WOJEWODA MAZOWIECKI

Warszawa, 15 lipca 2024 r.

WK-I.431.2.2.2024

Pan
Adrian Ejssymont
Starosta Pruszkowski

Starostwo Powiatowe w Pruszkowie
ul. Drzymały 30
05-800 Pruszków

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 28 ust. 1 pkt 2 ustawy o wojewodzie i administracji rządowej w województwie , art. 6 ust. 4 pkt. 3 ustawy o kontroli w administracji rządowej oraz art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, kontrolerzy: Andrzej Nieszporek, Maria Los – starsi inspektorzy wojewódzcy oraz Dariusz Lichtblau – inspektor wojewódzki w Oddziale Kontroli Jednostek Samorządu Terytorialnego Wydziału Kontroli, a także Łukasz Plaskot – kierownik Oddziału Serwisu Informatycznego w Biurze Informatyki Mazowieckiego Urzędu Wojewódzkiego w Warszawie (dalej MUW), przeprowadzili w dniach od 18 marca do 12 kwietnia 2024 r. kontrolę problemową w Starostwie Powiatowym w Pruszkowie, z siedzibą w Pruszkowie przy ul. Drzymały 30 (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 teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej – w okresie od 1 stycznia 2023 r. do 12 kwietnia 2024 r.

Nawiązując do projektu wystąpienia pokontrolnego z 12 czerwca 2024 r., do którego nie wniesiono zastrzeżeń, przekazuję wystąpienie pokontrolne.

Ocenie poddano trzy główne obszary kontroli, tj. wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami informatycznymi oraz wspomaganie usług drogą elektroniczną, system zarządzania bezpieczeństwem informacji w systemach teleinformatycznych oraz zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych.

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[1] (dalej rozporządzenie w sprawie KRI).

Kontroli poddano systemy teleinformatyczne *XXXXXXXX* oraz *XXXXXXXXX* używane w Starostwie do realizacji zadań publicznych.

I. 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[2]. Starostwo umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw w formatach danych określonych w załączniku nr 2 rozporządzenia w sprawie KRI.

Na stronie podmiotowej BIP Starostwa https://bip.powiat.pruszkow.pl w zakładce: *Jak załatwić sprawę* umieszczono przekierowanie do opisów usług realizowanych przez jednostkę

---

[1] 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).

[2] 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).

kontrolowaną. Przedmiotowe karty usług pogrupowane są w zakładkach tematycznych dedykowanych poszczególnym komórkom organizacyjnym odpowiedzialnym za realizację danych usług. 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, wymaganych opłatach oraz przysługujących środkach odwoławczych.

Ustalono, że Starostwo nie przekazywało wzorów dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych oraz nie korzysta ze 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 UE, 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[3], natomiast system informatyczny XXXXXXXXX pełni funkcje wspomagające wykonywanie czynności kancelaryjnych w systemie tradycyjnym. Przedmiotowy system, zapewnia zintegrowaną obsługę korespondencji przychodzącej, wychodzącej i wewnętrznej, poprzez rejestrację, dekretację i zarządzanie obiegiem korespondencji.

Ustalono, że Starostwo posiada udokumentowane procedury dotyczące dostarczania i zarządzania usługami na deklarowanym poziomie dostępności, zgodnie z § 15 ust. 2 rozporządzenia w sprawie KRI. Kontrolującym przedstawiono wykaz 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.**

---

[3] Zarządzenie Starosty Pruszkowskiego nr 2/2011 z 25 stycznia 2011 roku (zarządzenie wprowadzające) oraz Zarządzenie Starosty Pruszkowskiego nr 27/2017 z 4 sierpnia 2017 roku (zarządzenie zmieniające).

