Warszawa, dnia 25 września 2019 r.

WOJEWODA MAZOWIECKI

WK-I.431.9.1.2019

Pani
Mariola Kostewicz
Mazowiecki Wojewódzki Inspektor Farmaceutyczny

Wojewódzki Inspektorat Farmaceutyczny w Warszawie
ul. Floriańska 10
03-707 Warszawa

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 28 ust. 1 pkt 1 ustawy o wojewodzie i administracji rządowej w województwie[1], art. 6 ust. 4 pkt 1 ustawy o kontroli w administracji rządowej[2], art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[3], kontrolerzy: Katarzyna Możdżyńska i Marcel Paprocki – starsi inspektorzy wojewódzcy w Oddziale Kontroli Finansowej i Jednostek Samorządu Terytorialnego Wydziału Kontroli, a także Marek Lenarcik – kierownik Oddziału Administrowania Systemami i Zarządzania Sprzętem Informatycznym w Biurze Informatyki oraz Łukasz Plaskot – starszy inspektor wojewódzki w Oddziale Eksploatacji Systemów Informatycznych i Infrastruktury Serwerowej w Biurze Informatyki Mazowieckiego Urzędu Wojewódzkiego w Warszawie, przeprowadzili w dniach od 3 do 28 czerwca 2019 r. kontrolę problemową w Wojewódzkim Inspektoracie Farmaceutycznym w Warszawie, z siedzibą przy ul. Floriańskiej 10.

---

1 Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2017 r. poz. 2234 ze zm.).
2 Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092 ze zm.).
3 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700 ze zm.).

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

Kontrolą objęto okres od 1 stycznia 2017 r. do 30 maja 2019 r.

Nawiązując do projektu wystąpienia pokontrolnego z 29 lipca 2019 r. oraz stanowiska wobec zastrzeżeń, przekazuję Pani Inspektor wystąpienie pokontrolne.

I. Działanie systemów teleinformatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

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

Kontroli poddano system teleinformatyczny [redacted] używany do realizacji zadań publicznych.

I.A. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami informatycznymi oraz wspomaganie usług drogą elektroniczną

Wojewódzki Inspektorat Farmaceutyczny w Warszawie (dalej WIF) udostępnia elektroniczną skrzynkę podawczą (dalej ESP) znajdującą się na elektronicznej Platformie Usług Administracji Publicznej (dalej ePUAP) umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Zgodnie z § 3 ust. 1 pkt 2, 3, 4, 5 i 6 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii

dokumentów elektronicznych[4] na stronie internetowej Biuletynu Informacji Publicznej (dalej BIP) poinformowano o warunkach organizacyjno-technicznych doręczania dokumentów elektronicznych. WIF umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw w formatach danych określonych w załączniku nr 2 i 3 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej rozporządzenie KRI). Ustalono, że w jednostce nie prowadzono rejestrów publicznych, o których mowa w art. 14 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

Na stronie BIP jednostki w zakładce Menu Podstawowe→Informacje→Elektroniczna Skrzynka Podawcza ePUAP, znajduje się link do usługi „Pismo ogólne do podmiotu publicznego". Po kliknięciu na link następuje przekierowanie do opisu usługi na stronie ePUAP. Opis zawiera dane dotyczące: organu właściwego do realizacji usługi, kogo dotyczy, podstawy prawnej, wymaganych dokumentów, czasu realizacji, opłaty, trybu odwoławczego, rezultatu realizacji usługi, etapów realizacji usługi, poziomu dostępności usługi, poziomu uwierzytelnienia oraz czy usługa wymaga zalogowania.

W badanym okresie jednostka nie przekazywała wzorów dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych[6].

Stwierdzono, że system teleinformatyczny [redacted] powiązany jest z platformą ePUAP. Wymiana danych odbywa się za pomocą platformy ePUAP, która narzuca protokoły komunikacyjne i szyfrujące. Współpraca pomiędzy systemami jest możliwa dzięki wyposażaniu w odpowiedni sprzęt oraz oprogramowanie gwarantujące wymianę danych między systemami, zgodnie z § 16 ust. 1 rozporządzenia KRI. Kodowanie znaków w wysyłanych z systemów lub odbieranych przez te systemy dokumentach odbywa się według standardu UTF-8, w myśl § 17 ust. 1 ww. rozporządzenia.

