WOJEWODA ŚWIĘTOKRZYSKI

Kielce, dnia 16-11-2021

Znak: OK.V.431.1.2021

Pan Andrzej Gąsior
Burmistrz Miasta i Gminy Nowa Słupia

Wystąpienie pokontrolne

Kontrolę w Urzędzie Miasta i Gminy w Nowej Słupi, ul. Rynek 15 w dniach 21-22 września 2021 roku przeprowadził zespół kontrolerów w składzie:

Marek Rak - Główny specjalista Oddziału ds. Informatyki w Wydziale Organizacji i Kadr ŚUW, na podstawie pisemnego upoważnienia do przeprowadzenia kontroli numer 553/2021 z dnia 15.09.2021 r. wydanego z upoważnienia Wojewody Świętokrzyskiego przez Dyrektora Wydziału Organizacji i Kadr.

Maciej Terek - Główny specjalista Oddziału ds. Informatyki w Wydziale Organizacji i Kadr ŚUW, na podstawie pisemnego upoważnienia do przeprowadzenia kontroli numer 554/2021 z dnia 15.09.2021 r. wydanego z upoważnienia Wojewody Świętokrzyskiego przez Dyrektora Wydziału Organizacji i Kadr.

Zakres kontroli i okres objęty kontrolą:

Zakres kontroli obejmował działanie systemów teleinformatycznych używanych do realizacji zadań publicznych w okresie od 1.01.2017 do dnia kontroli. Zgodnie z Rozporządzeniem 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 (Dz. U. z dnia 16 maja 2012 r. poz. 526) wydanym na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2020 r. poz. 224), ocenie podlegały trzy główne obszary tematyczne:

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

2) System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

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

Wykonywanie zadań w kontrolowanym zakresie oceniam pozytywnie z uchybieniami i nieprawidłowościami.

W wyniku przeprowadzonej kontroli ustalono, że:

USTALENIA KONTROLI	
Akty prawne, na podstawie których dokonano ustaleń w toku kontroli	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
Obszar kontroli : **1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie usług drogą elektroniczną**	
1.1 usługi elektroniczne	
Podstawa prawna	§ 5 ust.2 pkt.1 i pkt.4 rozporządzenia: Interoperacyjność na poziomie organizacyjnym osiągana jest przez: • pkt.1 Informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty • pkt.4 Publikowanie i aktualizowanie w BIP przez przedmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Jedyną usługą świadczoną w formie elektronicznej przez Urząd Miasta i Gminy w Nowej Słupi jest skrzynka podawcza udostępniona na platformie ePUAP. Z informacji pozyskanych przez zespół kontrolny wynika, że Urząd Miasta i Gminy w Nowej Słupi nie oferuje innych usług w formie elektronicznej. Na stronie BIP kontrolowanego w zakładce „Jak załatwić sprawę" i dalej „Spis spraw", został opublikowany katalog, składający się z 22 pozycji w którym zamieszczono karty usług, formularze i wzory dokumentów w liczbie około 100. Dowód - akta kontroli plik : www-uslugi-bip.jpg
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.2 centralne repozytorium wzorów dokumentów elektronicznych	
Podstawa prawna	**Art. 19 b ust. 3 ustawy:** Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich bezpiecznym podpisem elektronicznym.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	UMiG Nowa Słupia nie przekazywał wzorów dokumentów do centralnego repozytorium wzorów dokumentów elektronicznych.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**