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

Zgodnie z § 19 ust. 1 rozporządzenia w sprawie KRI, w okresie objętym kontrolą funkcjonował system zarządzenia bezpieczeństwem informacji (dalej SZBI), w którego w skład wchodziły następujące regulacje wewnętrzne, wprowadzone poniższymi Zarządzeniami Starosty Pruszkowskiego:

- Nr 51/2019 z dnia 20 sierpnia 2019 r. w sprawie instrukcji określającej zabezpieczenie pomieszczeń i budynku Starostwa Powiatowego w Pruszkowie oraz zasady dysponowania kluczami,
- Nr 32/2020 z dnia 13 lipca 2020 r. w sprawie polityki ochrony danych osobowych,
- Nr 34/2020 z dnia 17 lipca 2020 r. w sprawie powołania koordynatora do spraw kontroli zarządczej w Starostwie Powiatowym w Pruszkowie,
- Nr 36/2020 z dnia 10 sierpnia 2020 r. w sprawie instrukcji zarządzania systemem informatycznym,
- Nr 46/2020 z 9 listopada 2020 r. w sprawie regulaminu kontroli zarządczej w Starostwie Powiatowym w Pruszkowie i jednostkach organizacyjnych powiatu pruszkowskiego,
- Nr 49/2020 z dnia 1 grudnia 2020 r. w sprawie wprowadzenia instrukcji inwentaryzacyjnej,
- Nr 20/2021 z dnia 21 maja 2021 r. w sprawie regulaminu zarządzania ryzykiem w Starostwie Powiatowym w Pruszkowie,
- Nr 41/2021 z dnia 22 grudnia 2021 r. w sprawie wprowadzenia regulaminu korzystania z elektronicznego systemu kontroli dostępu do pomieszczeń w Starostwie Powiatowym w Pruszkowie,
- Nr 25/2023 z dnia 31 sierpnia 2023 r. w sprawie wprowadzenia regulaminu pracy zdalnej w Starostwie Powiatowym w Pruszkowie,
- Nr 26/2023 z dnia 12 wrześnie 2023 r. w sprawie wprowadzenia regulaminu funkcjonowania, obsługi i eksploatacji monitoringu wizyjnego na terenie Starostwa Powiatowego w Pruszkowie,
- Nr 35/2023 z dnia 27 listopada 2023 r. w sprawie wyznaczenie osoby odpowiedzialnej w Starostwie Powiatowym w Pruszkowie za utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa,
- Nr 6/2024 z dnia 1 marca 2024 r. w sprawie powołania Zespołu Bezpieczeństwa Informacji,

- Nr 7/2024 z dnia 1 marca 2024 r. w sprawie wyznaczenia członków Zespołu Bezpieczeństwa Informacji,
- Nr 8/2024 z dnia 1 marca 2024 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Pruszkowie,
- Nr 9/2024 z dnia 1 marca 2024 r. w sprawie wprowadzenia systemu ciągłością działania w Starostwie Powiatowym w Pruszkowie.

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

W toku kontroli potwierdzono zaangażowanie kierownictwa Starostwa w proces ustanawiania i funkcjonowania systemu bezpieczeństwa informacji przejawiające się głównie ustanowieniem i wdrożeniem SZBI, udziałem kadry kierowniczej w szkoleniach dotyczących SZBI, a także powołaniem Zespołu Bezpieczeństwa Informacji składającego się z osób posiadających wiedzę ekspercką z obszaru bezpieczeństwa informacji, których zadaniem jest nadzór nad funkcjonowaniem SZBI, uczestnictwo w przeglądach i audytach bezpieczeństwa informacji.

W okresie poddanym kontroli Starostwo utrzymywało aktualność inwentaryzacji posiadanego sprzętu i oprogramowania służącego do przetwarzania informacji, poprzez prowadzenie w systemie teleinformatycznym[4] rejestru zasobów teleinformatycznych (tj. bazy konfiguracji CMDB[5]) zawierającego informację o wszystkich aktywach informatycznych, stosownie do wymogów określonych w § 19 ust. 2 pkt 2 rozporządzenia KRI.

W Starostwie obowiązywały procedury zarządzania ryzykiem stanowiące *Regulamin zarzadzania ryzykiem*. Przedmiotowa regulacja określa sposób identyfikacji ryzyka oraz zasady szacowania ryzyka w obszarze bezpieczeństwa informacji oraz przetwarzania danych osobowych. Ponadto w ww. regulaminie określono poziom akceptowalnego ryzyka, jak również plan postępowania z ryzykiem. Kontrolującym przedłożono arkusze analizy ryzyka przeprowadzonej dla dwóch wybranych komórek organizacyjnych Starostwa w roku 2023 oraz na początku roku 2024. Powyższej analizy dokonano na podstawie ww. regulaminu stosownie do wymogów określonych w § 19 ust. 2 pkt 3 rozporządzenia w sprawie KRI.

