Bydgoszcz, 20 sierpnia 2018 r.

WOJEWODA KUJAWSKO-POMORSKI

WNK.III.431.1.2.2018.BG.GL.

Pan
Wojciech Oskwarek
Wójt Gminy Nowa Wieś Wielka
ul. Ogrodowa 2
86-060 Nowa Wieś Wielka

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 16 ust. 2 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1] oraz art. 25 ust. 1 pkt 3a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2] (dalej: ustawa o informatyzacji) w Gminie Nowa Wieś Wielka, ul. Ogrodowa 2, 86-060 Nowa Wieś Wielka w dniach: 7, 11, 22 czerwca 2018 r. przeprowadzona została kontrola prawidłowości przez starszego inspektora wojewódzkiego, nr upoważnienia 371/2018 w zakresie:
1. przedmiot kontroli: wykorzystywanie systemów teleinformatycznych do realizacji zadań publicznych.
2. okres objęty kontrolą: od 1 stycznia 2017 r. do dnia rozpoczęcia kontroli.

W wyniku przeprowadzonej kontroli kontrolowaną działalność jednostki ocenia się pozytywnie z nieprawidłowościami.

Dokonana ocena została oparta o następującą skalę ocen:
- pozytywna,
- pozytywna z uchybieniami,
- pozytywna z nieprawidłowością,
- pozytywna z nieprawidłowościami,
- negatywna (po przekroczeniu przyjętego progu istotności).

Kontrolę przeprowadzono w poniższych obszarach.

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

[1] Dz.U. Nr 185, poz. 1092.
[2] Dz. U. z 2017 r. poz. 570, ze zm.

W ramach tego obszaru poddano kontroli:

1.1. Usługi elektroniczne;
1.2. Centralne repozytorium wzorów dokumentów elektronicznych;
1.3. Model usługowy;
1.4. Współpracę systemów teleinformatycznych z innymi systemami;
1.5. Obieg dokumentów w podmiocie publicznym;
1.6. Formaty danych udostępniane przez systemy teleinformatyczne.

2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

W ramach tego obszaru poddano kontroli:

2.1. Dokumenty z zakresu bezpieczeństwa informacji;
2.2. Analizę zagrożeń związanych z przetwarzaniem informacji;
2.3. Inwentaryzację sprzętu i oprogramowania informatycznego;
2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych;
2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji;
2.6. Pracę na odległość i mobilne przetwarzanie danych;
2.7. Serwis sprzętu informatycznego i oprogramowania;
2.8. Procedury zgłaszania incydentów naruszenia BI;
2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji;
2.10. Kopie zapasowe;
2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych;
2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji;
2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych;
2.14. Rozliczalność działań w systemach informatycznych.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych.

Oceny dokonano na podstawie poniższych ustaleń.

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami.

1.1. Usługi elektroniczne.

Podmiot kontrolowany udostępnia elektroniczną skrzynkę podawczą, zgodnie z art. 16 ust. 1a ustawy o informatyzacji.

Podmiot kontrolowany udostępnia przez sieć Internet 26 usług elektronicznych. Na stronie BIP Nowej Wsi Wielkiej znajduje się odesłanie do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[3] (dalej: rozporządzenie KRI).

1.2. Centralne repozytorium wzorów dokumentów elektronicznych.

W Centralnym Repozytorium Wzorów Dokumentów Elektronicznych zamieszczono następujące formularze: Deklaracja na podatek od nieruchomości, Informacja w sprawie

[3] Dz. U. z 2016 r. poz. 113

podatku od nieruchomości, Deklaracja na podatek rolny, Deklaracja na podatek leśny, Informacja w sprawie podatku leśnego. Kontrolowany podmiot przekazał do CRWDE procedury obsługi usług zgodnie z art. 19 b ust. 3 ustawy z dnia 24 lutego 2017 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.[4]

1.3. Model usługowy.
W podmiocie kontrolowanym nie istnieją wewnętrzne procedury dotyczące obsługi usług elektronicznych oraz monitoringu dotyczącego dostarczania ich na zadeklarowanym poziomie. Stanowi to naruszenie § 15 ust. 2 rozporządzenia KRI, w którym jest mowa o tym, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne odbywa się w oparciu o udokumentowane procedury. Tym samym nie ma możliwości zweryfikowania sposobu realizacji tych procedur.

Poszerzanie dostępu do usług świadczonych drogą elektroniczną jest realizowane przez zamieszczenie ich w ePuapie w formie kart usług.

1.4. Współpraca systemów teleinformatycznych z innymi systemami.
Kwestie współpracy systemów teleinformatycznych z innymi systemami regulują § 5 ust. 3 pkt 3 oraz § 16 ust. 1 rozporządzenia KRI.
W toku kontroli ustalono, że poziom współpracy wewnętrznych systemów z innymi systemami odbywa się głównie na poziomie komunikacji jednostronnej. W związku z powyższym Urząd Gminy Nowa Wieś Wielka nie posiada podpisanych umów z podmiotami prowadzącymi rejestry referencyjne.

Jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej, zdolność współdziałania systemów teleinformatycznych zwiększana jest poprzez trwające prace nad pełną integracją systemów. Ostatecznym efektem tych prac będzie wdrożenie Elektronicznego Biura Obsługi Interesanta (dalej: EBOI), do którego użytkownik będzie mógł zalogować się przy użyciu profilu zaufanego. Usprawnienie to obejmie również integrację z planowanym do wdrożenia elektronicznym obiegiem dokumentów „Proton". Po wdrożeniu wszystkich planowanych integracji wymiana danych będzie odbywała się pomiędzy systemami dziedzinowymi, obiegiem dokumentów oraz EBOI za pośrednictwem ePuapu.

1.5. Obieg dokumentów w podmiocie publicznym.
Do zagadnienia obiegu dokumentów odnosi się § 20 ust. 2 pkt 9 rozporządzenia KRI.
W podmiocie kontrolowanym nie wprowadzono wewnętrznych regulacji opisujących sposób zarządzania dokumentacją, w tym dotyczących stosowania elektronicznego obiegu dokumentów. Tym samym obieg dokumentów na chwilę obecną regulowany jest tylko przez rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.[5]
Jak wyjaśnił pełnomocnik ds. obsługi organów Gminy i obsługi informatycznej zastosowane systemy (księgowe i podatkowe) w Urzędzie Gminy Nowa Wieś Wielka umożliwiają wymianę danych między sobą w zakresie danych dotyczących podatników. Obecnie trwają prace nad pełną integracją systemów. Usprawnienie to obejmuje również integrację z planowanym do wdrożenia elektronicznym obiegiem dokumentów „Proton" firmy Sputnik Software. Po wdrożeniu wszystkich planowanych integracji wymiana danych, w tym obieg dokumentów, będzie odbywała się pomiędzy systemami dziedzinowymi oraz EBOI za pośrednictwem ePuapu.

[4] Dz.U. z 2017 r. poz. 570, ze zm.
[5] Dz. U. z 2011 r. nr 14 poz. 67, ze zm.

1.6. Formaty danych udostępniane przez systemy teleinformatyczne.
Omawiany obszar reguluje § 17 ust. 1 oraz § 18 ust. 1-2 rozporządzenia KRI.
Dokumenty kierowane na skrzynkę podawczą podmiotu mogą być tworzone w jednym z formatów: ODT, DOC, RTF, ODS, XLS, CSV, TXT, TIF, JPG, PDF, ZIP. Są to formaty danych określone w załączniku nr 2 do rozporządzenia KRI. Tym samym spełnione są wymagania określone ww. przepisach. Urząd umożliwia ponadto kierowanie do podmiotu formatów załączników nieprzewidzianych w rozporządzeniu KRI, tj. GIF oraz BMP.

2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.
2.1. Dokumenty z zakresu bezpieczeństwa informacji.
W zakres dokumentów stanowiących System zarządzania bezpieczeństwem informacji (dalej: SZBI) wchodzą:
a) wprowadzone zarządzeniem z dnia 22 września nr 20/15 Wójta Gminy Nowa Wieś Wielka:
- Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Nowa Wieś Wielka;
- Instrukcja zarządzania systemami informatycznymi w Urzędzie Gminy Nowa Wieś Wielka.

b) dokumentacja audytów wewnętrznych.

c) zarządzenie nr 7/18 Wójta Gminy Nowa Wieś Wielka z dnia 24 maja 2018 r. RO-I.120.7.2018 w sprawie wprowadzenia rejestru czynności przetwarzania danych osobowych w Urzędzie Gminy Nowa Wieś Wielka.

d) raport ze stycznia 2015 r. z analizy i oceny zgodności środków technicznych i organizacyjnych w Urzędzie Gminy Nowa Wieś Wielka z przepisami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz wymagań prawnych w zakresie ochrony danych osobowych oraz rekomendacja działań doskonalących w tym zakresie.

e) Jednolita Analiza Kontrolna Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych zgodnie z ustawą o informatyzacji z dnia 24 listopada 2017 r.

Istnienie powyższych dokumentów wypełnia wymagania określone w § 20 ust. 1 rozporządzenia KRI odnoszące się do opracowania, ustanowienia, wdrożenia SZBI.
Z kolei wypełnienie obowiązku wynikającego z § 20 ust. 2 pkt 1 rozporządzenia KRI dotyczącego aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia realizowane jest poprzez coroczne opracowywanie planu audytu oraz sprawozdania z audytu.
Należy zauważyć, że Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Nowa Wieś Wielka ogranicza się w swoich regulacjach do kwestii bezpieczeństwa przetwarzania danych osobowych pomijając aspekt bezpieczeństwa przetwarzania wszelkich innych informacji jakimi dysponuje podmiot kontrolowany. Ta sama uwaga dotyczy Instrukcji zarządzania systemem informatycznym.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji.
W jednostce brak jest regulacji wewnętrznych opisujących sposób zarządzania ryzykiem Bezpieczeństwa Informacji. Brak jest dokumentacji potwierdzającej przeprowadzanie okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestru ryzyk zawierającego informacje o zidentyfikowanych ryzykach, ich poziomie. Brak jest też planu postępowania z ryzykiem, co narusza § 20 ust. 2 pkt 3 rozporządzenia KRI