Ocena obszaru kontroli nr 1	Pozytywna
Obszar kontroli : **2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych**	
2.1 Dokumenty z zakresu bezpieczeństwa informacji . Zaangażowanie kierownictwa podmiotu	
Podstawa prawna	**§ 20 ust. 1 rozporządzenia:** Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. **§ 20 ust. 2 rozporządzenia:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji. **§ 20 ust. 2 pkt 1 rozporządzenia:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zarządzenie nr 118/2020 Burmistrza Miasta i Gminy Nowa Słupia z dnia 7.10.2020 roku w sprawie wprowadzenia Polityki Ochrony Danych a szczególnie załącznik nr 1 Polityka Ochrony Danych Osobowych (PODO) dotyczy tylko i wyłącznie ochrony danych osobowych, a nie ochrony wszelkich danych przetwarzanych i gromadzonych w UMiG w Nowej Słupi. Cały dokument został oparty o Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz o ustawę z dnia 10 maja 2018 o ochronie danych osobowych. Co prawda w Rozdziale 1 „Przepisy ogólne" wymieniono również w punkcie 3 Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, niemniej jednak zawężono całą Politykę Ochrony Danych tylko i wyłącznie do ochrony danych osobowych. Cytuję z Załącznika numer 1 „***Niniejsza Polityka ma zastosowanie do danych osobowych przetwarzanych w systemach informatycznych oraz w postaci papierowej będących w zasobach jednostki***". W załączniku numer 1, rozdział II „Polityka Ochrony Danych Osobowych", Art. 5 „Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych", punkt 1, podpunkt 7 jest mowa o „Rejestrze czynności przetwarzania danych osobowych (załącznik 8) oraz o Rejestrze kategorii czynności przetwarzania (załącznik 9). Zespołowi kontrolnemu przedłożono dokumentację w tym zakresie w postaci dwóch plików cyfrowych w formacie xlsx. Na załączniku

	numer 8 jako IODO wymieniony jest Pan RŁ, natomiast na załączniku numer 9 wymieniona jest Pani DJ jako IODO. Zespołowi kontrolującemu została przedłożona dokumentacja w postaci Zarządzenia nr 45/2021 Burmistrza Miasta i Gminy w Nowej Słupi w sprawie odwołania i powołania nowego IODO. Z dniem 1 kwietnia 2021 odwołano ze stanowiska Panią DJ a powołano na stanowisko IODO Pana RŁ. Stwierdzono brak aktualizacji dokumentów PODO przez ostanie 6 miesięcy przez nowego IODO. Oba załączniki przechowywane w formie elektronicznej nie posiadały autoryzacji Administratora a tym samym dokumentacja nie posiadała atrybutów autentyczności, rozliczalności i niezaprzeczalności. Nie została przedłożona zespołowi kontrolującemu dokumentacja związana z przeprowadzonymi sprawdzeniami z procesu wydawania upoważnień do przetwarzania danych i przydzielania uprawnień od systemów informatycznych. Do tych czynności zobowiązany jest IODO (patrz Załącznik 1 do POD, punkt 2, podpunkt 8). Art. 21 PODO „Zasady wykonywania kopii bezpieczeństwa" są bardzo ogólnie opisane, zespołowi kontrolującemu nie została przedłożona dokumentacja w której wynikałoby kiedy, jak często i z jakich zasobów tworzona jest kopia bezpieczeństwa. Pośrednio wynika to z logów które zostały okazane, oraz z audytu z roku 2020. Brak dokumentacji opisującej wykonywanie i testowanie backupów. W Art.21 punkt 6 PODO jest zapisane, że obsługa informatyczna zobowiązana jest do testowania kopii zapasowych. Zespołowi kontrolującemu nie została przedłożona żadna dokumentacja w tym zakresie. Na brak dokumentacji w tym zakresie wskazuje również przeprowadzony w roku 2020 audyt. W starej PBODO z roku 2018-2019 znajduje się w IZSI załącznik numer 1, tworzenie kopii zapasowych baz danych. W załączniku jest szczegółowo opisane jakie systemy w jaki sposób, jak często są kopiowane. Niestety załącznik w takiej postaci jak z lat 2018-2019 nie znalazł się w PODO z 2020. W Art.34 PODO „Zarządzanie ciągłością działania", w punkcie 4 jest napisane, że zostanie przez Administratora opracowany wraz z wyznaczoną osobą plan ciągłości działania według wzoru z załącznika numer 16. Zespołowi kontrolującemu została przedłożona dokumentacja w postaci załącznika numer 16 stanowiącego wzór do PODO, natomiast nie przedłożono dokumentacji dotyczącej ciągłości działania, która miała powstać na podstawie tego. Przedłożony załącznik 16 (wzór) nie nosi atrybutów autentyczności, niezaprzeczalności i rozliczalności. Plan awaryjny dotyczący procedury tworzenia backupów i archiwizacji plików, który wskazuje, że procedura znajduje się w PODO, ale w rzeczywistości w PODO takiej procedury nie ma.

