



WOJEWODA LUBUSKI

Gorzów Wlkp., 8 marca 2023 r.

Nasz znak: NK-II.1611.3.2022
Sprawę prowadzi: Robert Burek
Telefon: 95 7851 821
e-mail: robert.burek@lubuskie.uw.gov.pl

Pan
Marcin Cyganiak
Lubuski Wojewódzki Inspektor
Ochrony Roślin i Nasiennictwa
Gorzów Wlkp.

Dotyczy: wystąpienie pokontrolne z kontroli prowadzonej w trybie zwykłym w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.¹

W dniach od 20 września 2022 r. do 20 grudnia 2022 r. upoważnieni pracownicy Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp. w składzie:
- Robert Burek – starszy inspektor wojewódzki w Wydziale Nadzoru i Kontroli Lubuskiego Urzędu Wojewódzkiego - przewodniczący zespołu,
- Marta Gradowska – inspektor w Wydziale Nadzoru i Kontroli LUW,
- Michał Piskowski - kierownik Oddziału Informatyki w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych LUW,
- Izabela Milczarek - informatyk ds. administrowania systemami informatycznymi w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych LUW,
przeprowadzili kontrolę w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa ul. Zieleniecka 11, 66-400 Gorzów Wlkp.
Kontrolą objęto okres od 1 stycznia 2020 r. do 31 grudnia 2021 r.

Projekt wystąpienia pokontrolnego otrzymał Pan w dniu 23 lutego 2023 r., do którego w ustawowym terminie nie zostały zgłoszone pisemne zastrzeżenia.

W związku z powyższym przekazuję Panu wystąpienie pokontrolne.²

I. Zakres działalności Wojewódzkiego Inspektoratu objęty kontrolą.

Kontrola obejmowała swym zakresem realizację zadań wynikających z ustaw i innych aktów prawnych oraz bezpieczeństwo teleinformatyczne.

II. Ocena skontrolowanej działalności.

Kontrolowaną działalność w zakresie realizacji ww. zadań oceniono **pozytywnie**.

W ramach prowadzonych działań promujących ekologię, Lubuski Urząd Wojewódzki korzysta z papieru z recyklingu. Dbaj o naturę. Używaj papieru z odzysku.

Jednakże **negatywnie** należy ocenić system zarządzania bezpieczeństwem informacji w systemach informatycznych.

III. Zakres odpowiedzialności.

Pracę Wojewódzkiego Inspektoratu Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. (dalej „WIORiN”) kieruje Lubuski Wojewódzki Inspektor Ochrony Roślin i Nasiennictwa (dalej „LWIORiN”) przy pomocy zastępcy. W okresie objętym kontrolą, funkcję Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa pełnił pan Marcin Cyganiak. Natomiast funkcję zastępcy Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa w okresie od 17 sierpnia 2020 r. do 22 marca 2021 r. pełnił pan Seweryn Stuła, a w okresie od 11 października 2019 r. do 16 sierpnia 2020 r. pełnienie obowiązków zastępcy LWIORiN powierzono panu Leszkowi Mazurkiewiczowi.

IV. Opis ustalonego stanu faktycznego.

1. Kontrola wykonania wybranych zadań wynikający z ustawy o Państwowej Inspekcji Ochrony Roślin i Nasiennictwa

Kontrolą objęto realizację wybranych zadań określonych ustawą z dnia 13 lutego 2020 r. o Państwowej Inspekcji Ochrony Roślin i Nasiennictwa (Dz.U. z 2021 r. poz. 147 z późn. zm.), związanych z:

- ochroną roślin przed agrofagami,
- zapobieganiem zagrożeniom związanym z produkcją środków ochrony roślin, obrotem tymi środkami i stosowaniem tych środków,
- nadzorem nad wytwarzaniem i oceną materiału siewnego oraz obrotem tym materiałem,
- kontrolą upraw w zakresie organizmów genetycznie zmodyfikowanych,
- monitorowaniem zużycia środków ochrony roślin,
- nadzorem nad wprowadzaniem do obrotu nawozów, nawozów oznaczonych znakiem „NAWÓZ WE” i środków wspomagających uprawę roślin.

Kontrolującym przedłożono pełną dokumentację obejmującą kontrolowany zakres. W toku kontroli stwierdzono, że na dany rok kalendarzowy wydawane są stosowne uregulowania wewnętrzne obejmujące podstawę jak i wytyczne do realizacji zadań określonych ww. ustawą.