zobowiązujący do przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz do podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
Jednostka dysponuje szablonem, który mógłby być wykorzystany do sporządzenia takiego planu. Szablon ten określony jest w załączniku nr 6 do Jednolitej Analizy Kontrolnej Krajowych Ram Interoperacyjności przy przetwarzaniu danych osobowych zgodnie z ustawą o informatyzacji. Jest to jednak szablon, który dotyczy planu postępowania z ryzykiem tylko przy przetwarzaniu danych osobowych.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego.
Przepis § 20 ust. 2 pkt 2 rozporządzenia KRI, zobowiązuje do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Funkcję rejestru zasobów informatycznych pełni obecnie oprogramowanie Axence nVision, które umożliwia kontrolę nad infrastrukturą IT, prowadzenie listy zainstalowanego/używanego oprogramowania, usprawnienie zarządzania stacjami roboczymi oraz łatwiejsze planowanie nowych zakupów, a także ewidencję środków trwałych IT.

W jednostce nie zostały ustanowione procedury przydzielania, zwrotu sprzętu i oprogramowania. Niemniej w sytuacji konieczności utylizacji sprzętu zawierana jest stosowna umowa zlecenia, w ramach której podmiot zewnętrzny obliguje się do fizycznego zniszczenia wskazanych nośników, sprzętu. Ponadto dokumentacja środków trwałych prowadzona w księgowości wskazuje kto jest użytkownikiem danego sprzętu. W praktyce przydzielanie i zwrot sprzętu i oprogramowania odbywa się w oparciu o bieżące potrzeby -- w razie zmian kadrowych lub zmian wynikających ze zużycia sprzętu i wystąpienia nieodwracalnych awarii.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych.
Obowiązek wynikający z § 20 ust. 2 pkt 4 rozporządzenia KRI dotyczy podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.
Uprawnienia administratora zasobów IT w Urzędzie Gminy posiada podinspektor ds. obsługi organów Gminy i obsługi informatycznej, który pełni funkcję administratora systemu informatycznego.
Ochrona systemów i sieci teleinformatycznych należy do obowiązków pełnomocnika ds. ochrony informacji niejawnych, bezpieczeństwa publicznego, spraw obronnych i bhp.
W § 11 Polityki bezpieczeństwa (...) wskazano, że dane osobowe mogą być przetwarzane w Urzędzie tylko przez osoby posiadające upoważnienie do przetwarzania danych wydane przez Wójta. Zgodnie z § 11 ust. 2 Polityki bezpieczeństwa (...) w Urzędzie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych. Upoważnienie do przetwarzania danych dla pracownika Urzędu wydawane jest zgodnie z § 12 ust. 1 Polityki bezpieczeństwa (...) na wniosek kierownika referatu lub samodzielnego stanowiska.

Ponadto w ramach dostosowania do obowiązujących przepisów związanych z wejściem RODO[6] w jednostce wprowadzone zostało zarządzenie nr 7/18 Wójta Gminy Nowa Wieś Wielka z dnia 24 maja 2018 r. RO-I.120.7.2018 w sprawie wprowadzenia rejestru czynności

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

przetwarzania danych osobowych w Urzędzie Gminy Nowa Wieś Wielka.

Z kolei § 20 ust. 2 pkt 5 rozporządzenia KRI zobowiązuje do bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób uczestniczących w procesie przetwarzania informacji.
W okresie kontrolowanym jedna osoba przeszła na emeryturę i jej obowiązki przejął pracownik zatrudniony już wcześniej w Urzędzie. Należy zaznaczyć, że wspomniane obowiązki dotyczyły pracy z systemem „Źródło", którym zarządza Ministerstwo Cyfryzacji. Zgodnie ze złożonymi wyjaśnieniami procedura odebrania i nadania uprawnień jest przeprowadzana za pośrednictwem portalu internetowego Ministerstwa Cyfryzacji. Tym samym procedurę nadania i odebrania uprawień przeprowadza Ministerstwo Cyfryzacji, a Urząd tylko ją inicjuje. Osoba obsługująca „Źródło" legitymuje się stosownym certyfikatem.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.
W jednostce nie istnieją regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesy przetwarzania informacji w systemach teleinformatycznych.
W świetle złożonych wyjaśnień szkolenia w zakresie bezpieczeństwa informacji przeszedł każdy pracownik. Jak wyjaśniono każdy pracownik podpisał też stosowną informację, która jest wpięta w jego akta osobowe. Przy czym informacja odnosi się tylko do danych osobowych konkretnego pracownika.
Należy zauważyć, że w kontrolowanym okresie nie wszyscy pracownicy zaangażowani w proces przetwarzania informacji brali udział w szkoleniach.
W kontrolowanym okresie odbyło się pięć szkoleń związanych z obszarem kontroli.
- 31sierpnia 2017 r. - „Prowadzenie Biuletynu Informacji Publicznej - informacje praktyczne". Udział wzięły dwie osoby.
- 14 maja 2018 r. - „Ochrona danych osobowych w działach kadr zgodnie z RODO - praktyczne stosowanie nowego rozporządzenia w sprawie ochrony (...) danych osobowych od rekrutacji do rozwiązania umowy o pracę". Udział wzięła jedna osoba.
- 18 maja 2018 r. - „Stosowanie przepisów europejskiego ogólnego rozporządzenia o ochronie danych osobowych w jst". Udział wzięły dwie osoby.
- 23 maja 2018 r. - „Rozporządzenie RODO i nowelizacja ustaw o ewidencji ludności i dowodach osobistych od 25.05.2018 r. i ich wpływ na aplikację Źródło i na prowadzone rejestry mieszkańców". Udział wzięła jedna osoba.
- 29 maja 2018 r. - „Udostępnianie informacji publicznej w świetle wymogów RODO i nowej ustawy o ochronie danych osobowych". Udział wzięły dwie osoby.
Tematyka szkoleń nie wyczerpuje zakresu wskazanego w § 20 ust. 2 pkt 6 rozporządzenia KRI, zgodnie z którym w ramach szkolenia należy uwzględnić takie zagadnienia jak:
a) zagrożenia bezpieczeństwa informacji,
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