1.3 Model usługowy	
Podstawa prawna	**§ 15 ust. 2 rozporządzenia:** Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W UMiG Nowa Słupia nie została wdrożona żadna platforma usług elektronicznych dla mieszkańców Miasta i Gminy Nowa Słupia, która wymagałaby stosowania modelu usługowego.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.4 Współpraca systemów informatycznych z innymi systemami	
Podstawa prawna	**§ 5 ust. 3 pkt 3 rozporządzenia:** Interoperacyjność na poziomie semantycznym osiągana jest przez, m.in. stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań. **§ 16 ust. 1 rozporządzenia:** Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się 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 ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Oprogramowanie aplikacyjne firmy **FORTES**: program finansowo-księgowy, ewidencja środków trwałych i wyposażenia, podatki i opłaty gminne, system monitorowania odpadów komunalnych posiada możliwość wymiany informacji z innymi systemami, innymi instytucjami. **PUMA /Platforma Uruchomieniowa Modułów Aplikacyjnych/** jest w pełni zintegrowanym systemem informatycznym wspomagającym realizacje zadań jednostek samorządu terytorialnego. System umożliwia podłączenie aplikacji napisanych w różnych technologiach programistycznych, z różnych systemów operacyjnych, a także daje możliwość integracji z systemami obiegu dokumentów oraz z internetowymi systemami obsługi obywatela tzn. zapewnia praktyczną realizację koncepcji e-Urzędu. W UMiG Nowa Słupia w systemie tym prowadzony jest rejestr wyborców. **ŻRÓDŁO** program do edycji oraz przetwarzania danych gromadzonych w Systemie Rejestrów Państwowych: rejestr PESEL, dowody osobiste, rejestry stanu cywilnego, Centralny Rejestr Sprzeciwów oraz System Odznaczeń Państwowych. **CEIDG** czyli Centralna Ewidencja Informacji o Działalności Gospodarczej jest centralnym systemem umożliwiającym prowadzenie ewidencji przedsiębiorców, którzy są osobami fizycznymi oraz dostarczanie informacji o podmiotach gospodarczych w zakresie wskazanym w ustawie o CEIDG.

Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.5 Obieg dokumentów w urzędzie	
Podstawa prawna	**§ 20 ust. 2 pkt 9 rozporządzenia:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególność przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Podstawowym sposobem dokumentowania przebiegu spraw oraz wykonywania czynności kancelaryjnych jest system tradycyjny. We wdrożonym Systemie Elektronicznego Obiegu Dokumentów EDICTA rejestrowane są jedynie sprawy przychodzące w UMiG w Nowej Słupi (Zarządzenie 25/2017 Wójta Gminy Nowa Słupia z dnia 27 marca 2017) w sprawie wprowadzenia Systemu elektronicznego Obiegu Dokumentów EDICTA. Dowód - akta kontroli, kserokopia zarządzenia
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.6 Formaty danych udostępniane przez systemy informatyczne	
Podstawa prawna	**§ 17 ust. 1 rozporządzenia:** Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą. **§ 18 ust. 1 rozporządzenia:** Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia. **§ 18 ust. 2 rozporządzenia:** Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Wymiana danych w systemach PUMA i ŹRÓDŁO z systemami wspomagającymi zapewniona jest przez eksport części danych w formacie XML. Podobnie ma się sytuacja z oprogramowaniem firmy Fortes moduły tej firmy albo współdzielą informacje albo używają wewnętrznego formatu wymiany danych. Natomiast wymiana danych z innymi zewnętrznymi systemami typu Płatnik czy Bestia oparte są o plik w formacie XML.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**