Kontrolującym udostępniono:

- Wytyczne do planu pracy Wojewódzkich Inspektoratów Ochrony Roślin i Nasiennictwa wydane przez Państwową Inspekcję Ochrony Roślin i Nasiennictwa i zatwierdzone przez Głównego Inspektora Ochrony Roślin i Nasiennictwa,
- Wytyczne do planu pracy Wojewódzkiego Inspektoratu Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. z zakresu nadzoru fitosanitarnego zatwierdzone przez Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.,
- Zarządzenie nr 6/2020 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 28 maja 2020 r. w sprawie wprowadzenia zasad kontroli upraw pod kątem obecności GMO w roku 2020,
- Zarządzenie nr 15/2020 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 17 listopada 2020 r. w sprawie wprowadzenia procedury kontroli w zakresie wprowadzania do obrotu nawozów, nawozów oznaczonych znakiem „Nawóz WE” oraz środków wspomagających uprawę roślin,

- Zarządzenie nr 11/2019 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 16 maja 2019 r. w sprawie wprowadzenia instrukcji przeprowadzenia kontroli składu, właściwości fizycznych oraz właściwości chemicznych środków ochrony roślin,
 - Zarządzenie nr 18/2020 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 26 listopada 2020 r. w sprawie wprowadzenia instrukcji przeprowadzenia kontroli składu, właściwości fizycznych oraz właściwości chemicznych środków ochrony roślin,
 - Zarządzenie nr 1/2016 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 9 lutego 2016 r. w sprawie wytycznych do systemu kontroli występowania oraz zwalczania i ograniczania rozprzestrzeniania się bakterii *Clavibacter michiganensis* ssp. *sepedonicus* i *Ralstonia solanacearum*,
 - Zarządzenie nr 21/2020 z dnia 30 grudnia 2020 r. zmieniające zarządzenie Głównego Inspektora Ochrony Roślin i Nasiennictwa nr 1/2016 z dnia 9 lutego 2016 r. w sprawie wytycznych do systemu kontroli występowania oraz zwalczania i ograniczania rozprzestrzeniania się bakterii *Clavibacter michiganensis* ssp. *sepedonicus* i *Ralstonia solanacearum*,
 - Zarządzenie nr 4/2021 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 26 stycznia 2021 r. w sprawie wprowadzenia zasad nadzoru nad próbkobiorcami ISTA oraz organizacji wydawania dokumentacji OECD dla materiału siewnego,
 - Zarządzenie nr 12/2021 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 29 kwietnia 2021 r. w sprawie wprowadzenia procedury pobierania próbek nawozów, nawozów oznaczonych znakiem „Nawóz WE” oraz środków wspomagających uprawę roślin,
 - Zarządzenie nr 13/2021 Głównego Inspektora Ochrony Roślin i Nasiennictwa z dnia 14 maja 2021 r. w sprawie wprowadzenia zasad kontroli upraw pod kątem obecności GMO w roku 2021,
 - Plan kontroli WIORiN w Gorzowie Wlkp. z zakresu nasiennictwa na 2020 i 2021 r.,
 - Ramowy plan pracy WIORiN w Gorzowie Wlkp. w zakresie nasiennictwa na 2020 i 2021 rok,
 - Plan kontroli WIORiN w Gorzowie Wlkp. z zakresu środków ochrony roślin w 2020 i 2021 rok,
 - Plan kontroli występowania agrofagów kwarantannowych i agrofagów objętych dodatkowymi środkami fitosanitarnymi UE (kontrola poszukiwawcze) 2020 i 2021 rok.
- Akty wewnętrzne przywołują obowiązujące przepisy prawne, omawiają ogólne zasady realizacji określonych zadań, a także szczegółowo omawiają wykonywanie określonych procedur. Opisują podejmowane działania kontrolne, sposób pobierania i liczbę prób kontrolnych, określają m.in. liczbę kontroli, zakres diagnostyki laboratoryjnej, opis postępowania w przypadku otrzymania określonych wyników badań laboratoryjnych. Każdego roku do Głównego Inspektora Ochrony Roślin i Nasiennictwa WIORiN w Gorzowie Wlkp. przesyła sprawozdania z prowadzonej działalności. Zakres tych sprawozdań obejmuje m.in. zagadnienia nadzoru fitosanitarnego, nadzoru nad nasiennictwem, kontroli obrotu i stosowania środków ochrony roślin, kontroli wprowadzenia do obrotu nawozów, nawozów oznaczonych znakiem „NAWÓZ WE” oraz środków wspomagających uprawę roślin. Analiza przedłożonych dokumentów wykazała, że zadania objęte kontrolą, WIORiN wykonuje w pełni. Kontrola wykazała ponadto, że wszystkie opisane na wstępie zadania zostały w okresie objętym kontrolą zrealizowane, w związku z powyższym kontrolujący nie wnoszą uwag do realizacji zadań wynikających z ustawy o Państwowej Inspekcji Ochrony Roślin i Nasiennictwa.

