WOJEWODA LUBUSKI

Gorzów Wlkp., dnia 14 grudnia 2019 r.

NK-II.1611.1.2019.RBur

Pan
bryg. Patryk Maruszak
Lubuski Komendant Wojewódzki
Państwowej Straży Pożarnej

Wystąpienie pokontrolne
z kontroli przeprowadzonej w trybie zwykłym w Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wlkp.

Na podstawie art. 28 ust. 1 pkt. 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz.U.2019.1464 t.j.) oraz art. 6 ust. 4 pkt. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U.2011.185.1092 ze zm.), w dniach od 9 kwietnia 2019 r. do 9 lipca 2019 r. upoważnieni pracownicy Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp. w składzie:

- Robert Burek – starszy inspektor wojewódzki - przewodniczący zespołu,
- Agnieszka Mróz – kierownik Oddziału Kadr i Szkolenia w Biurze Organizacji i Kadr LUW,
- Daniela Milczarczyk – główny specjalista w Biurze Organizacji i Kadr LUW,
- Michał Szerwiński – inspektor wojewódzki w Biurze Organizacji i Kadr LUW,
- Aleksandra Fąfara – starszy inspektor wojewódzki w Biurze Organizacji i Kadr LUW,
- Przemysław Pikuła – samodzielne stanowisko pracy: ABI,
- Michał Piaskowski – kierownik Oddziału Informatyki w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych LUW,
- Izabela Milczarek – informatyka ds. administrowania systemami informatycznymi w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych LUW,

przeprowadzili kontrolę w Komendzie Wojewódzkiej Państwowej Straży Pożarnej, ul. Wyszyńskiego 64, 66-400 Gorzów Wlkp.

Kontrolą objęto okres od 1 stycznia 2017 r. do 31 grudnia 2018 r., z tym że:

- optymalizacja zatrudnienia, zakres i szczegółowość informacji publicznych udostępnianych w Biuletynie Informacji Publicznej oraz ich aktualizacja od 1 stycznia 2017 r. do dnia rozpoczęcia kontroli,
- ochrona danych osobowych od 1 stycznia 2017 r. do dnia zakończenia kontroli,
- działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej – stan obecny.

Projekt wystąpienia pokontrolnego otrzymał Pan w dniu 2 grudnia 2019 r., do którego nie zostały wniesione zastrzeżenia.

W związku z powyższym na podstawie art. 47 ustawy o kontroli w administracji rządowej przekazuję Panu wystąpienie pokontrolne.

1. Zakres działalności Komendy Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wlkp. objęty kontrolą.

Kontrola obejmowała swym zakresem optymalizację zatrudnienia, realizację przepisów ustawy o służbie cywilnej (nabory na wolne stanowiska, służba przygotowawcza, oceny pracownicze) i ustawy o dostępie do informacji publicznej. Dokonywanie zamówień publicznych, zawieranie umów cywilnoprawnych. Gospodarowanie mieniem ruchomym, w tym środkami transportu samochodowego. Ochronę danych osobowych. Działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.

2. Ocena skontrolowanej działalności.

Kontrolowaną działalność oceniono **pozytywnie**.

Pomimo pozytywnej oceny ogólnej, stwierdzono jednak **uchybienia** w związku z brakiem Indywidualnego Programu Rozwoju Zawodowego oraz Programu Zarządzania Zasobami Ludzkimi, natomiast **nieprawidłowości** stwierdzono w zakresie oceny:
- systemu zarządzania bezpieczeństwem informacji w systemach informatycznych,
- zapewnienia dostępności informacji zawartych na stronach internetowych dla osób niepełnosprawnych.

3. Zakres odpowiedzialności.

Pracą Komendy Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wlkp. (dalej „KW PSP") kieruje Lubuski Komendant Wojewódzki Państwowej Straży Pożarnej bryg. Patryk Maruszak (dalej „LKW PSP") przy pomocy zastępców, bryg. Janusza Drozdy oraz st. bryg. Lesława Glińskiego. W okresie do 28 września 2017 r. funkcję LKWPSP pełnił st. bryg. Sławomir Klusek.