W jednostce nie udostępnia się w systemach teleinformatycznych usług sieciowych, więc nie opisywano usług sieciowych za pomocą języka WSDL[7].

Zgodnie z Zarządzeniem Nr 2 Mazowieckiego Wojewódzkiego Inspektora Farmaceutycznego z dnia 8 stycznia 2016 r. w sprawie wprowadzenia zmian do zarządzenia

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

[5] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. 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).

[6] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.: *„(…) Nie było zgłaszanych do CRWDE wzorów dokumentów elektronicznych przez WIF".*

[7] Web Services Description Language.

w sprawie wskazania elektronicznego systemu wykonywania czynności kancelaryjnych jako pomocniczego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw, zasad użytkowania systemu [redacted] oraz stosowania Instrukcji kancelaryjnej, Instrukcji archiwalnej i Jednolitego rzeczowego wykazu akt w WIF w Warszawie – wprowadzono zmiany polegające na tym, że w WIF system [redacted] jest podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw dla Urzędu.

W wyniku kontroli stwierdzono brak udostępnienia adresu ESP na stronie BIP, co jest niezgodne z wymaganiami określonymi w § 3 ust. 1 pkt 1 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępnia formularzy, wzorów i kopii dokumentów elektronicznych[8], zgodnie z którym cyt.: *„Podmioty publiczne informują na swoich stronach podmiotowych Biuletynu Informacji Publicznej (…) o: udostępnionym adresie elektronicznej skrzynki podawczej, podanym w formie identyfikatora URI; (…).”*

Przedstawiając powyższe informuję, że realizację zadań dotyczących wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami informatycznymi oraz wspomaganie usług drogą elektroniczną **ocenia się pozytywnie pomimo nieprawidłowości.**

Wskazana ocena wynika z faktu, że w WIF udostępniono elektroniczną skrzynkę podawczą oraz zapewniono jej obsługę, świadczono usługi w formie elektronicznej, jednostka wyposażona jest w odpowiedni sprzęt oraz oprogramowanie umożliwiające wymianę danych między systemami, a także prawidłowo zarządzano obiegiem dokumentacji w jednostce. Mając natomiast na uwadze wyżej opisaną nieprawidłowość dotyczącą braku udostępnienia na BIP adresu ESP, uzasadnione jest sformułowanie oceny pozytywnej pomimo nieprawidłowości.

I.B. Systemy zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

Zgodnie z § 20 ust. 1 rozporządzenia KRI, w okresie objętym kontrolą w jednostce obowiązywało Zarządzenie nr 8/2018 Mazowieckiego Wojewódzkiego Inspektora Farmaceutycznego z dnia 20 lipca 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa i ochrony danych osobowych w Wojewódzkim Inspektoracie Farmaceutycznym w Warszawie (dalej *Polityka*)[9]. W jednostce opracowana została również Instrukcja Zarządzania Systemem

[8] Zgodnie z wyjaśnieniami z dnia 13 czerwca 2019 r. cyt.: *„Na stronie BIP w zakładce Informacje jest zakładka Elektroniczna Skrzynka Podawcza ePUAP. W zakładce tej, oprócz ogólnych informacji o ePUAP jest link do formularza umożliwiającego złożenie wniosku do Wojewódzkiego Inspektora Farmaceutycznego w Warszawie pod nazwą - Pismo ogólne do podmiotu publicznego. Kliknięcie w link powoduje przekierowanie do ePUAP. Po zalogowaniu się na swoje konto w portalu otwiera się automatycznie wspomniany formularz. Ma on pole wyszukiwania, w którym po wpisaniu Wojewódzkiego Inspektoratu Farmaceutycznego w Warszawie pojawia się adres skrytki*”.

[9] *Polityka* opisuje zagadnienia takie jak:

Informatyczny służącym do przetwarzania danych osobowych w Wojewódzkim Inspektoracie Farmaceutycznym (dalej *Instrukcja*)[10] stanowiąca załącznik nr 1 do wyżej opisanej *Polityki.*

Obowiązujące w okresie kontrolowanym ww. dokumenty opisują sposoby nadawania/odbierania uprawnień użytkownikom, określają sposoby pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.