2. Przestrzeganie przepisów ustawy kodeks postępowania administracyjnego w zakresie wydawanych decyzji

W okresie objętym kontrolą LWIORiN w Gorzowie Wlkp. wydał łącznie 203 decyzje administracyjne, tj. w 2020 r. - 82, a w 2021 r. - 121. Kontrolą objęto losowo wybraną próbę reprezentatywną wydanych decyzji obejmującą postępowania administracyjne, które zostały wszczęte na podstawie złożonych wniosków lub w wyniku ustaleń dokonanych podczas przeprowadzonych kontroli.

Postępowania administracyjne poddano następującym kryteriom oceny:

- czas trwania postępowania,
- skuteczne doręczenie stronie informacji o wszczęciu postępowania,
- poinformowanie strony o możliwości zapoznania się z aktami sprawy w trybie art. 10 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735 z późn. zm.) (dalej k.p.a.),
- podstawa prawna wydania decyzji kończącej postępowanie,
- elementy decyzji,
- skuteczność doręczenia,
- prawidłowość kwalifikacji prawnej.

Ustalono, że postępowania administracyjne były prowadzone zgodnie z przepisami k.p.a. w zakresie terminu załatwienia sprawy. Zgodnie z obowiązującym przepisami zawiadomienie strony o wszczęciu postępowania jest realizacją zasady ogólnej czynnego udziału strony w postępowaniu, a organ prowadzący sprawę jest obowiązany do zapewnienia stronom czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji umożliwić im wypowiedzenie się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. We wszystkich skontrolowanych sprawach znajdowały się zawiadomienia o wszczęciu postępowania, zawierające szczegółową informację na temat obowiązujących przepisów prawnych oraz wskazujące przewidywany termin zakończenia danego postępowania administracyjnego. Wszystkie pisma wychodzące w poszczególnych sprawach oraz decyzje administracyjne podpisywali inspektorzy z upoważnienia i w imieniu organu dokonującego kontroli, czyli LWIORiN. Wszystkie badane decyzje zawierały prawidłowe wskazanie podstawy prawnej, a także szczegółowe uzasadnienie, w którym wskazano odpowiednie normy prawa materialnego, opisywano stan faktyczny wynikający ze zgromadzonego materiału dowodowego oraz jego ocenę. Decyzje zawierały również pouczenie zgodne z przepisami k.p.a. W toku kontroli stwierdzono, iż wydając decyzje nakładającą karę pieniężną w każdym przypadku organ podał nr rachunku konta bankowego, na który należy wpłacić orzeczoną należność.

3. Celowość i gospodarność zawierania umów zleceń i o dzieło, w tym zawieranie umów cywilnoprawnych z pracownikami

Zawieranie umów cywilnoprawnych z osobami fizycznymi lub prawnymi nie zostało uregulowane w Regulaminie Organizacyjnym, jak również żadnym aktem wewnętrznym kierownictwa. Zgodnie z zapisami Regulaminu organizacyjnego WIORiN w Gorzowie Wlkp. do zadań Działu Administracyjnego należy opracowywanie projektów umów z wykonawcami i dostawcami. Kontrolującym udostępniono rejestry umów, które zawierały wykazy umów zawartych przez LWIORiN. Łącznie zarejestrowano 64 umowy. Analiza rejestrów wykazała, że nie zawierały one żadnych pozycji świadczących

o zawartych umowach cywilno - prawnych z pracownikami jednostki.

W rejestrach odnotowuje się m. in. strony umowy, ich przedmiot, datę zawarcia i okres obowiązywania. Umowy zostały zawarte m.in. na:

- wykonanie prac remontowych,
- świadczenie pomocy prawnej,
- monitorowanie obiektów WIORiN,
- przeprowadzenie szkolenia z zakresu ppoż i udzielania pierwszej pomocy,
- przeprowadzenie prac kancelaryjnych – archiwizowanie dokumentów, obsługa korespondencji,
- przewóz osób,
- konserwację i eksploatację systemów alarmowych.

Kontrolujący nie wnieśli uwag do zasadności, celowości i gospodarności zawieranych umów.

Umowy wynikały z bieżących potrzeb jednostki, braków kadrowych czy odpowiednich kwalifikacji zawodowych i zapewniały właściwe wykonywanie zadań Inspektoratu.

Wszystkie umowy zostały podpisane przez LWIORiN Marcina Cyganiaka.

Kontrola wykazała również, że płatności wynagrodzeń za wykonane zlecenia dokonywane były terminowo, każdorazowo przelewem na wskazane konta bankowe, po wcześniejszym wystawieniu rachunku i przedłożeniu ewidencji godzin wykonywania umowy zlecenia przez zleceniobiorcę.

