy w trybie zdalnym[16]. W wyniku ww. analizy stwierdzono, że we wszystkich przypadkach przedmiotowe wnioski zostały złożone na obowiązujących formularzach i zawierały komplet wymaganych załączników. Ponadto ustalono, że w okresie od 1 stycznia do 20 października 2024 roku osoby zatrudnione w Starostwie nie świadczyły pracy na odległość[17].

Kontroli poddano 14 umów zawartych pomiędzy Starostwem a podmiotami zewnętrznymi, przy czym 10 spośród ww. umów miała charakter typowo serwisowy, natomiast pozostałe 4 dotyczyły ochrony budynków, w których mieszczą się komórki organizacyjne Starostwa. Ustalono, że we wszystkich analizowanych umowach serwisowych określono precyzyjnie czas reakcji na przyjęte zgłoszenia usterek i awarii oraz maksymalny czas realizacji tych zgłoszeń. W umowach zawartych z agencją ochrony zawarto zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 10 rozporządzenia w sprawie KRI.

Stosownie do zapisów § 19 ust. 2 pkt 13 rozporządzenia w sprawie KRI, w Starostwie określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji[18]. W okresie objętym kontrolą miały miejsce incydenty naruszenia bezpieczeństwa informacji[19]. We wszystkich badanych przypadkach organ postępował zgodnie z obowiązującą w jednostce procedurą.

Zgodnie z wymogiem określonym w § 19 ust. 2 pkt 14 powyższego rozporządzenia, w okresie kontrolowanym w Starostwie przeprowadzono audyt w zakresie bezpieczeństwa informacji[20].

W okresie objętym kontrolą nie wystąpiły przypadki projektowania i wdrażania systemów teleinformatycznych, wobec czego spełnienie warunków określonych w § 15 ust. 1 rozporządzenia w sprawie KRI nie było przedmiotem kontroli.

W toku kontroli ustalono, że zgodnie z zapisami § 19 ust. 2 pkt 7, 9, 11 i 12 rozporządzenia w sprawie KRI, Starostwo zapewnia ochronę przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także stosuje zabezpieczanie

---

16 Dotyczy 14 wniosków, w tym 4 wniosków złożonych w roku 2024 oraz 10 wniosków złożonych w roku 2025.

17 Możliwość wykonywania pracy na odległość dotyczyła wówczas tylko telepracy i była uregulowana w §26 Regulaminu pracy Starostwa Powiatowego w Wołominie oraz załączniku nr 6 do przedmiotowego regulaminu, określającym warunki wykonywania telepracy. Powyższe regulacje zostały uchylone zarządzeniem wprowadzającym Regulamin pracy zdalnej.

18 Sposób postępowania zgłaszania i postępowania z incydentami bezpieczeństwa informacji określono w Procedurze zarządzania incydentami, będącej częścią składową obowiązującego w Starostwie SZBI.

19 Kontrolującym przedłożono dokumenty dotyczące 5 incydentów. We wszystkich ww. przypadkach zgłoszenia dotyczyły naruszeń ochrony danych osobowych.

20 Kontrolującym przedłożono harmonogram działań dotyczących realizacji zaleceń sformułowanych w raporcie z przeprowadzonego audytu. Z dokumentu wynika, które z ww. zaleceń już zrealizowano, a także w jakim terminie planowane jest zrealizowanie pozostałych zaleceń.

informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie, poprzez:

- zapewnienie zewnętrznej i wewnętrznej ochrony fizycznej obiektów,
- określenie pomieszczeń z ograniczonym dostępem, np. serwerowni oraz ustalenie zasad pobierania i zdawania kluczy do poszczególnych pomieszczeń,
- ustanowienie regulacji wewnętrznych określających zasady postępowania z informacjami w jednostce, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń, a także zasad zapewniających odpowiedni poziom bezpieczeństwa systemów teleinformatycznych,
- ograniczenie uprawnień użytkowników na stacjach roboczych,
- automatyczną aktualizację oprogramowania systemów operacyjnych serwerów oraz stacji roboczych,
- wykorzystywania na serwerach i stacjach roboczych systemów operacyjnych korzystających ze wsparcia producenta,
- tworzenie kopii zapasowych baz danych oraz systemów,
- wykorzystywanie urządzeń brzegowych typu firewall,
- zabezpieczenie serwerów i stacji roboczych aktualnym oprogramowaniem antywirusowym, automatycznie aktualizującym sygnatury wirusów,
- wyposażenie serwerów i urządzeń sieciowych w zasilanie awaryjne zabezpieczające system przed przepięciami i chwilowymi zanikami napięcia,
- ustanowienie regulacji dotyczących konserwacji, napraw i utylizacji sprzętu i oprogramowania,
- ustanowienie zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość.

Ponadto ustalono, że informacje w dziennikach systemów (logi) są przechowywane przez okres nie krótszy niż wskazany w § 20 ust. 3 rozporządzenia w sprawie KRI[21].

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
2. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

[21] Z protokołu sporządzonego 27 marca 2025 roku z rozmowy z informatykami zatrudnionymi w Starostwie oraz uzyskanych wyjaśnień wynika, że logi gromadzone są za pomocą oprogramowania xxxxxxxxx sukcesywnie od momentu uruchomienia każdej nowej stacji roboczej. Powyższa praktyka stosowana jest od momentu wdrożenia w Starostwie xxxxxxxxxxxxx, tj. od 2016 roku.

Ponadto podczas kontroli stwierdzono również, że w okresie objętym kontrolą miały miejsce przypadki XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXX.

Przedstawiając powyższe informuję, że realizację zadań w zakresie działania systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych **ocenia się pozytywnie pomimo stwierdzonych nieprawidłowości.**

Mając na uwadze powyższe ustalenia zobowiązuję Pana Starostę do podjęcia działań w celu wyeliminowania stwierdzonych nieprawidłowości, a w szczególności do:

1. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
2. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
3. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Ponadto zwracam uwagę na konieczność XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Przedstawiając powyższe informuję, że od wystąpienia pokontrolnego nie przysługują środki odwoławcze oraz zobowiązuję Pana Starostę do przekazania, w terminie 14 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków pokontrolnych lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości. Proszę o udzielenie powyższej informacji za pośrednictwem e-Doręczeń lub ePUAP.

Z wyrazami szacunku
z upoważnienia Wojewody Mazowieckiego
Lesław Kuczyński
Zastępca Dyrektora Wydziału Kontroli
/podpisano kwalifikowanym podpisem elektronicznym/