W toku kontroli potwierdzono zaangażowanie kierownictwa jednostki w proces ustanawiania i funkcjonowania systemu bezpieczeństwa informacji m.in. poprzez wprowadzenie *Polityki*, *Instrukcji, Procedur dotyczących kontroli zarządczej*, sporządzania *Planu kontroli Delegatur*, zwoływanie narad i spotkań poświęconych m.in. tematyce dotyczącej bezpieczeństwa informacji, zmian *Regulaminu organizacyjnego*. Wszyscy pracownicy WIF zostali zapoznani z obowiązującą w okresie kontrolowanym *Polityką* i zobowiązani do stosowania określonych w niej zasad.

Zarządzeniem Mazowieckiego Wojewódzkiego Inspektora Farmaceutycznego z dnia 4 stycznia 2010 r. w sprawie wprowadzenia polityki zarzadzania ryzykiem związanym z działalnością WIF, wprowadzono zarządzanie ryzykiem w WIF. Zgodnie z treścią dokumentu zarządzanie ryzykiem jest jednym z elementów sprawowania kontroli zarządczej[11].

- przepisy ogólne,
- obowiązki i odpowiedzialność w zakresie przetwarzania danych,
- zasady przetwarzania danych osobowych,
- obszar przetwarzania danych osobowych,
- bezpieczeństwo i ochrona danych osobowych,
- zasady postępowania w przypadku naruszenia ochrony danych osobowych,
- przekazywanie danych do państwa trzeciego,
- postanowienia końcowe.

[10] *Instrukcja* opisuje zagadnienia takie jak:

- postanowienia ogólne, w tym: podstawy prawne, słownik pojęć, cel i zakres stosowania instrukcji, konfiguracja sprzętu komputerowego użytkownika systemu,
- procedury nadawania uprawnień. Metody i środki uwierzytelniania. Wygaszacze ekranu, w tym: procedury nadawania uprawnień, metody oraz środki uwierzytelniania, wygaszacze ekranu,
- procedury rozpoczynania, zawieszania i kończenia pracy w systemie informatycznym, w tym rozpoczęcie, zawieszenie i zakończenie pracy,
- zabezpieczanie danych w systemie informatycznym, w tym: procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, sposób, miejsce i okres przechowywania kopii zapasowych i elektronicznych nośników informacji, sposób zabezpieczania systemu informatycznego, obowiązki Administratora w zakresie zabezpieczenia systemu informatycznego, procedury wykonywania przeglądów i konserwacji systemu informatycznego, procedura w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego,
- postanowienia końcowe.

[11] Proces zarządzania ryzykiem obejmuje etapy takie jak: określenie misji i zadań Inspektoratu, identyfikacje ryzyka towarzyszącego działalności Inspektoratu, jego analizę i ocenę punktową, określenie metod przeciwdziałania ryzyku oraz monitorowanie zarzadzania ryzykiem. W ww. dokumencie ustalono następujące kategorie ryzyka, podlegające identyfikacji i ocenie: ryzyko finansowe, ryzyko dotyczące zasobów ludzkich, ryzyko działalności, ryzyko zewnętrzne. Ponadto ustalono poziom istotności ryzyka w oparciu o jego oddziaływanie w razie wystąpienia na jednostkę i dzieli się na: ryzyko poważne, ryzyko umiarkowane oraz ryzyko nieznaczne. Kontrolującym przedłożone zostało sprawozdanie z funkcjonowania Kontroli Zarządczej w WIF w Warszawie za 2017 r. i 2018 r. W dokumencie opisane zostały m. in. mechanizmy kontroli dotyczące systemów informatycznych.

Pracownicy wykonujący zadania w badanym systemie teleinformatycznym uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do przypisanych obowiązków, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI.

W okresie objętym kontrolą nie wystąpiły przypadki projektowania i wdrażania systemów teleinformatycznych.

Stosownie do zapisów § 20 ust. 2 pkt 13 ww. rozporządzenia, w jednostce obowiązywały zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji, uregulowane w *Polityce* obowiązującej w okresie kontrolowanym. Zgodnie z udzielonymi wyjaśnieniami w okresie kontrolowanym nie wystąpiły incydenty naruszenia bezpieczeństwa informacji [12].