4. Gospodarowanie mieniem ruchomym

4.1 Wykorzystanie służbowych środków transportu

Zasady korzystania przez pracowników ze służbowych środków transportu samochodowego zostały określone w Zarządzeniu Lubuskiego Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa z dnia 24 kwietnia 2018 roku, w sprawie wprowadzenia Instrukcji korzystania z samochodów służbowych, samochodów prywatnych do celów służbowych oraz korzystania z usług zewnętrznych firm transportowych w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa. Nadzorem nad prawidłową eksploatacją środków transportu zajmuje się osoba na stanowisku ds. informatyki.

W kontrolowanym okresie do obsługi siedziby WIORiN w Gorzowie Wlkp. były wykorzystywane następujące samochody: Citroen Berlingo FG6268E, Chevrolet Epica FG67886, Fiat Doblo FG5204J oraz od 2021 roku Hyundai Tucson FG6044M.

Skontrolowano karty drogowe i delegacje służbowe za lata 2020 – 2021.

Rozliczanie kart drogowych dla każdego z pojazdów następowało do 10 dni po zakończeniu każdego miesiąca, w postaci zestawienia faktycznego zużycia paliwa z normami zakładowymi, wyliczonego na podstawie miesięcznego przebiegu kilometrów. Nie wniesiono uwag do rzetelności rozliczania delegacji służbowych dla osób wykorzystujących kontrolowane pojazdy obsługujące siedzibę WIORiN w Gorzowie Wlkp. W kartach drogowych pojazdu z 2021 r. o numerze rejestracyjnym FG6044M oraz FG5204J, jak również FG67886 z 2020 r., stwierdzono brak uzupełnionych tabel dotyczących norm zużycia paliwa, natomiast w kartach drogowych pojazdu FG6268E z czerwca 2021 r. brak jest podpisu dysponenta, uzupełnionych tabel dotyczących norm zużycia paliwa oraz brak uzupełnionej kolumny stanu licznika przy powrocie.

W związku z powyższymi nieprawidłowościami dla pojazdu FG6268E pobrano stosowne wyjaśnienia z których wynika, iż wobec byłego pracownika, który wówczas był kierownikiem Oddziału Gorzów jak również użytkownikiem ww. pojazdu, toczy się

postępowanie sądowe z tytułu wykrycia niezgodności w rozliczaniu kilometrów oraz zużycia paliwa. Karty do dnia rozpoczęcia kontroli nie zostały uzupełnione, gdyż stanowią kluczowy materiał dowodowy w sprawie sądowej.

Z uwagi na charakter sprawy oraz to, że jednostka wykryła nieprawidłowości wskazane powyżej w ramach wewnętrznego systemu nadzoru, ta część kontrolowanego zakresu nie będzie miała odzwierciedlenia w ogólnej ocenie jednostki.

Wyjazdy służbowe LWIORiN na terenie województwa nie wymagały wystawienia polecenia wyjazdu służbowego, a poza województwo odbywały się na podstawie delegacji wystawionej przez Wojewodę Lubuskiego.

Delegacje wystawiane były na wyjazdy do miejscowości zlokalizowanych w Polsce, tj. Białystok, Kraków, Bednary, Poznań, Zamość i Warszawa.

Sprawdzono zasadność wyjazdów służbowych do poleceń nr 505/2021, 495/2021, 383/2021, 295/2021, 202/2021, 82/2021, 25/2020, 36/2020, 515/2020. Wszystkie wyjazdy zostały należycie udokumentowane potwierdzając zasadność wyjazdu służbowego. W okresie objętym kontrolą na wyposażeniu WIORiN było siedemnaście pojazdów, których używano do wyjazdów służbowych. Według zapisów § 7 ust. 3 ww. zarządzenia przekazanie samochodu służbowego w użytkowanie następuje każdorazowo na podstawie protokołu przekazania. Kontrolującym przedstawiono pięć protokołów z 2020 roku. Przekazanie pojazdów odbywały się pomiędzy oddziałami - WIORiN. Uwag nie wniesiono.

Zgodnie z § 14 ust. 1 ww. zarządzenia do celów służbowych mogą być wykorzystywane samochody prywatne. Skontrolowano cztery wnioski z 2020 roku oraz dwa wnioski z 2021 roku w tym zakresie. Przedstawiona dokumentacja zawierała kolejno podpisany przez LWIORiN wniosek o zgodę na korzystanie z samochodu prywatnego, rozliczoną względem przejechanych kilometrów i kosztów delegację służbową oraz potwierdzenie zwrotu kosztów. Zgodnie § 14 ust. 4 zwrot kosztów następuje na zasadach określonych w przepisach rozporządzenia Ministra Infrastruktury wydanego na podstawie art. 34a ust. 2 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz.U. z 2017 r. poz. 2200, z późn. zm.)