4. Opis ustalonego stanu faktycznego.

Optymalizacja zatrudnienia

Stwierdzono, że w kontrolowanej jednostce nie prowadzi się analizy w zakresie optymalizacji zatrudnienia z uwzględnieniem prawidłowego obciążenia zadaniami zaangażowanych etatów, a tym samym aktualizacji obciążenia zaangażowanych etatów w odniesieniu do zmieniających się zadań. Przyjęty Regulamin organizacyjny KW PSP w Gorzowie Wlkp. reguluje kwestie zadań wspólnych wszystkich wydziałów jak i zadań szczegółowych dla poszczególnych wydziałów oraz samodzielnych stanowisk pracy. Natomiast osoby wyznaczone do kierowania wydziałami odpowiadają za prawidłowy podział pracy, organizację i ciągłość pracy oraz prawidłowość realizowanych zadań.

Analiza zaangażowania stanu osobowego w realizację zadań ustawowych lub zleconych w stosunku do obsługi administracyjnej i funkcjonowania KW PSP przedstawia się następująco: w latach 2017/2018 był to stosunek 14/4, przy czym zatrudnionych w tym czasie w jednostce było jeszcze, odpowiednio 56/58 funkcjonariuszy.

W toku czynności kontrolnych dokonano analizy zakresów czynności pracowników Wydziału Finansów, Wydziału Kadr, samodzielnych stanowisk pracy oraz dwóch pomocniczych stanowisk służbowych (robotnik gospodarczy, technik) w stosunku do realizacji ustawowych zadań jednostki oraz zapisów regulaminu organizacyjnego, w tym schematu organizacyjnego. Kontrolujący ustalili, że zapisy w zakresach czynności są zgodne z zadaniami Komendy Wojewódzkiej PSP, zgodne z zadaniami wspólnymi i zakresami działania komórek organizacyjnych i samodzielnych stanowisk pracy. Nie stwierdzono mnożenia tych samych czynności w odniesieniu do zadań merytorycznych zapisanych w zakresach obowiązków pracowników na poszczególnych stanowiskach pracy.

Sprawdzono, czy pracownicy biorą udział w dodatkowych zadaniach wykonywanych w czasie pracy, za które otrzymują dodatkowe wynagrodzenie. Ustalono, że w kontrolowanym okresie, przyznano 2 pracownikom dodatki zadaniowe na łączną kwotę 6000,00 zł. W poszczególnych latach przedstawiało się to następująco: 2017 r. – 4000,00 zł, 2018 r. – 2000,00 zł. Sprawdzono, czy zadania za które otrzymano dodatkowe wynagrodzenie nie pokrywają się z obowiązkami służbowymi określonymi w zakresach czynności poszczególnych pracowników. Zbieżności stwierdzono w jednym przypadku, jak ustalono wynikły one z przejęcia i wykonywania dodatkowych czynności z powodu redukcji etatu, odejścia pracownika z pracy i przejęcia części jego zadań. Pozostałe dodatki zadaniowe zostały przyznane w związku z zaistniałymi bieżącymi potrzebami niezbędnymi do realizacji i wykonywania zadań, pełnienia określonych funkcji i prawidłowego funkcjonowania jednostki.

W kontrolowanej jednostce zostały utworzone samodzielne stanowiska pracy oraz pomocnicze stanowiska. W związku z tym dokonano oceny zasadności utworzenia tych stanowisk oraz ilościowej obsady kadrowej. W okresie objętym kontrolą funkcjonowały następujące stanowiska:

- samodzielne stanowisko pracy ds. pomocy prawnej,
- samodzielne stanowisko pracy ds. ochrony danych,
- pomocnicze stanowisko pracy – technik,

- pomocnicze stanowisko pracy – robotnik gospodarczy,
- psycholog.

Poza stanowiskami technika i robotnika gospodarczego, gdzie zatrudniono po 2 osoby, w pozostałych przypadkach stanowiska zostały obsadzone jednoosobowo.

Zadania przypisane do poszczególnych samodzielnych stanowisk są realizowane. Kontrolujący nie wnoszą uwag do kontrolowanego zakresu.

Skontrolowano zaangażowanie stanowisk pomocniczych i obsługi KW PSP w strukturze całej Komendy. Kontrola wykazała, że w strukturze organizacyjnej funkcjonują jedynie dwa wyżej opisane stanowiska pracy (technik, robotnik gospodarczy) oraz, że nie przewidziano stanowisk pracy dla kierowcy samochodu służbowego. Pracownicy Komendy osobiście kierują pojazdami służbowymi.