W Inspektoracie stworzona jest procedura odnosząca się do tworzenia i przechowywania kopii zapasowych. Procedura opisana została w *Instrukcji* stanowiącej załącznik nr 1 do *Polityki* wprowadzonej Zarządzeniem nr 8/2018 Mazowieckiego Wojewódzkiego Inspektora Farmaceutycznego z dnia 20 lipca 2018 r.

Zasady korzystania z urządzeń przenośnych i pracy na odległość zostały uregulowane w *Polityce*. W dokumencie wskazano, że wynoszenie urządzeń mobilnych odbywa się po uzyskaniu zgody Mazowieckiego Wojewódzkiego Inspektora Farmaceutycznego lub jego Zastępcy, a następnie wpisaniu na listę wypożyczeń znajdującą się u Administratora Systemu Informatycznego[13]. Osoba korzystająca z ww. urządzeń zobowiązana jest do zabezpieczenia ich przed kradzieżą, utratą lub zniszczeniem. Po zakończeniu pracy na laptopie użytkownik jest zobowiązany do usunięcia dokumentów zawierających dane osobowe[14]. Zasady wykonywania przeglądów i konserwacji systemu teleinformatycznego określone zostały w *Instrukcji*[15].

Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami w jednostce, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków

---

[12] W trakcie kontroli przedłożono do wglądu *„Rejestr incydentów naruszenia bezpieczeństwa informacji”* – brak zapisów w rejestrze w okresie kontrolowanym.

[13] Funkcję Administratora Systemu Informatycznego w WIF pełni informatyk.

[14] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.: *„W okresie objętym kontrolą zaistniały przypadki korzystania z przenośnych laptopów poza budynkiem. Użytkownicy, którzy korzystali z laptopów poza budynkiem mieli na to zgodę Mazowieckiego Wojewódzkiego Inspektora Farmaceutycznego (…)”*. Kontrolującym przedłożono do wglądu przykładową zgodę oraz listę wypożyczeń sprzętu.

[15] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.*: „W okresie objętym kontrolą w WIF w Warszawie dokonywano przeglądu i konserwacji sprzętu komputerowego będącego na wyposażeniu jednostki. Wymieniono m.in. wszystkie zużyte baterie w UPS-ach podłączonych do komputerów, okresowo są przeglądane systemy i oprogramowanie komputerów. W skład przeglądu okresowego wchodziły m.in.:*

- *regularne sprawdzanie sprzętu komputerowego i wymiana zużytych elementów;*
- *regularne przeprowadzanie czyszczenia dysku;*
- *kontrola programów uruchamianych przy starcie systemu (wpisanie w Wyszukaj programy i pliki “msconfig” i odznaczenie z listy Uruchamianie niepotrzebnych aplikacji);*
- *kontrola działających w tle procesów (przez Menadżera zadań);*
- *systematyczne sprawdzanie komputera programami antywirusowymi i antyspyware;*

Pomoc przy występowaniu problemów technicznych udzielana jest na bieżąco”.

przetwarzania informacji, w tym urządzeń oraz zasady dotyczące zapewnienia ochrony przetwarzanych informacji, zostały zawarte w *Polityce* i *Instrukcji* obowiązujących w okresie kontrolowanym.

W toku kontroli ustalono, że zgodnie z § 20 ust. 2 pkt 7, 9, 11 i 12 rozporządzenia KRI, WIF zapewnia ochronę przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, zabezpieczenie informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie, poprzez:

- ustanowienie regulacji wewnętrznych, w których ustalono zasady postępowania z informacjami w jednostce i zapewnienie ochrony przetwarzanych informacji oraz zasady zapewniające odpowiedni poziom bezpieczeństwa systemów teleinformatycznych,
- wyznaczenie stref bezpieczeństwa[16], np. [redacted], ustalenie zasad pobierania i zdawania kluczy do pomieszczeń,
- nadawanie użytkownikom uprawnień do systemów,
- wymóg logowania się do systemu poprzez uwierzytelnianie hasłem przy logowaniu,
- automatyczną aktualizację oprogramowania systemów operacyjnych komputerów,
- aktualizację systemów operacyjnych serwerów,
- funkcjonowanie urządzeń brzegowych typu firewall,
- zabezpieczenie komputerów użytkowników aktualnym oprogramowaniem antywirusowym,
- ustanowienie regulacji dotyczących konserwacji, napraw i utylizacji sprzętu i oprogramowania.