Pracownicy wykonujący zadania w systemach teleinformatycznych uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do przypisanych obowiązków,

---

4 Przy pomocy oprogramowania *XXXXXXXXX*.
5 Configuration Management Database.

zgodnie z § 19 ust. 2 pkt. 4 powyższego rozporządzenia. W Starostwie działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych podejmowanie są przez Naczelników Wydziału. W trakcie trwania czynności kontrolnych analizie poddano historię odbierania uprawnień do systemu *XXXXXXX* oraz *XXXXXXX* funkcjonującego w Starostwie dla dwunastu pracowników Wydziału XXXXXXXXXXXX, tj. dla trzech osób nowo zatrudnionych (nadanie uprawnień), czterech osób, które zakończyły zatrudnienie w jednostce (odebranie uprawnień), oraz pięciu użytkowników, którym zmieniono uprawnienia (zmiana zakresu czynności), stwierdzając odpowiednio adekwatność poziomu ich uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i realizowanych zadań oraz bezzwłoczne odbieranie posiadanych uprawnień, czym spełniono wymagania wskazane w 19 ust. 2 pkt 4 i 5 rozporządzenia KRI. Ponadto stwierdzono, że czynności nadania, utraty i zmiany uprawnień dla pracowników Starostwa dokonywano zgodnie z funkcjonującą w Starostwie Instrukcją Zarządzania Systemem Informatycznym[6].

W kontrolowanej jednostce zapewniono szkolenie osób zaangażowanych w proces przetwarzania informacji, stosownie do § 19 ust. 2 pkt 6 rozporządzenia KRI. Kontrolującym przedłożono dokumentację dotyczącą przeprowadzonych w okresie kontrolowanym szkoleń z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji w postaci programów szkoleń, list uczestników, a także harmonogramu szkoleń zaplanowanych w najbliższym okresie (związanych z wprowadzoną 1 marca 2024 r. Polityką Bezpieczeństwa Informacji).

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 Regulamin pracy zdalnej obowiązujący w okresie objętym kontrolą, jak również wszystkie złożone w tym okresie wnioski o wyrażenie zgody na świadczenie pracy w trybie zdalnym[7]. W wyniku ww. analizy stwierdzono, że we wszystkich przypadkach przedmiotowe wnioski zostały złożone na obowiązujących formularzach i zawierały komplet wymaganych załączników.

W umowach zawartych pomiędzy Starostwem a podmiotami zewnętrznymi[8] wskazano zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 10 powyższego rozporządzenia. Ponadto ustalono, że we wszystkich umowach typowo

---

[6] Aktualnie nadawanie, zmiana oraz odbieranie uprawnień dostępu do zasobów informatycznych Starostwa odbywa się na podstawie Procedury zarządzania systemem informatycznym, stanowiącej załącznik nr 5 do Polityki Bezpieczeństwa Informacji wprowadzonej 1 marca 2024 r.

[7] Dotyczy 6 wniosków, w tym 3 wniosków złożonych w roku 2023 oraz 3 wniosków złożonych w roku 2024.

[8] Wykaz zawartych przez Starostwo umów z podmiotami zewnętrznymi ujęto w arkuszu ustaleń kontroli nr 3.

serwisowych określono precyzyjnie czas reakcji na przyjęte zgłoszenia usterek i awarii oraz maksymalny czas realizacji tych zgłoszeń. Jednocześnie we wszystkich przypadkach, gdy umowa dotyczyła, lub potencjalnie mogła dotyczyć, przetwarzania danych osobowych, z wykonawcą zawierano stosowną umowę o powierzeniu przetwarzania danych osobowych.

Stosownie do zapisów § 19 ust. 2 pkt 13 rozporządzenia KRI, w Starostwie określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji[9].

Zgodnie z wymogiem określonym w § 19 ust. 2 pkt 14 powyższego rozporządzenia, w okresie kontrolowanym w Starostwie przeprowadzono audyt w zakresie bezpieczeństwa informacji, a także audyt zgodności z ustawą o Krajowym Systemie Cyberbezpieczeństwa[10].

W okresie objętym kontrolą w Starostwie tworzono i testowano kopie zapasowe baz danych i systemów czym spełniono wymogi określone § 19 ust. 2 pkt 12 lit. b powyższego rozporządzenia.