Dnia 1 lutego 2021 r. LWIORiN zawarł umowę z Mazowiecką Instytucją Gospodarki Budżetowej MAZOVIA o wydanie i używanie kart flotowych. Umowa została zawarta na czas określony do dnia 31 stycznia 2022 r. Zgodnie z zawartą umową faktury na transakcje dokonywane przez WIORiN z użyciem kart flotowych wystawiane są dwa razy w miesiącu, po zakończeniu każdego z okresów rozliczeniowych. Okres rozliczeniowy zaczyna się od 1 do 15 dnia miesiąca oraz od 16 dnia do ostatniego dnia miesiąca. Każdy z oddziałów otrzymał karty flotowe.

4.2 Ewidencjonowanie środków trwałych

Gospodarowanie mieniem ruchomym zostało uregulowane poprzez wprowadzenie zarządzenia Lubuskiego Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa z dnia 28 października 2019 r. w sprawie ustalenia zasad (polityki) rachunkowości w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. Składniki majątku podlegające ewidencji to także elementy majątku ruchomego przekazane do indywidualnego korzystania m.in. laptopy, telefony komórkowe, drukarki, skanery mobilne, napęd DVD i koncentrator USB.

Wszystkie składniki mienia ruchomego od chwili zakupu są wprowadzane do ewidencji. W jednostce nie wprowadzono uregulowań wewnętrznych w zakresie udostępniania pracownikom składników mienia ruchomego. Jak ustalono, pracownikom jednostki przekazano do użytkowania telefony komórkowe i sprzęt komputerowy. O ile telefony komórkowe zostały przekazane na podstawie Protokołu przekazania zawierającego zasady użytkowania, to sprzęt komputerowy przekazano Protokołem bez żadnych dodatkowych uregulowań.

Opracowany dokument wewnętrzny – „Protokół przekazania oraz zasady użytkowania telefonu komórkowego w WIORiN” zawiera informacje takie jak, imię i nazwisko użytkownika, nr telefonu, nr karty SIM, numer IMEI urządzenia, datę i podpis przekazującego oraz użytkownika. W dokumencie zawarto zasady użytkowania urządzenia oraz pokrywania kosztów związanych z opłatą abonamentu i napraw telefonu, a także finansowania opłat za przekroczenia wysokości przyznanego abonamentu. Określono również zakres odpowiedzialności za sprzęt i przedstawiono procedury jakie należy wykonać w przypadku wystąpienia usterki, kradzieży lub utraty służbowego telefonu komórkowego.

W kontrolowanym okresie nie wystąpiły przypadki utraty, zniszczenia czy uszkodzenia powierzonych pracownikom rzeczowych składników majątku ruchomego.

Przekazanie pozostałego mienia ruchomego pracownikom odbywa się na podstawie Protokołów zawierających określenie przedmiotu użyczenia, określenie użytkownika, datę i podpis osoby przekazującej oraz użytkownika. W związku z powyższym kontrolujący nie wnoszą uwag to kontrolowanego zakresu.

Likwidacja aktywa trwałego odbywa się w oparciu o następujące akty wewnętrzne:

- zarządzenie Lubuskiego Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa z dnia 22 stycznia 2021 r. w sprawie powołania komisji likwidacyjnej i komisji do oceny przydatności składników rzeczowych mienia ruchomego do dalszego użytkowania w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.,
- zarządzenie Lubuskiego Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa z dnia 19 stycznia 2021 r. w sprawie powołania komisji inwentaryzacyjnej do przeprowadzenia inwentaryzacji okazjonalnej w Pracowni Oceny Nasion w Zielonej Górze,
- zarządzenie Lubuskiego Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa z dnia 8 listopada 2021 r. w sprawie powołania komisji likwidacyjnej i komisji do oceny przydatności składników rzeczowych mienia ruchomego do dalszego użytkowania w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.

Kontrolującym okazano dokumenty z działania komisji likwidacyjnej i komisji do oceny przydatności składników rzeczowych mienia ruchomego, takie jak: wnioski o dokonanie likwidacji mienia, opinie o stanie majątku ruchomego, Protokół oceny przydatności składników rzeczowych mienia, Protokół likwidacji mienia ruchomego oraz Protokół przekazania do utylizacji.

Dokonana ocena przydatności do dalszego użytkowania kwalifikowała majątek jednostki jako niezdatny do użytkowania lub nadający się do użytkowania, ale zbędny przy realizacji zadań związanych z działalnością WIORiN.