2.6. Praca na odległość i mobilne przetwarzanie danych.
Jednostka nie ustanowiła podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Stanowi to naruszenie wymogu wynikającego z § 20 ust. 2 pkt 8 rozporządzenia KRI.
Ze złożonych wyjaśnień wynika, że powyższe uchybienie wynika z tego, że nie przewiduje się potrzeby i konieczności pracy na odległość. Poza tym pracownicy nie mają dostępu

do zasobów informatycznych (w tym baz danych) spoza wewnętrznej sieci urzędowej.

2.7. Serwis sprzętu informatycznego i oprogramowania.
Regulacje wewnętrzne odnoszące się do wykonywania przeglądów i konserwacji systemu znajdują się w rozdziale 10 Instrukcji zarządzania systemem informatycznym (wspomnianej w pkt 2.1. lit. a). Zgodnie z zawartymi tam uregulowaniami przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu. Ponadto konserwacja baz danych powinna być przeprowadzana zgodnie z zaleceniami twórców poszczególnych programów.
Brak jest natomiast regulacji wewnętrznych określających zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych.
Natomiast zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI w umowach serwisowych podpisanych ze stronami trzecimi powinny znajdować się zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.
Umowa zawarta 2 stycznia 2018 r. nr 79/OI/2018 pomiędzy Gminą Nowa Wieś Wielka a Ośrodkiem Informatyki w Bydgoszczy - Centrum Edukacyjnym Spółką z ograniczoną odpowiedzialnością (wykonawcą) zobowiązała wykonawcę do nadzoru autorskiego nad zainstalowanymi w Urzędzie dziewięcioma systemami informatycznymi. Wspomniany nadzór autorski ma polegać na dostarczaniu nowych wersji oprogramowania wynikających ze zmiany przepisów oraz wprowadzanych przez autorów tych systemów ulepszeń z wyłączeniem zmian powodujących konieczność przebudowy relacyjnej struktury bazy danych lub wewnętrznej architektury aplikacji. W § 7 umowy wskazano, że wykonawca zobowiązuje się do zachowania w tajemnicy i do nieudostępniania innym osobom informacji, do których ma dostęp w wykonywaniu umowy oraz zobowiązuje się do przestrzegania postanowień wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.[7] *Umowa wymaga przeglądu i aktualizacji chociażby ze względu na nieaktualność wskazanej w niej ustawy o ochronie danych osobowych.*

Ponadto Gmina Nowa Wieś Wielka zawarła z innym wykonawcą 2 stycznia 2018 r. umowę nr 032.2.2018 obejmującą odpłatne administrowanie serwera i bramy internetowej. W ramach umowy wykonawca zobowiązał się do następujących czynności:

1) w zakresie instalacji oprogramowania:
   a) instalacja oprogramowania serwerowego,
   b) reinstalacja systemu w razie potrzeby,
2) w zakresie konserwacji zainstalowanego oprogramowania:
   a) porządkowanie danych w systemie,
   b) nadawanie niezbędnych uprawnień do zasobów zarządzania,
   c) konfiguracja aktualizacji:
      - sprawowanie nadzoru i kontroli nad bezpieczeństwem systemu,
      - tworzenie comiesięcznych backup-ów wybranych zasobów,
   d) w zakresie wykonywania konserwacji zainstalowanego systemu:
   - ocena efektywności zabezpieczeń systemu oraz dokonywanie ewentualnych zmian, rozbudowa sieci,
   e) w zakresie doradztwa:
   - informowanie o nowych technologiach informatycznych możliwych do zaimplementowania.

W § 3 ust. 3 umowy określono czas reakcji na zgłoszenie problemu na osiem godzin. Wszelkie naprawy systemu na 24 godziny. *Wspomniana umowa nakłada na wykonawcę*

[7] Umowa odwołuje się do Dz. U. z 2016 r. poz. 922, natomiast obecnie obowiązuje ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

w § 3 ust. 3 obowiązek składania „pisemnego raportu (notatki służbowej) o stanie faktycznej sprawności urządzeń do ostatecznego dnia miesiąca rozliczeniowego". W trakcie kontroli stwierdzono, że obowiązek ten nie jest realizowany, a ze strony zamawiającego nie są podejmowane odpowiednie kroki w celu jego wyegzekwowania.