W okresie objętym kontrolą nie wystąpiły przypadki projektowania i wdrażania systemów teleinformatycznych, wobec czego spełnienie warunków określonych w § 15 ust. 1 powyższego rozporządzenia nie było przedmiotem kontroli[11].

Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami w jednostce, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji w tym urządzeń oraz zasady dotyczące zapewnienia ochrony przetwarzanych informacji, zostały zawarte w Instrukcji zarzadzania systemem informatycznym w Starostwie Powiatowym w Pruszkowie, obowiązującej w okresie objętym kontrolą[12].

W toku kontroli ustalono, że zgodnie z zapisami § 19 ust. 2 pkt 7, 9, 11 i 12 rozporządzenia KRI, Starostwo zapewnia ochronę przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także stosuje zabezpieczanie informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie[13].

---

[9] Sposób zgłaszania i postępowania z incydentami bezpieczeństwa informacji określono w Procedurze zarządzania incydentem bezpieczeństwa informacji, stanowiącej załącznik nr 4 do Polityki Bezpieczeństwa Informacji wprowadzonej 1 marca 2024 r. Pierwotny brak ww. procedury był przedmiotem wniosku sformułowanego w raporcie z audytu przeprowadzonego 15 grudnia 2023 roku.

[10] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, ze zm.).

[11] Kontrolującym przedstawiono 4 umowy dotyczące wdrożenia elementów infrastruktury teleinformatycznej lub gotowych systemów informatycznych objętych zakupionymi licencjami.

[12] Aktualnie opisywane zagadnienia reguluje Procedura zarządzania systemem informatycznym, stanowiąca załącznik nr 5 do Polityki Bezpieczeństwa Informacji wprowadzonej 1 marca 2024 r.

[13] Ochrona informacji jest realizowana poprzez m.in.:
- zapewnienie zewnętrznej i wewnętrznej ochrony fizycznej obiektów,
- określenie pomieszczeń z ograniczonym dostępem, np. serwerowni oraz ustalenie zasad pobierania i zdawania kluczy do poszczególnych pomieszczeń,

W wyniku kontroli stwierdzono nieprawidłowość polegającą na XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX..

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

III. Zapewnienie dostępności informacji zawartych na stronach internetowych jednostki dla osób niepełnosprawnych.

Strony internetowe Starostwa działające pod adresami https://samorzad.gov.pl/web/powiat-pruszkowski (strona internetowa Starostwa) oraz https://bip.powiat.pruszkow.pl/ (strona podmiotowa BIP Starostwa) poddano weryfikacji zgodności ze standardem WCAG 2.0 za pomocą narzędzia Wave Accessibility Evaluation Tool.

Przeprowadzona przez kontrolujących w dniu 9 kwietnia 2024 r. walidacja ww. stron internetowych Starostwa za pomocą ww. narzędzia wykazała odpowiednio XXXXXXXXXX w przypadku strony internetowej Starostwa oraz XXXXXXXXX w przypadku strony podmiotowej BIP Starostwa.

- 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,
- 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.

Po weryfikacji ww. stron internetowych stwierdzono spełnienie wymagań WCAG 2.0 określonych w załączniku nr 4 rozporządzenia w sprawie KRI. W wyniku kontroli stwierdzono, że dostępna strona internetowa i strona BIP Starostwa zawierają rozwiązania techniczne umożliwiające osobom niepełnosprawnym zapoznanie się z treścią informacji, czym spełniono wymogi określone w § 19 powyższego rozporządzenia[14].

Przedstawiając powyższe informuję, że realizację zadania w przedmiocie zapewnienia dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych ocenia się **pozytywnie**.

Mając na uwadze powyższe ustalenia zobowiązuję Pana Starostę do podjęcia działań w celu wyeliminowania stwierdzonej nieprawidłowości poprzez XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

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 up. WOJEWODY MAZOWIECKIEGO

Artur Subda
Dyrektor Wydziału Kontroli

/podpisano kwalifikowanym
podpisem elektronicznym/

[14] W brzmieniu obowiązującym do 23 maja 2024 r. Aktualnie wymagania dotyczące dostępności stron internetowych regulowane są w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).