Wykorzystywany w WIF system [redacted] zapewnia rozliczalność operacji. W stosunku do systemu [redacted] przeglądu logów dokonują pracownicy Mazowieckiego Urzędu Wojewódzkiego w Warszawie.

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. Nieprzeprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji[17], mimo obowiązku wynikającego z § 20 ust. 2 pkt 3 rozporządzenia KRI, zgodnie z którym cyt.: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności*

[16] Obszar, w którym przetwarzane są dane osobowe obejmuje wydzielone pomieszczenia. W WIF wydzielone zostały trzy strefy, a mianowicie:
- strefa A – ogólnodostępna gdzie dostęp posiadają wszyscy pracownicy,
- strefa B – dostępna tylko dla pracowników, a dla osób trzecich np. interesantów tylko w obecności pracownika. Do przyjmowania interesantów wydzielone zostało miejsce mieszczące się na korytarzu,
- strefa C – dostępna tylko dla pracowników.

Wykaz obszarów przetwarzania danych osobowych przedłożony został kontrolującym.

[17] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.: *„W WIF w Warszawie w okresie objętym kontrolą nie przeprowadzano okresowych analiz ryzyka. Ostatnia udokumentowana analiza ryzyka była utworzona za 2015 rok. Z analizy ryzyka wynikało, że poziom ryzyka dla jednostki jest minimalny. Zabezpieczenia systemów są na bieżąco monitorowane, systemy antywirusowe aktualizowane są na bieżąco. (…) W 2018 r. W związku z wprowadzeniem w 2018 r. Polityki bezpieczeństwa i ochrony danych osobowych w Wojewódzkim Inspektoracie Farmaceutycznym w Warszawie przewidywane jest przeprowadzenie w III kwartale 2019 r. analizy ryzyka”.*

przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (…) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji (…)".

2. Nieprzeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji[18]. Działaniem takim naruszono dyspozycję § 20 ust. 2 pkt 14 ww. rozporządzenia, zgodnie z którym kierownictwo umożliwia realizację i egzekwowanie działań w zakresie cyt.: *„(…) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok"*.
3. Niezapewnienie osobom zaangażowanym w proces przetwarzania informacji, szkoleń ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna czy stosowanie środków zapewniających bezpieczeństwo informacji[19], czym naruszono wymogi § 20 ust. 2 pkt 6 rozporządzenia KRI.

---

[18] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.: *„W WIF w Warszawie w okresie objętym kontrolą nie przeprowadzano audytu wewnętrznego w zakresie bezpieczeństwa informacji. Były przeprowadzane kontrole wewnętrzne przez informatyka. WIF w Warszawie jest niewielką jednostką i z powodu ograniczonych środków budżetowych nie ma możliwości zatrudnienia audytora (…)"*.