Wśród zakwalifikowanych do składników majątku niezdatnego do użytkowania lub nieprzydatnego dla jednostki znajdowały się m.in. środki transportu, sprzęt komputerowy, urządzenia i meble biurowe oraz inne.

Składniki majątku zdatne do użytkowania, ale takie które nie nadają się do użytkowania w WIORiN w Gorzowie Wlkp. były zbywane, darowane lub nieodpłatnie przekazywane jednostkom realizującym zadania publiczne, które złożyły stosowne wnioski. Informacje o zbędnych składnikach majątku zamieszczone zostały na stronie Biuletynu Informacji Publicznej WIORiN w Gorzowie Wlkp. Przekazanie składników odbywało się na podstawie Protokołu zdawczo-odbiorczego, który podpisali – przekazujący i przyjmujący. Zbywanie niepotrzebnego majątku odbywało się poprzez organizowanie przetargów, o których informowano na stronie Biuletynu Informacji Publicznej WIORiN w Gorzowie Wlkp. Z protokołów utylizacji mienia ruchomego wynika, że zbędny majątek został przekazany do specjalistycznych firm zajmujących się recyklingiem, odbiorem odpadów niebezpiecznych, utylizacją lub do zakładu demontażu pojazdów. Kontrolujący nie wnoszą uwag to kontrolowanego zakresu.

Działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej

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

5.1 Usługi elektroniczne

Zgodnie z art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 670, z późn. zm.), zwanej dalej „ustawą o informatyzacji”, „podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę”.

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 (Dz.U. z 2017 r. poz. 2247), zwanego dalej „rozporządzeniem KRI”, interoperacyjność na poziomie organizacyjnym osiągnana jest przez m.in.:

- 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;
- publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Na stronie BIP kontrolowanej jednostki w zakładce „Załatwianie Spraw”, „Instrukcje postępowania” opisane są sposoby postępowania w celu załatwienia spraw przez osoby zainteresowane. Inspektorat udostępnia „Pismo ogólne do Urzędu” za pomocą platformy ePUAP.

5.2 Centralne repozytorium wzorów dokumentów elektronicznych

Zgodnie z art. 19 b ust. 3 ustawy o informatyzacji „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".

W trakcie kontroli ustalono, że Inspektorat w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów ePUAP.

5.3 Model usługowy

Zgodnie z § 15 ust. 2 rozporządzenia KRI „zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury”.

W WIORIN brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług. Na stronie internetowej Inspektoratu w zakładce „Załatwianie spraw” znajduje się zakładka „Instrukcje postępowania” gdzie znajduje się 12 plików do pobrania w których opisane jest postępowanie w sprawach. W zakładce formularze są do pobrania 54 wnioski, które można złożyć w siedzibie WIORIN.

5.4 Współpraca systemów teleinformatycznych z innymi systemami

Zgodnie z § 5 ust. 3 pkt 3 rozporządzenia KRI „interoperacyjność na poziomie semantycznym osiągnięta jest przez m.in. stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań”.

Według § 16 ust. 1 rozporządzenia KRI „systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się 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”.

Z uwagi na ograniczony zakres informatyzacji interoperacyjność systemów informatycznych w jednostce jest na poziomie podstawowym.

5.5 Obieg dokumentów w Urzędzie

Zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizacją i egzekwowanie m. in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie”.

W Inspektoracie w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do jednostki zawarte w Instrukcji Kancelaryjnej, stanowiącej załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych i rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67). W WIORIN obowiązuje elektroniczny system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania spraw.

5.6 Formaty danych udostępniane przez systemy teleinformatyczne

Zgodnie z § 17 ust. 1 rozporządzenia KRI „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".

W myśl § 18 ust. 1 rozporządzenia KRI „systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia".

Stosownie do zapisów § 18 ust. 2 rozporządzenia KRI „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".

W toku kontroli dokonano weryfikacji kodowania znaków, w odniesieniu do informacji wymienianych przez systemy Urzędu z innymi systemami zewnętrznymi, na drodze teletransmisji, która wykazała stosowanie standardu Unicode UTF-8.

6. System zarządzania bezpieczeństwem informacji w systemach informatycznych

6.1 Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 1 rozporządzenia KRI „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".

Zgodnie z § 20 ust. 2 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji".

Zgodnie z § 20 ust. 2 pkt 1 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie aktualizacji regulacji wewnętrznych w zakresie - dotyczącym zmieniającego się otoczenia".

W WIORiN wprowadzono Zarządzenie Lubuskiego Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. z dnia 24 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. Dokumentacja ta dotyczy wyłącznie bezpieczeństwa danych osobowych co stanowi naruszenie § 20 ust.1 rozporządzenia KRI.