W § 6 zawarte zostały zobowiązania obu stron umowy do zachowania w tajemnicy wszelkich informacji na temat drugiej strony.

2.8. Procedury zgłaszania incydentów naruszenia BI.

W jednostce nie wprowadzono regulacji wewnętrznych określonych w § 20 ust. 2 pkt 13 rozporządzenia KRI, tj. dotyczących zgłaszania incydentów naruszenia bezpieczeństwa informacji. Nie jest prowadzony rejestr incydentów naruszenia BI. Wskutek powyższego brak jest też dokumentacji potwierdzającej wykonywanie takich procedur.

Ze złożonych wyjaśnień wynika, że w kontrolowanym okresie nie doszło do incydentów naruszenia bezpieczeństwa informacji.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Jednostka nie posiada regulacji wewnętrznych, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI, co narusza § 20 ust. 2 pkt 14 rozporządzenia KRI.

Niemniej jednak audyty wewnętrzne obejmujące kwestie związane z bezpieczeństwem informacji są cyklicznie przeprowadzane, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.

Jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej wyniki audytów wykorzystano m.in. do zakupienia programu Axence nVision.

Wspomnieć tu należy również o raporcie ze stycznia 2015 r. z analizy i oceny zgodności środków technicznych i organizacyjnych w Urzędzie Gminy Nowa Wieś Wielka z przepisami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz wymagań prawnych w zakresie ochrony danych osobowych oraz rekomendacji działań doskonalących w tym zakresie. *Krytycznie należy się jednak odnieść do faktu, że część rekomendacji sformułowanych w ramach tego dokumentu nie została do tej pory zrealizowana. Na przykład autorzy stwierdzili, że ewidencja sprzętu prowadzona jest jedynie w księgowości jako środki trwałe oraz brak jest opisu konfiguracji infrastruktury i sieci. W związku z tym przedłożyli kilka rekomendacji:*

- wdrożenie procedury zarządzania zmianą, której elementem powinno być zagwarantowanie aktualności prowadzonej dokumentacji.

2.10. Kopie zapasowe.

Regulacje prawa powszechnie obowiązującego odnoszące się do sporządzania kopii zapasowych znajdują się w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, mówiącego o konieczności minimalizowania ryzyka utraty informacji w wyniku awarii.

Regulacje wewnętrzne dotyczące tworzenia kopii zapasowych znajdują się w rozdziale 5 Instrukcji zarządzania systemem informatycznym (...). Zgodnie z treścią rozdziału 5 ust. 2 Instrukcji zarządzania systemem informatycznym (...) za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego, w przypadku jego nieobecności inna wyznaczona osoba. Zgodnie z ust. 3 pełne kopie bezpieczeństwa serwerów wykonywane są codziennie i zapisywane na osobnych dyskach USB lub dyskach sieciowych przy pomocy programów służących do wykonywania kopii zapasowych. Z kolei ust. 4 określa, że zabezpieczenie danych znajdujących się na stacjach roboczych wykonywane jest przez program do kopiowania danych zainstalowanych na stacji roboczej. Dane kopiowane są na dysk sieciowy i kompresowane.

Zgodnie ze złożonymi wyjaśnieniami obowiązek wykonywania kopii bezpieczeństwa spoczywa na firmie zarządzającej serwerem Firebird Urzędu Gminy Nowa Wieś Wielka

na podstawie umowy nr 032.2.2018 z dnia 2 stycznia 2018 r. *Jak wspomniano w pkt 2.7. umowa obliguje wykonawcę do tworzenia comiesięcznych backup-ów wybranych zasobów. W toku kontroli nie stwierdzono aby ze strony jednostki kontrolowanej w odpowiedni sposób były weryfikowane czynności z tym związane. Ponadto umowa nie gwarantuje zamawiającemu możliwości kontrolowania wykonawcy w zakresie zobowiązań wynikających z umowy.*