[19] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.: *„Mazowiecki Wojewódzki Inspektor Farmaceutyczny odbywa cykliczne spotkania z pracownikami Wojewódzkiego Inspektoratu Farmaceutycznego. Spotkania odbywają się w każdy poniedziałek, z pracownikami Delegatur poprzez wideokonferencję. Ponadto, raz na kwartał Mazowiecki Wojewódzki Inspektor Farmaceutyczny organizuje spotkania ze wszystkimi pracownikami Wojewódzkiego Inspektoratu Farmaceutycznego w siedzibie Inspektoratu w Warszawie.*
W trakcie przedmiotowych spotkań poruszane są różne zagadnienia, w szczególności związane z bieżącymi zadaniami realizowanymi przez Inspekcję Farmaceutyczną w ramach zmieniającego się otoczenia prawnego. Zmiany w zakresie przepisów prawa omawiane są przez pracowników Działu Prawno-Organizacyjnego Wojewódzkiego Inspektoratu Farmaceutycznego. W trakcie jednego ze spotkań w dniu 25 maja 2018 r. omówione zostały przepisy Rozporządzenia 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. Ponadto , w trakcie spotkania Mazowiecki Wojewódzki Inspektor Farmaceutyczny omówił sposób postępowania z przekazywaną do Wojewódzkiego Inspektoratu Farmaceutycznego dokumentacją oraz sposób jej zabezpieczenia, w tym zwrócił uwagę na konieczność zamykania pomieszczeń oraz zasadę tzw. czystego biurka. Mazowiecki Wojewódzki Inspektor Farmaceutyczny poinformował również o możliwych zagrożeniach w związku z przetwarzaniem informacji oraz wskazał na odpowiedzialność pracowniczą w związku z niedochowaniem warunków prawidłowego przetwarzania danych osobowych" oraz zgodnie z wyjaśnieniami z dnia 18 czerwca 2019 r. cyt.*:" (…) Dodatkowo czterech pracowników WIF uczestniczyło w dniu 23 maja 2018 r. w wykładzie eksperckim „RODO w pigułce" organizowanym przez Krajową Szkołę Administracji Publicznej (…). Ponadto pracownik zatrudniony na stanowisku informatyka uczestniczył w szkoleniach:*
„Nowa ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych – WCAG 2.0 – standardy dostępności w praktyce", które odbyło się w dniu 24.04.2019 r.;
„Umiejętności wdrożenia i świadczenia e-usług na rzecz osób fizycznych i przedsiębiorstw, prawa i obowiązki stron wynikające z przepisów dotyczących elektronicznej komunikacji z urzędem, w tym Analiza procesów + podstawy BPMN z elementami warsztatu", które odbyło się w dniach 23-25.10.2017 r.
„Świadczenie e-usług na platformie e-PUAP, Funkcjonowanie Elektronicznej Skrzynki Podawczej", które odbyło się w dniach 8-9.11.2017 r. (…).
MWIF informuje, że z uwagi na możliwości finansowych Wojewódzkiego Inspektoratu Farmaceutycznego uczestnictwo pracowników WIF w szkoleniach zewnętrznych jest ograniczone. Dlatego też spotkania, o których mowa powyżej i dzielenie się wiedzą jest istotnym elementem doskonalenia zawodowego i szkolenia pracowników WIF".

4. Niewystarczające doprecyzowanie w umowach zawartych pomiędzy WIF, a podmiotami zewnętrznymi[20], zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Działaniem takim naruszono wymóg § 20 ust. 2 pkt 10 ww. rozporządzenia.
5. Niezapewnienie aktualności inwentaryzacji sprzętu i oprogramowania służących do przetwarzania informacji obejmującej ich rodzaj i konfigurację[21], czym naruszono § 20 ust. 2 pkt 2 rozporządzenia KRI.
6. Nieodebranie byłym pracownikom uprawnień do systemu [redacted] czym naruszono zapis § 20 ust. 2 pkt 5 powyższego rozporządzenia. Ustalono, że odbieranie byłym pracownikom uprawnień do pracy w systemie [redacted] odbywa się poprzez opcję „Ukryj" dostępną na koncie użytkownika. Powyższa opcja jest niewłaściwa ponieważ konto oznaczone jako „Ukryte" nadal pozostaje aktywne i można się na nie logować.
7. Kopie zapasowe [redacted] pełniącego rolę kontrolera domeny w jednostce nie są wykonywane. Okresowe testy odtworzeniowe też nie są wykonywane jak również część kopii zapasowych[22] przechowywana jest w tym samym miejscu co kopiowane dane. Powyższe nie spełnia wymogów zapisu określonego w § 20 ust. 2 pkt 7 i 12 lit. b i e rozporządzenia KRI, zgodnie z którym cyt.: *"Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: (…) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami (…) oraz zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: (…), minimalizowaniu ryzyka utraty informacji w wyniku awarii, (…), zapewnieniu bezpieczeństwa plików systemowych (…)"*.
8. Nie przestrzegano przyjętych wymagań dotyczących haseł dostępu do systemów informatycznych[23], co było niezgodne z § 20 ust. 2 pkt 7 rozporządzenia KRI, zgodnie z którym