6.2 Analiza zagrożeń związanych z przetwarzaniem informacji

Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI „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".

Inspektorat nie ma przeprowadzonej analizy ryzyka. Brak analizy ryzyka bezpieczeństwa informacji narusza § 20 ust. 2 pkt 3 rozporządzenia KRI.

6.3 Inwentaryzacja sprzętu i oprogramowania informatycznego

Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację”.

W toku kontroli ustalono, że inwentaryzacja zasobów informatycznych w jednostce prowadzona jest w formie elektronicznej. Specyfikacje sprzętu i oprogramowania są zgodne z rzeczywistością.

6.4 Zarządzanie uprawnieniami

Zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez min. 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”.

Zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4”.

W jednostce brak jest określonych ścisłych zasad i procedur w zarządzaniu uprawnieniami. Nadawanie i odbieranie uprawnień odbywa się poprzez ustne zgłoszenie z działu kadrowego. Lista uprawnień jest na zasadzie upoważnień i nie jest usystematyzowana.

6.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

- zagrożenia bezpieczeństwa informacji,
- skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
- stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich”.

Z ustnych wyjaśnień wynika, że nowi pracownicy są przeszkalani przez pracowników jednostki. Brak dowodów na systematyczne szkolenia pracowników w zakresie bezpieczeństwa.

6.6 Praca na odległość i mobilne przetwarzanie danych

Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość”.

W WIORiN brak jest zapisów o pracy zdalnej. Komputery mobilne nie posiadają szyfrowanych dysków.

6.7 Serwis sprzętu informatycznego i oprogramowania

Zgodnie z zapisami § 20 ust. 2 pkt 10 rozporządzenia KRI: „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zawieranie w umowach

serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji".

Wszystkie zewnętrzne umowy jakie posiada Inspektorat zawierają wymagane zapisy prawne dotyczące powierzenia przetwarzania danych osobowych.

6.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m. in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiając szybkie podjęcie działań korygujących".

Jednostka nie posiada żadnych procedur dotyczących zarządzania incydentami, nie ma określonego pojęcia „incydent”. W WIORiN nie jest prowadzony rejestr incydentów.

Zarządzanie incydentami jest bardzo ważnym aspektem systemu zarządzania bezpieczeństwem informacji. Jest to podstawowe narzędzie przy badaniu podatności systemów informatycznych. Nieprawidłowe zarządzanie incydentami narusza § 20 ust. 2 pkt 13 rozporządzenia.

6.9 Audyt wewnętrzny w zakresie bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok".

Inspektorat nie przeprowadza audytów wewnętrznych w zakresie bezpieczeństwa informacji. Brak przeprowadzania audytów wewnętrznych przekłada się na poziom bezpieczeństwa informacji i stanowi naruszenie § 20 ust. 2 pkt 14 rozporządzenia.

6.10 Kopie zapasowe

Zgodnie z regulacjami § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. minimalizowanie ryzyka utraty informacji w wyniku awarii".

Wykonywanie kopii zapasowych w pewnym sensie reguluje Polityka Bezpieczeństwa Danych Osobowych. Kopie systemów informatycznych tworzone są codziennie i są przechowywane na nośniku danych zlokalizowanym poza lokalizacją danych produkcyjnych. W jednostce brakuje jednak potwierdzenia przeprowadzania testowego odtwarzania kopii zapasowych.

6.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Zgodnie z § 15 ust. 1 rozporządzenia KRI „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".

Inspektorat nie posiada żadnych formalnych regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych, nie prowadził i prowadzi on żadnych prac związanych z wdrożeniami systemów informatycznych. Systemy są narzucone przez jednostki nadrzędne.

6.12 Zabezpieczenia techniczno-organizacyjne informacji

Zgodnie z § 20 ust. 2 rozporządzenia KRI „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:

- monitorowanie dostępu do informacji;
- czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
- 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: ustalenia zasad postępowania z informacjami, zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji środków przetwarzania informacji, w tym urządzeń mobilnych”.

W Inspektoracie istnieją zabezpieczenia fizyczne minimalizujące wystąpienie ryzyka kradzieży informacji i środków przetwarzania informacji. Dostęp do pomieszczeń w których znajdują się urządzenia jest ograniczony do wyznaczonych osób. W głównej lokalizacji Inspektoratu jest wyznaczone osobne pomieszczenie techniczne do którego dostęp mają wyłącznie uprawnione osoby.

Zarządzanie kluczami dostępu do pomieszczeń nie jest uregulowane pisemną procedurą. Z ustnych ustaleń wynika, że istnieją niespisane procedury zarządzania kluczami według których postępują pracownicy.