	Podobna sytuacja ma się z załącznikiem numer 15 „Wykaz Planów ciągłości działania". Zespołowi kontrolującemu został jedynie przedstawiony wzór załącznika numer 15. Brak jest natomiast śladów zastosowania załącznika numer 15 w praktyce. Punkt 1 załącznika numer 15 który mówi o tym, że przynajmniej raz w roku wykonywana jest symulacja odtworzenia bazy z kopii zapasowej, przynajmniej raz na kwartał (4 razy w roku) jest przeprowadzony przegląd nośników pod kątem ich dalszej przydatności. Brak dokumentacji w tym zakresie. W Art.30 PODO opisano zasady korzystania z elektronicznych nośników danych. Zasady z przenośnej pamięci „PenDrive" zostały określone w załączniku numer 18 w punktach 1-14. Zespołowi kontrolnemu nie została przedłożona dokumentacja, która świadczyłaby, że zdefiniowane zasady w załączniku numer 18 są stosowane, przestrzegane przez osoby do tego celu wyznaczone. Brak pisemnej dokumentacji dotyczącej przyznawania służbowego nośnika danych dla pracowników UMiG. Brak systemu ewidencji pamięci pendrive (SEPP), za utworzenie którego odpowiedzialny jest ASI (patrz załącznik 18, punkt 5). Brak dokumentacji z kontroli pendrivów przeprowadzonej przez IODO (patrz załącznik 18, V, punkt 1). Załącznik numer 1 do załącznika numer 18 (oświadczenia z lat 2020-2021) zostały dosłane w trakcie prac nad wystąpieniem pokontrolnym. Reasumując Art. 30 PODO oraz załącznik numer 18 są dokumentami martwymi, które nie są stosowane w UMiG w Nowej Słupi. Przeglądając udostępnioną PODO (plik w postaci cyfrowej w formacie docx, który nie posiadał autoryzacji Administratora a tym samy nie posiadał atrybutów autentyczności, rozliczalności, niezaprzeczalności) zespół kontrolny zauważył iż w dokumencie brakuje artykułów o numerze 25, 26. Oba artykuły ujęte są w spisie treści (patrz strona 2 PODO): Art. 25 Zarządzanie pojemnością przestrzeni dyskowej Art. 26 Zasady bezpiecznego przydzielania przestrzeni dyskowej Analizując Art.39 w którym zapisano, że na końcu PODO powinien znajdować się Rejestr Modyfikacji Polityki w którym powinny być odnotowane wszelkie zmiany w PODO, zespół kontrolny stwierdza, że w przedłożonej PODO brakuje Rejestru Modyfikacji Polityki. W Art. 39 chyba już kolejny raz zapisano, że PODO podlega regularnym przeglądom przez IODO. Reasumując brak jest załącznika numer 16 czyli planu ciągłości działania, ten który został przedłożony zespołowi kontrolującemu jest tylko wzorem, brak jest planu awaryjnego dotyczącego procedury tworzenia backupów i archiwizacji plików na który wskazuje załącznik 16 (wzór). Brak zastosowania w rzeczywistości załącznika numer 15 oraz dowodów realizacji zadań w nim zdefiniowanych. Wytworzona dokumentacja przechowywana w postaci elektronicznej

	powinna być zatwierdzona, autoryzowana przez Administratora i przechowywana w wyznaczonym miejscu, powinna nosić atrybuty niezaprzeczalności, autentyczności, niezawodności i niezaprzeczalności. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
Ustalone nieprawidłowości	Zarządzenie 118/2021 Burmistrza Miasta i Gminy Nowa Słupia z dnia 7.10.2021 roku w sprawie wprowadzenia PODO **dotyczy jedynie ochrony szczególnych danych jakimi są dane osobowe**, natomiast zbiór danych przetwarzanych, gromadzonych w UMiG jest znacznie szerszy i również powinien podlegać ochronie i sposób tej ochrony danych powinien być ujęty w wyżej wymienionej dokumentacji. Dokumentacja wprowadzona Zarządzeniem nr 118/2021 Burmistrza Miasta i Gminy Nowa Słupia z dnia 7.10.2021 roku nie posiada atrybutów autentyczności, rozliczalności, niezaprzeczalności i niezawodności o których mowa w wytycznych zdefiniowanych w KRI. Patrz: § 20, ust1, ust.2, pkt 1,pkt 8, pkt 13 Brak dowodów na wykonywanie przeglądów i aktualizacji PODO, nie wszystkie czynności określone w PODO są realizowane, dokument główny PODO, udostępniony zespołowi kontrolnemu wygląda na nieukończony lub nieprzystosowany do specyfiki pracy w UMiG. Według PODO UMiG w Nowej Słupi za PODO odpowiedzialny jest Administrator i IODO. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
2.2 Analiza zagrożeń związanych z przetwarzaniem informacji	
Podstawa prawna	§ 20 ust. 2 pkt 3 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolnemu została przedłożona dokumentacja z przeprowadzonej analizy ryzyka w latach 2019-2020. Analiza ryzyka z roku 2019 została przeprowadzona tylko w odniesieniu do przepisów zawartych w RODO. Analiza ryzyka z roku 2020 dotyczy tylko i wyłącznie danych osobowych, tytuł dokumentu „Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych". Dowód - akta kontroli plik : OK.V.431.1.2021 Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Brak analizy ryzyka i zagrożeń w szerszym ujęciu wszelkich danych przetwarzanych, przechowywanych w UMiG a nie tylko osobowych. Nie zmienia to faktu iż analiza przeprowadzona w latach 2019-2020 w swoim zakresie jest właściwa.
2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego	
Podstawa prawna	**§ 20 ust. 2 pkt 2** Zarządzanie bezpieczeństwem informacji