[20] Dotyczy umów określających zasady udostępniania [redacted]

[21] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.: *„W WIF w Warszawie nie posiadamy* [redacted] *Są szczegółowe dane odnośnie komputerów używanych w WIF w Warszawie, zarówno jeśli chodzi o konfigurację sprzętową, jak i oprogramowanie (…)"*. Zgodnie z rozmową z informatykiem przeprowadzoną w dniach 19 i 26 czerwca 2019 r. ustalono, że raz do roku przeprowadzana jest przez informatyka kontrola wewnętrzna stacji roboczych, w wyniku której powstaje szczegółowe zestawienie konfiguracji sprzętu i oprogramowania.

[22] Raz w miesiącu Administrator wykonuje kopie udziałów sieciowych z [redacted] Ustalenia zawarte zostały w protokole z przeprowadzonej w dniach 19 i 26 czerwca 2019 r. rozmowie z informatykiem.

[23] Brak wymagania odpowiedniej złożoności hasła oraz automatycznego wymuszenia jego zmiany do większości komputerów w jednostce. Ustalenia zweryfikowano na przykładowej jednostce z systemem Windows 7. Odpowiednie wymagania spełnia tylko kilka komputerów podłączonych do domeny jednostki. Według wyjaśnień Administratora, użytkownicy są poinstruowani, aby hasła do komputerów były odpowiednio silne oraz zmieniane

cyt.: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: (…) zapewnienia ochrony przetwarzanych 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".*

Podczas przeprowadzania czynności kontrolnych stwierdzono także, że Polityka bezpieczeństwa i ochrony danych osobowych wprowadzona została w WIF w dniu 20 lipca 2018 r.[24] pomimo, że obowiązek wynikający z § 20 ust. 1 rozporządzenia KRI zgodnie z którym cyt.: *„Podmiot realizujący zadania publiczne opracowuje i ustanawia, (…) system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność"*, obowiązuje od 31 maja 2012 r.

Ponadto stwierdzono, że podstawowe zasady, które miały zapewnić bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość zostały uregulowane w *Polityce.* Podano w nich m.in., że osoba korzystająca z ww. urządzeń zobowiązana jest do zabezpieczenia ich przed kradzieżą, utratą lub zniszczeniem, a po zakończeniu pracy na laptopie użytkownik jest zobowiązany do usunięcia dokumentów zawierających dane osobowe. W ww. zasadach nie zostało opisane w jaki skuteczny sposób użytkownik winien dokonać tych zabezpieczeń oraz w jaki skuteczny sposób usunąć dokumenty zawierające dane osobowe.

Stwierdzono także, że w procedurze dotyczącej tworzenia kopii zapasowych opisanej w *Instrukcji* niedookreślone zostały terminy, miejsce, czas oraz sposób usunięcia wytworzonych kopii zapasowych.

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

---

nie rzadziej, niż co 30 dni. Powyższe wynika z rozmowy z informatykiem przeprowadzonej w dniach 19 i 26 czerwca 2019 r.

[24] Zgodnie z wyjaśnieniami z dnia 12 czerwca 2019 r. cyt.: *"Oprócz przedłożonych już dokumentów Wojewódzki Inspektorat Farmaceutyczny w Warszawie nie posiada innych dokumentów dotyczących Systemu Zarządzania Bezpieczeństwem Informacji (…)"*.

Ustalenia kontroli wykazały, że w jednostce opracowano dokumentację systemu zarządzania bezpieczeństwem informacji[25], z którą pracownicy zostali zapoznani, a osoby zaangażowane w proces przetwarzania informacji posiadały stosowne uprawnienia. Ponadto systemy teleinformatyczne funkcjonujące w jednostce posiadały wymagane zabezpieczenia techniczno-organizacyjne.

Mając natomiast na uwadze: nieprzeprowadzenie okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji, nieprzeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, niezapewnienia szkolenia osobom zaangażowanym w proces przetwarzania informacji, niedoprecyzowanie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, niezapewnienie aktualności inwentaryzacji sprzętu i oprogramowania służących do przetwarzania informacji obejmującej ich rodzaj i konfigurację, nieodebranie byłym pracownikom uprawnień, nie wykonywanie kopii bezpieczeństwa, nie przestrzeganie wymagań dotyczących haseł dostępu do systemów oraz inne opisane powyższej nieprawidłowości, uzasadnione jest sformułowanie oceny negatywnej.