6.13 Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia KRI „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

- dbałości o aktualizację oprogramowania;
- minimalizowaniu ryzyka utraty informacji w wyniku awarii;
- ochronie przed błędami, utratą, nieuprawnioną modyfikacją;
- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa;
- zapewnieniu bezpieczeństwa plików systemowych;
- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa”.

Zgodnie z § 20 ust. 4 rozporządzenia KRI „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”.

W jednostce na komputerach jest zainstalowane oprogramowanie antywirusowe z aktualnymi definicjami wirusów, brak centralnego zarządzania systemem

antywirusowym. Oprogramowanie serwera jest poza wsparciem producenta i należy je wymienić. W jednostce znajdują się komputery pod kontrolą systemów operacyjnych, które posiadają wsparcie producenta. Jednostki zdalne łączą się do jednostki głównej za pomocą sieci VPN.

6.14 Rozliczalność działań w systemach informatycznych

Zgodnie z zapisami § 21 ust. 2 rozporządzenia KRI „w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:

- systemu z uprawnieniami administracyjnymi;
- konfiguracji systemu, w tym konfiguracji zabezpieczeń;
- przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa”.

Zgodnie z § 21 ust. 3 rozporządzenia KRI „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:

- działań użytkowników nieposiadających uprawnień administracyjnych,
- zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
- zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny — w zakresie wynikającym z analizy ryzyka”.

Zgodnie z § 21 ust. 4 rozporządzenia KRI „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”.

Wszystkie systemy informatyczne stosowane w Inspektoracie posiadają logi systemowe. Nie są one jednak nigdzie kopiowane i niektóre ulegają nadpisaniu, co narusza § 21 ust. 4 rozporządzenia KRI.

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

Zgodnie z § 19 rozporządzenia KRI „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”.

W toku kontroli dokonano weryfikacji zgodności strony internetowej BIP Inspektoratu ze standardem WCAG 2.0 poprzez wykorzystanie narzędzi dostępnych na stronie internetowej <https://validator.w3.org>. Walidacja strony wykazała 17 błędów, jednak nie miały one istotnego wpływu na prezentowanie treści dla osób niepełnosprawnych. Jest ona nadzorowana przez jednostkę nadrzędną i Inspektorat nie ma wpływu na budowę strony. Strona BIP zawiera elementy zmiany kontrastu oraz wielkości czcionki.

8. Realizacja zaleceń pokontrolnych

Kontrolujący sprawdzili stan realizacji zaleceń pokontrolnych wydanych po ostatniej kontroli przeprowadzonej w 2018 r. Z uwagi na część zakresu obecnej kontroli

pokrywającego się z kontrolą prowadzoną w 2018 r., w tym punkcie odniesiono się tylko do tych zagadnień, które nie zostały ujęte w Programie kontroli sporządzonym na potrzeby obecnej kontroli.

W kontrolowanym zakresie uwag nie wniesiono, gdyż zalecenia w przedmiocie ustalania szacunkowej wartości przedmiotu zamówienia, udostępniania informacji publicznej na wnioski, uzupełnienia wykazanych elementów w dokumentacji ochrony danych osobowych oraz nadzoru nad rejestrowaniem umów cywilno-prawnych zostały wdrożone i są realizowane.

Przedstawiając powyższe ustalenia, **zalecam** podjęcie następujących działań:

1. wzmoczenia nadzoru i dokonania takich działań zarządczych, które zapewnią przestrzeganie Instrukcji korzystania z samochodów służbowych, a w szczególności rzetelne wypełnianie karty drogowej;
2. stworzenie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji;
3. wykonywania analizy ryzyka w zakresie bezpieczeństwa informacji;
4. przeprowadzania corocznie wewnętrznych audytów bezpieczeństwa informacji;
5. rozszerzenie zakresu i częstotliwości szkoleń pracowników z zakresu bezpieczeństwa informacji;
6. prowadzenia rejestru incydentów zgodnie z dokumentacją SZBI;
7. stworzenie procedury korzystania z urządzeń mobilnych oraz dostosowania technicznego rozwiązania do wymogów prawnych;
8. wymianę systemu operacyjnego na serwerze;
9. stworzenie formalnych procedur zarządzania uprawnieniami;
10. wdrożenia rozwiązania teleinformatycznego zapewniającego możliwość przechowywania logów systemowych przez okres minimum 2 lat.

W terminie 30 dni liczonym od daty otrzymania niniejszego wystąpienia pokontrolnego, proszę o pisemną informację o sposobie wykonania zaleceń i wykorzystaniu wniosków lub o przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

Podstawa prawna:

¹ art. 46 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224).

² art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej.

WOJEWODA LUBUSKI

Władysław Dajczak