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.
Zgodnie ze złożonymi wyjaśnieniami w Urzędzie Gminy Nowa Wieś Wielka nie stworzono sformalizowanych procedur w zakresie projektowania systemów teleinformatycznych dotyczących architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. z ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągniecia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu. Narusza to § 15 ust. 1 rozporządzenia KRI.
Jak wyjaśniono, w Urzędzie Gminy Nowa Wieś Wielka nie wprowadzono sformalizowanych regulacji wewnętrznych w zakresie wdrażania systemów teleinformatycznych, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji, a także warunków i kryteriów odbioru. Zgodnie z wyjaśnieniami wdrożenia nowych rozwiązań teleinformatycznych odbywają się na zasadzie zaspokajania bieżących potrzeb Urzędu w tym zakresie oraz realizacji działań zmierzających do usprawnienia jego pracy i ułatwienia dostępu dla mieszkańców.
Jak wyjaśniono, w Urzędzie Gminy Nowa Wieś Wielka nie stworzono również regulacji wewnętrznych opisujących sposób przeprowadzania zmian w systemach teleinformatycznych. Zmiany w systemach, zgodnie z wyjaśnieniami, odbywają się na bieżąco w zakresie dostosowania do zmieniających się przepisów prawa. Zmiany te wprowadza autor danego oprogramowania.
Jak wyjaśniono w Urzędzie Gminy Nowa Wieś Wielka nie stworzono regulacji wewnętrznych opisujących proces monitorowania systemów teleinformatycznych. Niemniej funkcjonuje oprogramowanie Axence nVision, które umożliwia monitorowanie. Oprogramowanie umożliwia prowadzenie kompleksowej kontroli nad infrastrukturą IT, a także pełnej listy zainstalowanego/używanego oprogramowania. Oprogramowanie w sposób kompleksowy wpływa na podniesienie poziomu bezpieczeństwa i ograniczenie wystąpienia zagrożeń w całym systemie teleinformatycznym.

Dokumentację z wdrożeń nowych systemów teleinformatycznych stanowią jedynie umowy na realizację tych zadań.

Jak wyjaśniono zmiany w systemie informatycznym prowadzone są według bieżących potrzeb. Aktualizację oprogramowania dziedzinowego, w zakresie dostosowania do zmian w przepisach prawa dokonuje autor oprogramowania na podstawie nadzoru autorskiego. Jak wyjaśniono, na przełomie 2014 i 2015 roku przeprowadzono modernizację sieci teleinformatycznej Urzędu Gminy.

Działanie systemu teleinformatycznego monitorowane jest za pomocą oprogramowania Axence nVision, które zostało wdrożone w kontrolowanym okresie. Umożliwia ono monitorowanie pracy sieci, użytkowników, zainstalowanego i używanego oprogramowania, zdarzeń systemowych, odwiedzanych witryn internetowych.

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji.
Regulacje prawa powszechnie obowiązującego odnoszące się do ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami

znajdują się w § 20 ust. 2 pkt 7, 9, 11 rozporządzenia KRI.
Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji określono w tabeli form naruszeń danych osobowych, która stanowi załącznik nr 1 do Polityki Bezpieczeństwa Informacji.

W celu monitorowania działań użytkowników w systemie w Urzędzie funkcjonuje system Axence nVision umożliwiający monitorowanie działań użytkowników. Umożliwia ponadto blokowanie niebezpiecznych domen WWW przed przypadkowym wejściem i pobraniem złośliwego oprogramowania.

W Urzędzie Gminy Nowa Wieś Wielka nie istnieje sformalizowana procedura dotycząca wejść i wyjść do pomieszczenia serwerowni. Zgodnie ze złożonymi wyjaśnieniami osobą upoważnioną do wejścia do serwerowni jest osoba pełniąca w Urzędzie funkcję informatyka i administratora systemu informatycznego. Osoba ta, jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej, jako jedyna ma dostęp do karty odblokowującej zamek elektromagnetyczny drzwi do serwerowni. *Brak sformalizowanej procedury dotyczącej wejść i wyjść do serwerowni oraz przypisania dostępu do karty odblokowującej stanowi istotne zagrożenie bezpieczeństwa informacji chociażby w aspekcie ustalenia zakresu i osób odpowiedzialnych w przypadku nieautoryzowanego skorzystania z karty przez osobę trzecią i wyrządzenia przez nią szkody.*

Wejście do serwerowni możliwe jest po wcześniejszym odblokowaniu alarmu zabezpieczającego oraz użyciu karty magnetycznej odblokowującej zamek elektromagnetyczny. Dodatkowym zabezpieczeniem jest zastosowanie tradycyjnego klucza odblokowującego zamek główny. Jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej do zabezpieczenia serwerowni zastosowano drzwi stalowe przeciwpożarowe i dymoszczelne o zwiększonej odporności na włamanie. W zakresie obciążeń środowiskowych zastosowano klimatyzator, płytki antystatyczne oraz zabezpieczono ściany przed przedostawaniem się wilgoci.

Jak wynika ze złożonych wyjaśnień sprzęt informatyczny przeznaczony do utylizacji przekazywany jest po usunięciu z niego dysków twardych. Dyski utylizowane są osobno przez certyfikowaną firmę.

Jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej mechanizmy kryptograficzne w Urzędzie wykorzystywane są do podpisów kwalifikowanych podczas wysyłki pism drogą elektroniczną.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.
Do kwestii zabezpieczeń techniczno-organizacyjnych systemów informatycznych odnosi się § 20 ust. 2 pkt 12 rozporządzenia KRI.
Do tej pory nie prowadzono w Urzędzie Gminy Nowa Wieś Wielka kontroli logów systemowych. Jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej spowodowane to jest tym, że nie stwierdzono ryzyka wystąpienia incydentów bezpieczeństwa przetwarzanych informacji, które wymagałoby podjęcia takich działań. *Brak podejmowania działań w zakresie kontroli logów stanowi naruszenie § 21 rozporządzenia KRI, które wymaga obligatoryjnego odnotowywania działań użytkowników lub obiektów systemowych. Zgodnie z ust. 4 wspomnianego przepisu informacje w dziennikach systemów powinny być przechowywane od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*
Obecnie możliwość kontroli logów systemowych umożliwia wdrożone oprogramowanie Axence nVision. *Sam fakt stworzenia możliwości kontroli logów jest niewystarczający*

dla zapewnienia bezpieczeństwa informacji. Wynika to z wykładni celowościowej przytoczonych przepisów, gdyż odnotowywanie działań użytkowników lub obiektów systemowych nie ma służyć temu celowi samemu w sobie, a winno umożliwiać podejmowanie adekwatnych działań wynikających z efektów ich kontroli. Brak podejmowania kontroli w tym zakresie uniemożliwia potwierdzenie lub zdeprecjonowanie istnienia ewentualnych zagrożeń i podejmowanie odpowiednich działań.
Jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej zabezpieczenie systemów przed wirusami i awariami zapewnia zastosowanie oprogramowania, w tym antywirusowego i do zarządzania zasobami (Axence nVision).

2.14. Rozliczalność działań w systemach informatycznych.
Ten obszar został uregulowany w § 21 ust. 2-4 rozporządzenia KRI.
W Urzędzie Gminy Nowa Wieś Wielka nie istnieją regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów). Podgląd logów systemowych umożliwia zainstalowane oprogramowanie do zarządzania siecią Axence nVision. Wspomaga ono kompleksową kontrolę dzienników z poziomu komputera administratora bez konieczności bezpośredniej fizycznej ingerencji na innych stanowiskach komputerowych.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych.
Strona Biuletynu Informacji Publicznej Urzędu Gminy Nowa Wieś Wielka umożliwia odczytywanie treści w powiększonej czcionce oraz w zwiększonym kontraście. Ponadto, jak wyjaśnił podinspektor ds. obsługi organów Gminy i obsługi informatycznej, stronę www.bip.nowawieswielka.pl oraz www.nowawieswielka.pl poddano walidacji pod kątem zgodności z WCAG 2.0 i obie, z nielicznymi błędami, zostały zweryfikowane jako zgodne na poziomie AA, co odpowiada wymaganiom określonym w § 19 rozporządzenia KRI.

Wskazuje się następujący zakres stwierdzonych uchybień:
- Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Nowa Wieś Wielka ogranicza się w swoich regulacjach do kwestii bezpieczeństwa przetwarzania danych osobowych pomijając aspekt bezpieczeństwa przetwarzania wszelkich innych informacji jakimi dysponuje podmiot kontrolowany. To samo uchybienie dotyczy Instrukcji zarządzania systemem informatycznym;
- brak jest regulacji wewnętrznych opisujących sposób zarządzania ryzykiem Bezpieczeństwa Informacji;
- brak jest dokumentacji potwierdzającej przeprowadzanie okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestru ryzyk zawierającego informacje o zidentyfikowanych ryzykach, ich poziomie;
- nie zostały ustanowione procedury przydzielania, zwrotu sprzętu i oprogramowania;
- brak regulacji wewnętrznych dotyczących przeprowadzania szkoleń użytkowników zaangażowanych w procesy przetwarzania informacji w systemach teleinformatycznych;
- w kontrolowanym okresie nie wszyscy pracownicy zaangażowani w proces przetwarzania informacji brali udział w szkoleniach;
- tematyka przeprowadzanych szkoleń nie wyczerpuje zakresu wskazanego w § 20 ust. 2 pkt 6 rozporządzenia KRI;
- brak jest regulacji wewnętrznych określających zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych;
- nie jest prowadzony rejestr incydentów naruszenia BI;
- brak regulacji wewnętrznych, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI;

- część rekomendacji sformułowanych w raporcie ze stycznia 2015 r. z analizy i oceny zgodności środków technicznych i organizacyjnych w Urzędzie Gminy Nowa Wieś Wielka z przepisami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz wymagań prawnych w zakresie ochrony danych osobowych oraz rekomendacji działań doskonalących w tym zakresie nie została zrealizowana;
- nie stworzono regulacji wewnętrznych opisujących sposób przeprowadzania zmian w systemach teleinformatycznych;
- brak regulacji wewnętrznych zawierających zasady prowadzenia i wykorzystania dzienników systemowych (logów).