	realizowane jest w szczególności przez, m.in. utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolnemu została przedłożona dokumentacja dotycząca „Inwentaryzacji sprzętu i oprogramowania". Inwentaryzację przeprowadzono 23 lipca 2021 roku. Dokument posiada autoryzację Administratora z dnia 21 września 2021 roku. Dodatkowo został udostępniony dokument „Wykaz licencji i oprogramowania", który posiadał autoryzację Administratora z dnia 21 września 2021 roku. Inwentaryzacja zawiera informację o urządzeniach (konfiguracja, adres IP, zainstalowane oprogramowanie, numer inwentarzowy, imię i nazwisko osoby), stan urządzenia, data ostatniego serwisu, datę przeprowadzenia inwentaryzacji, nazwisko i imię osoby przeprowadzającej inwentaryzację. Dokumentacja jest prowadzona w wersji elektronicznej w plikach w formacie doc, xls. Oba pliki po zakończeniu inwentaryzacji powinny być elektronicznie autoryzowane (podpis kwalifikowany) przez Administratora lub osobę do tego wyznaczoną i w takiej postaci dokumentacja powinna być przechowywana i udostępniana. Dowód - akta kontroli plik: Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych	
Podstawa prawna	**§ 20 ust. 2 pkt 4:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. podejmowanie 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. **§ 20 ust. 2 pkt 5** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespół kontrolny przeanalizował proces zakładania, modyfikacji i usuwania kont z systemów informatycznych opisany w PODO. Zgodnie z PODO na wniosek Administratora wypełniany jest załącznik numer 14, który jest jednocześnie upoważnieniem do przetwarzania danych osobowych i oświadczeniem o zachowaniu tajemnicy danych osobowych. Wniosek zawiera również informacje do jakich systemów i w jakim zakresie ma mieć dostęp konkretny pracownik UMiG (patrz pani AŁ). Podobnie ma się sytuacja z odbieraniem i modyfikacją uprawnień w systemach informatycznych. W załączniku nie zostały wypełnione informacje na temat strefy. Być może jest to informacja zbędna wówczas należy zaktualizować format załącznika numer 14. W innym przypadku należałoby tą informację uzupełnić.

	Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Należałoby przeanalizować czy załącznik numer 14 w takiej postaci jak jest używany obecnie nie należy zaktualizować (patrz brak wypełnionych informacji o strefach).
2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji	
Podstawa prawna	**§ 20 ust. 2 pkt 6** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, 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.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolującemu została przedłożona dokumentacja dotycząca szkoleń pracowników UMiG z lat 2018-2021, dokładnie listy obecności wraz z podpisami osób biorących udział w szkoleniu. W roku 2018 zostało przeprowadzone szkolenie w zakresie przepisów RODO. W 2020 roku zostało przeprowadzone szkolenie w zakresie „Ochrony danych osobowych i Polityki Bezpieczeństwa" to samo szkolenie przeprowadzono w roku 2021. W 2020 szkolenie „Ochrona danych osobowych w świetle Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016r." Przeszkolonych zostało 34 osoby, na szkoleniu nie było 8 osób. Został opracowany informator (załącznik numer 10, 10a) z zakresu bezpieczeństwa i ochrony danych osobowych udostępniony pracownikom UMiG. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Zespół kontrolny zauważył, że cześć pracowników nie brało udziału w szkoleniach (CZD,RA,WM). Brak dodatkowych terminów szkoleń dla osób nieobecnych podczas szkolenia. Brak monitoringu w tym zakresie.
2.6 Praca na odległość i mobilne przetwarzanie danych	
Podstawa prawna	**§ 20 ust. 2 pkt 8:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W Art. 27 PODO określono zasady pracy na odległość. W praktyce połączenie zdalne firm (FORTES, Zeto, Asseco lub innych) odbywa się pod nadzorem obsługi informatycznej UMiG. Generowane jest jednorazowe hasło do połącznia zdalnego z zewnątrz. Dobrze by było uwzględnić, wdrożyć zalecenia po audytowe w tym zakresie z roku 2020. Dowód - akta kontroli plik:

	Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.7 serwis sprzętu komputerowego i oprogramowania	
Podstawa prawna	**§ 20 ust. 2 pkt 10:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolującemu została udostępniona dokumentacja „Protokół trwałego kasowania danych z nośników magnetycznych". Dokument został autoryzowany przez wyznaczonego pracownika UMiG oraz przez osobę reprezentującą firmę która dokonała kasowania danych. Zostały wówczas wykasowane dane z 65 nośników, dokonano wówczas również fizycznego zniszczenia nośników z których dane zostały wykasowane. Brak jest natomiast dokumentacji dotyczącej serwisu sprzętu komputerowego i oprogramowania. Brak procedur podejmowanych w czasie serwisu sprzętu komputerowego, instalacji, konfiguracji, konserwacji oprogramowania wykonywanego przez firmy zewnętrzne. Kontrolujący zapoznali się również z umowami serwisowymi dotyczącymi opieki autorskiej systemu PUMA oraz EDICTA. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Brak dokumentacji z przeglądów i konserwacji urządzeń wchodzących w skład platformy sprzętowej UMiG w Nowej Słupi w latach 2018-2020.
2.8 Procedury zgłaszania incydentów naruszenia BI	
Podstawa prawna	**§ 20 ust. 2 pkt 13:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określonym i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W Art. 17 PODO „Naruszenia ochrony danych osobowych" zapisy są lakoniczne a procedura zgłoszenia naruszenia ochrony danych osobowych jest zdefiniowana w załączniku numer 13. Sama procedura w postaci załącznika numer 13 dotyczy tylko i wyłącznie danych osobowych a nie całości informacji przetwarzanych i przechowywanych w UMiG w Nowej Słupi o czym mowa w § 20 ust 2, pkt 13 rozporządzenia o KRI (np. informacje finansowe są wyłączone z całej procedury). W latach 2018-2021 odnotowano jeden incydent naruszenia ochrony danych osobowych polegający na przesłaniu pocztą elektroniczną danych osobowych niezgodnie z procedurami. Incydent został ujęty w stosownym rejestrze. Funkcję IODO w UMiG w Nowej Słupi pełni osoba z zewnątrz. W Procedurze nie ma podanych danych typu numer telefonu, adres email na który pracownik UMiG w Nowej Słupi mógłby niezwłocznie

	podjąć kontakt z IODO po wykryciu naruszenia ochronny danych. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Cała procedura dotyczy tylko i wyłącznie naruszenia ochrony danych osobowych (patrz tytuł załącznika numer 13). Brak procedury zgłaszania incydentów naruszenia bezpieczeństwa pozostałych informacji przetwarzanych przez kontrolowanego.
2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji	
Podstawa prawna	**§ 20 ust. 2 pkt 14:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolującemu przedłożono dokumentację dotyczącą przeprowadzonych audytów z lat 2018-2020. UMiG w Nowej Słupi w części realizuje w miarę możliwości zalecenia i rekomendacje po audytowe. Dowód - akta kontroli plik :OK.V.431.1.2021 Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.10 Kopie zapasowe	
Podstawa prawna	**§ 20 ust. 2 pkt 12 lit. b:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. minimalizowanie ryzyka utraty informacji w wyniku awarii.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Brak dokumentacji dotyczącej wykonywania kopii zapasowych (patrz punkt **2.1** wystąpienia). Audyt bezpieczeństwa przeprowadzony w roku 2020 wskazuje również na brak dokumentacji w tym zakresie. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Niewątpliwie obsługa informatyczna wykonuje kopie bezpieczeństwa, brak jest natomiast dokumentacji wytworzonej dotyczącej tych działań. W szczególności brak dokumentacji opisującej jakie systemy, zbiory i dane są kopiowane, gdzie na jakie urządzenia, jak często są kopiowane i jak długo są przechowywane. Dokumentacja która w trakcie pracy nad wystąpieniem pokontrolnym została dosłana a dokładnie „Lista kontrolna kopii zapasowych" (6 wpisów) dokument bez autoryzacji, zawiera wykaz czynności przy okazji których odtwarzane były dane z kopii zapasowych. Nie jest to tożsame z testowanie kopii zapasowych o którym jest mowa w PODO w IZSI Art. 21 pozycja 6 (czynności 1-5). Dokumentacja której brak powinna mieć atrybuty rozliczalności, niezaprzeczalności autentyczności i niezawodności.
2.11 Projektowanie, wdrażanie i eksploatowanie systemów teleinformatycznych	
Podstawa prawna	**§ 15 ust. 1 rozporządzenia:** Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności

	i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	System EDICTA wdrożony częściowo (Elektroniczne Zarzadzanie Dokumentacją) oraz system PUMA (dziedzinowy system do obsługi jednostek samorządu terytorialnego) zostały wdrożone w ramach realizacji projektu e-świętokrzyskie. ŹRÓDŁO to bezpłatna aplikacja ogólnopolska służąca do obsługi Systemu Rejestrów Państwowych. CEIDG jest centralnym systemem umożliwiającym prowadzenie ewidencji przedsiębiorców.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.12 Bezpieczeństwo techniczno-organizacyjne dostępu do informacji	
Podstawa prawna	**§ 20 ust. 2** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in.: **pkt 7:** zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b)czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c)zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. **pkt 9:** zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. **pkt 11 rozporządzenia:** ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespół kontrolny sprawdził większość zabezpieczeń (monitoring, wejścia do budynku, pomieszczenie serwerowni), które zostały sprawdzone w czasie przeprowadzonych oględzin przez zespół kontrolny (patrz protokół oględzin). Budynek wyposażony jest w system sygnalizacji włamania i napadu oraz system przeciwpożarowy. Zamontowane są urządzenia monitoringu wizyjnego, w oknach zamontowane są kraty i rolety antywłamaniowe. Wdrożona została polityka kluczy. Klucze są zdawane i pobierane w sekretariacie. Przy zdawaniu i pobieraniu kluczy każdy pracownik wpisuje do odpowiedniej ewidencji czas pobrania i czas zdania kluczy. Wydane są upoważnienia do zarządzania kluczami i kodem cyfrowym do systemu alarmowego. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf Protokol_ogledzin_pomieszczen.doc
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.13 Zabezpieczenia techniczno-organizacyjne systemów informatycznych	
Podstawa prawna	**§ 20 ust. 2 pkt 12 zarządzenia:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie

	odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, utratą nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa. **§ 20 ust. 4 zarządzenia:** Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespół kontrolujący sprawdził wybrane stacje robocze z systemem ŹRÓDŁO i CEIDG pod kątem zabezpieczenia antywirusowego, przeciwprzepięciowego. Urządzenia znajdujące się w serwerowni są zamontowane w szafie dystrybucyjnej i podłączone do urządzeń zapewniających zasilanie awaryjne. Serwerownia jest uporządkowana nie ma w niej zbędnego nie działającego sprzętu. UG posiada urządzenie UTM zamontowane w serwerowni, wykupione i zainstalowane są licencje na poszczególne moduły odpowiedzialne za bezpieczeństwo. Podczas oględzin zespół kontrolny stwierdził, że kontrolowany używa jeszcze komputerów z systemem operacyjnym Windows 7, który nie jest już wspierany przez producenta. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Kontrolowany używa wciąż komputerów z systemem operacyjnym Windows 7, który nie jest już wspierany przez producenta.
2.14 Rozliczalność działań w systemach teleinformatycznych	
Podstawa prawna	**§ 21 ust. 2 rozporządzenia:** W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa. **§ 21 ust. 3 rozporządzenia:** w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów

	systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka. **§ 21 ust. 4 rozporządzenia:** informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Systemy firmy FORTES, PUMA, CEIDG i ŹRÓDŁO posiadają mechanizmy do zarządzania kontami, uprawnieniami, hasłami do tych systemów. Posiadają funkcje umożliwiające odnotowywanie wykonywanych czynności na koncie administratora jak również na kontach użytkowników. Taka sama sytuacja dotyczy stacji roboczych, serwerów oraz urządzeń UTM. Dowód - akta kontroli plik : Protokol_ogledzin_pomieszczen.pdf Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
Ocena obszaru kontroli nr 2	**Pozytywna z uchybieniami i nieprawidłowościami**
Obszar kontroli : 3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych	
3.1 Czy system teleinformatyczny spełnia wymagania WCAG 2.0 z uwzględnieniem poziomu AA, określonym w załączniku nr 4 do rozporządzenia KRI?	
Podstawa prawna	**§ 19 rozporządzenia:** W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Strony www.nowaslupia.bip.jur.pl i www.nowaslupia.pl UMiG w Nowej Słupi zostały przetestowane za pomocą oprogramowania NVDA (czytnik ekranu), zostały również wyświetlone w przeglądarce FireFox i EDGE. Strona www.nowaslupia.pl posiada zdefiniowane skróty klawiaturowe: -przejdź do menu głównego Alt+1 -przejdź do treści Alt+2 -przejdź do wyszukiwarki Alt+3 -uruchom wersję dla słabowidzących Alt+4 Wszystkie skróty działają poprawnie jedynie na stronie głównej serwisu, na pozostałych stronach np. aktualności, historia skróty nie działają. Skróty nie działają w przeglądarce Edge.