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

Stronę internetową oraz stronę BIP jednostki działające pod adresami www.wif.waw.pl oraz www.bip.wif.waw.pl poddano weryfikacji zgodności ze standardem WCAG 2.0 za pomocą walidatorów http://validator.w3.org oraz http://jigsaw.w3.org/css-validator/. Po weryfikacji ww. stron stwierdzono spełnienie wymagań WCAG 2.0 określonych w załączniku nr 4 rozporządzenia KRI. W wyniku kontroli stwierdzono, że dostępna strona internetowa i strona BIP jednostki zawierają rozwiązania techniczne umożliwiające osobom niepełnosprawnym zapoznanie się z treścią informacji, czym spełniono wymogi określone w § 19 ww. rozporządzenia.

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

Ustalenia kontroli wykazały, że w jednostce zapewniono dostępność informacji zawartych na stronie internetowej oraz stronie BIP urzędu dla osób niepełnosprawnych. Mając na uwadze powyższe uzasadnionym jest sformułowanie oceny pozytywnej.

[25] Dokument wprowadzony został w dniu 20 lipca 2018 r.

Przedstawiając powyższe ustalenia, zobowiązuję Panią Inspektor do podjęcia działań w celu wyeliminowania stwierdzonych nieprawidłowości, a w szczególności do:

1. Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, zgodnie z obowiązkiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI.
2. Przeprowadzania nie rzadziej niż raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z dyspozycją § 20 ust. 2 pkt 14 ww. rozporządzenia.
3. Zapewnienia osobom zaangażowanym w proces przetwarzania informacji, szkoleń ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna czy stosowanie środków zapewniających bezpieczeństwo informacji, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.
4. Doprecyzowania w umowach zawartych pomiędzy WIF, a podmiotami zewnętrznymi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z wymogiem określonym w § 20 ust. 2 pkt 10 ww. rozporządzenia.
5. Zapewnienia aktualności inwentaryzacji sprzętu oraz oprogramowania służących do przetwarzania informacji obejmującej ich rodzaj i konfigurację, zgodnie z dyspozycją zawartą w § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI.
6. Wykonywania kopii zapasowych serwera [redacted] pełniącego rolę kontrolera domeny w jednostce oraz wykonywania okresowych testów odtworzenia, a także do przechowywania kopii zapasowych w innym miejscu niż kopiowane dane, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 7 i 12 lit. b i e rozporządzenia w sprawie KRI .
7. Przestrzegania przyjętych wymagań dotyczących haseł dostępu do systemów informatycznych, stosownie do zapisów określonych w § 20 ust. 2 pkt 7 ww. rozporządzenia.

Ponadto wskazanym byłoby również doprecyzowanie w *Polityce* w części dotyczącej podstawowych zasad zapewnienia bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość opisu w jaki skuteczny sposób użytkownik winien dokonać zabezpieczeń przed kradzieżą, utratą lub zniszczeniem urządzeń oraz w jaki skuteczny sposób usunąć dokumenty zawierające dane osobowe. Natomiast w procedurze dotyczącej tworzenia kopii zapasowych opisanej w *Instrukcji* wskazanym byłoby dookreślenie terminów, miejsca, czasu oraz sposobu usunięcia wytworzonych kopii zapasowych.

Odstępuje się natomiast od sformułowania zaleceń pokontrolnych do nieprawidłowości opisanych na: stronie 4 w części I.A., stronie 9 pkt 6 w części I.B., niniejszego wystąpienia pokontrolnego, w związku z ich wyeliminowaniem przez jednostkę kontrolowaną po zakończeniu czynności kontrolnych.

Przedstawiając powyższe informuję, że zgodnie z art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze oraz zobowiązuję Panią Inspektor na podstawie art. 49 ww. ustawy do przekazania, w terminie 14 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków pokontrolnych lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości i uchybień.

Z up. WOJEWODY MAZOWIECKIEGO

Bogusław Krupa
Zastępca Dyrektora
Wydziału Kontroli