Wskazuje się następujący zakres stwierdzonych nieprawidłowości:

- w podmiocie kontrolowanym nie istnieją wewnętrzne procedury dotyczące obsługi usług elektronicznych oraz monitoringu dotyczącego dostarczania ich na zadeklarowanym poziomie. Stanowi to naruszenie § 15 ust. 2 rozporządzenia KRI, w którym jest mowa o tym, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne odbywa się w oparciu o udokumentowane procedury;
- brak jest planu postępowania z ryzykiem, co narusza § 20 ust. 2 pkt 3 rozporządzenia KRI zobowiązujący do przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz do podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
- brak utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację przed wprowadzeniem programu Axence nVision, co naruszało § 20 ust. 2 pkt 2 rozporządzenia KRI;
- nie ustanowiono podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Stanowi to naruszenie wymogu wynikającego z § 20 ust. 2 pkt 8 rozporządzenia KRI;
- nie wprowadzono regulacji wewnętrznych określonych w § 20 ust. 2 pkt 13 rozporządzenia KRI, tj. dotyczących zgłaszania incydentów naruszenia bezpieczeństwa informacji;
- nie stworzono sformalizowanych procedur w zakresie projektowania systemów teleinformatycznych dotyczących architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. z ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągniecia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu. Narusza to § 15 ust. 1 rozporządzenia KRI;
- nie wprowadzono sformalizowanych regulacji wewnętrznych w zakresie wdrażania systemów teleinformatycznych, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji, a także warunków i kryteriów odbioru. Narusza to § 15 ust. 1 rozporządzenia KRI;
- brak sformalizowanej procedury dotyczącej wejść i wyjść do serwerowni oraz przypisania dostępu do karty odblokowującej konkretnej osobie lub osobom;
- brak podejmowania działań w zakresie kontroli logów, co stanowi naruszenie § 21 rozporządzenia KRI, które wymaga obligatoryjnego odnotowywania działań użytkowników lub obiektów systemowych.

Ponadto wskazuje się następujące przyczyny i skutki stwierdzonych nieprawidłowości.

Przyczyną stwierdzonych nieprawidłowości jest nieprzestrzeganie wskazanych przepisów rozporządzenia KRI oraz niezrealizowanie rekomendacji zawartych w raporcie

ze stycznia 2015 r. z analizy i oceny zgodności środków technicznych i organizacyjnych w Urzędzie Gminy Nowa Wieś Wielka z przepisami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz wymagań prawnych w zakresie ochrony danych osobowych oraz rekomendacja działań doskonalących w tym zakresie.

Skutkiem powyższego jest obniżenie możliwości zapewnienia bezpieczeństwa przetwarzanych informacji.

Za stwierdzone nieprawidłowości odpowiedzialność ponosi podinspektor ds. obsługi organów Gminy i obsługi informatycznej, pełnomocnik ds. ochrony informacji niejawnych, bezpieczeństwa publicznego, spraw obronnych i bhp oraz z tytułu nadzoru Wójt Gminy Nowa Wieś Wielka.

Kontrolę wpisano do książki kontroli pod nr 2/2018.

Do Projektu wystąpienia pokontrolnego z 24 lipca 2018 r. nie zostały zgłoszone zastrzeżenia.

W Projekcie wystąpienia pokontrolnego nie dokonano sprostowań/ skreśleń/ uzupełnień.

W związku z powyższymi ocenami, uwagami i wnioskami zalecam Panu podjęcie następujących działań w celu wyeliminowania stwierdzonych w wyniku kontroli nieprawidłowości lub usprawnienia funkcjonowania działalności jednostki kontrolowanej:
- stworzenie wewnętrznej procedury dotyczącej obsługi usług elektronicznych oraz monitoringu dotyczącego dostarczania ich na zadeklarowanym poziomie, zgodnie z § 15 ust. 2 rozporządzenia KRI, w którym jest mowa o tym, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne odbywa się w oparciu o udokumentowane procedury;

- stworzenie planu postępowania z ryzykiem, zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI zobowiązującym do przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz do podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

- ustanowienie zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość zgodnie z wymogiem określonym w § 20 ust. 2 pkt 8 rozporządzenia KRI;

- wprowadzenie regulacji wewnętrznych określonych w § 20 ust. 2 pkt 13 rozporządzenia KRI, tj. dotyczących zgłaszania incydentów naruszenia bezpieczeństwa informacji;

- stworzenie, zgodnie z § 15 ust. 1 rozporządzenia KRI, sformalizowanych procedur w zakresie projektowania systemów teleinformatycznych dotyczących architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. z ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągniecia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu;

- wprowadzenie, zgodnie z § 15 ust. 1 rozporządzenia KRI, sformalizowanych regulacji

wewnętrznych w zakresie wdrażania systemów teleinformatycznych, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji, a także warunków i kryteriów odbioru;

- stworzenie sformalizowanej procedury dotyczącej wejść i wyjść do serwerowni oraz przypisanie dostępu do karty odblokowującej konkretnej osobie lub osobom;

- podejmowanie działań w zakresie kontroli logów, zgodnie z § 21 rozporządzenia KRI, który wymaga obligatoryjnego odnotowywania działań użytkowników lub obiektów systemowych;

- zrealizowanie rekomendacji zawartych w raporcie ze stycznia 2015 r. z analizy i oceny zgodności środków technicznych i organizacyjnych w Urzędzie Gminy Nowa Wieś Wielka z przepisami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz wymagań prawnych w zakresie ochrony danych osobowych (...).

Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach, z których jeden egzemplarz otrzymuje kierownik jednostki kontrolowanej, a drugi egzemplarz pozostaje w aktach kontroli.

Oczekuję od Pana w terminie 30 dni od daty otrzymania niniejszego wystąpienia, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości

Wojewoda Kujawsko-Pomorski