	Skrót Alt+2 działa tylko na stronie głównej, na innych stronach naciśnięcie skrótu Alt+2 nie przynosi żadnego efektu. Skrót Alt+3 faktycznie przechodzi do wyszukiwarki, pojawia się komunikat o wpisaniu szukanego słowa ale tego szukanego słowa nie da się wpisać używając jedynie klawiatury. Został zdefiniowany przycisk „wersja dla słabo widzących" do którego jest dostęp poprzez klawiaturę oraz jest możliwość uruchomienia tego przycisku przy pomocy klawisza enter. Dostępny jest przycisk (skrót CTRL+U) menu dostępności z kilkoma funkcjami: -kontrast -podświetlanie linków -duży tekst -odstępy między tekstami -zatrzymaj animacje -przyjazne dla dyslektyków -kursor -podpowiedzi -wysokość linii -wyrównaj tekst Funkcje te można obsłużyć za pomocą klawiatury. Dowód – strony internetowe: Pobrane-dokumenty-UMiG.pdf
Ustalone uchybienia	Problem ze skrótami klawiaturowymi, w większości działają tylko na stronie głównej.
Ocena obszaru kontroli nr 3	**Pozytywna z uchybieniami**
Zalecenia	1. Rozszerzyć dokumentację o ochronę danych innych niż osobowe. System zarządzania bezpieczeństwem informacji powinien obejmować wszystkie dane przetwarzane w jednostce. 2. Dostosować dokumentację do wymogów rozporządzenia o KRI, tak aby posiadała atrybuty autentyczności, rozliczalności, niezaprzeczalności i niezawodności. 3. Dokumentacja dotycząca ochrony danych powinna być regularnie przeglądana i aktualizowana. 4. Należy okresowo przeprowadzać analizę ryzyka utraty integralności, poufności i dostępności w odniesieniu do wszystkich danych przetwarzanych w urzędzie, a nie tylko danych osobowych. 5. Należałoby przeanalizować, czy załącznik numer 14 do PODO w takiej postaci jak jest używany obecnie nie wymaga aktualizacji (chodzi o brak informacji o strefach). 6. Zapewnić szkolenie wszystkich pracowników zaangażowanych

	w proces przetwarzania informacji zgodnie z zaleceniami KRI. 7. Prowadzić dokumentację przeglądów i konserwacji urządzeń wchodzących w skład platformy sprzętowej UMiG w Nowej Słupi. 8. Rozszerzyć dokumentację dotyczącą zgłaszania incydentów naruszenia bezpieczeństwa informacji tak aby nie ograniczała się jedynie do danych osobowych.. Powinna zawierać w szczególności dane kontaktowe osób, którym należy zgłaszać informacje o incydencie. 9. Prowadzić dokumentację dotyczącą kopii zapasowych opisującą jakie systemy, zbiory i dane są kopiowane, gdzie, na jakie urządzenia i nośniki oraz jak długo są przechowywane. Dokumentacja ta powinna mieć atrybuty rozliczalności, niezaprzeczalności autentyczności i niezawodności. 10. W miarę możliwości należy zaktualizować systemy operacyjne tak aby nie było w jednostce systemów nie posiadających wsparcia producenta. 11. W miarę możliwości poprawić strony internetowe, tak aby były łatwiejsze w obsłudze za pomocą klawiatury.

Na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i uchybień, a także o przekazanie w terminie **30 dni** od daty otrzymania niniejszego wystąpienia pokontrolnego informacji o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz o wykonaniu zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

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

Zbigniew Koniusz
Wojewoda Świętokrzyski