Realizacja przepisów ustawy o służbie cywilnej

Zasady organizacji służby przygotowawczej. W kontrolowanej jednostce, w zakresie organizacji służby przygotowawczej skontrolowano wszystkie dokumenty dotyczące ww. obszaru. Stwierdzono, że służba przygotowawcza odbywa się zgodnie z przepisami z art. 36 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej. W okresie objętym kontrolą obowiązkowi odbycia służby podlegało 4 pracowników. Wszyscy pracownicy zostali zwolnieni z odbywania służby przygotowawczej. Zgodnie z art. 36 ust. 5 ww. ustawy, pracownicy przystąpili do egzaminu i zdali z wynikiem pozytywnym. Wszystkie dokumenty potwierdzające powyższe fakty znajdują się w aktach osobowych pracownika.

Oceny w służbie cywilnej. W kontrolowanej jednostce, w zakresie terminowości i zgodności z prawem przeprowadzania pierwszej oceny w służbie cywilnej, skontrolowano wszystkie dokumenty dotyczące ww. obszaru. Kontroli podlegało 4 pierwsze oceny.

W toku kontroli stwierdzono, że pierwsza ocena w służbie cywilnej została dokonana prawidłowo, zgodnie z przepisami ustawy z dnia 21 listopada 2008 roku o służbie cywilnej, rozporządzenia Prezesa Rady Ministrów z dnia 23 lipca 2015 r. w sprawie szczegółowych warunków i sposobu dokonywania pierwszej oceny w służbie cywilnej (Dz. U. 2015, poz. 1144). W toku kontroli ustalono, że arkusze I oceny w służbie cywilnej dla 4 pracowników zostały wypełnione prawidłowo. Całość dokumentacji związanej z pierwszą oceną przechowywana jest w aktach osobowych pracowników objętych obowiązkiem przeprowadzenia pierwszej oceny.

W kontrolowanej jednostce, w zakresie terminowości i zgodności z prawem przeprowadzania ocen okresowych w służbie cywilnej, skontrolowano wszystkie oceny, tj. 6 arkuszy ocen okresowych pracowników. Oceny dokonywane były na podstawie rozporządzenia Prezesa Rady Ministrów z dnia 23 lipca 2015 r. w sprawie warunków i sposobu przeprowadzania ocen okresowych członków korpusu służby cywilnej (Dz.U.2015.1143) oraz rozporządzenia Prezesa Rady Ministrów z dnia 4 kwietnia 2016 r. w sprawie warunków i sposobu przeprowadzania ocen okresowych urzędników służby cywilnej i pracowników

służby cywilnej (Dz.U.2016.470). We wszystkich przypadkach, oceny okresowe zostały sporządzone prawidłowo zgodnie z obowiązującymi przepisami. Stwierdzono również, że w okresie kontrolowanym nie wystąpiły przypadki przyznania ocen negatywnych, stąd też brak jest możliwości sprawdzenia czy została zachowana procedura w momencie przyznania takowej oceny.

Nie stwierdzono odwołania od jakiejkolwiek oceny okresowej przez pracownika do pracodawcy, czy też Sądu Pracy.

W toku kontroli stwierdzono również, że każdemu z 6 pracowników podlegającym ocenie okresowej, bezpośredni przełożeni nie ustalili na osobnym druku Indywidualnego Programu Rozwoju Zawodowego. Obowiązek ten wynika z art. 108 ustawy dnia 21 listopada 2008 roku o służbie cywilnej. W Komendzie nie wprowadzono Procedury Indywidulanego Programu Rozwoju Zawodowego dla pracowników służby cywilnej Komendy Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wlkp. Wynika to z faktu bardzo małej liczby pracowników zatrudnionych w służbie cywilnej. Wnioski dotyczące rozwoju pracowników zostały zawarte w arkuszu oceny w części II.
Kontrola wykazała również, że w Komendzie Wojewódzkiej nie wprowadzono Programu Zarządzania Zasobami Ludzkimi, którego obowiązek sporządzenia wynika z art. 25 ust. 4 pkt 2 lit. a ustawy z dnia 21 listopada 2008 r. o służbie cywilnej oraz zarządzenia nr 3 Szefa Służby Cywilnej z dnia 30 maja 2012 r. w sprawie standardów zarzadzania zasobami ludzkimi w służbie cywilnej. Fakt ten wynika z bardzo małej liczby pracowników zatrudnionych w służbie cywilnej oraz z objęcia tych pracowników systemem rozwoju i organizacji obowiązujących w strukturach Państwowej Straży Pożarnej.

Ocena rzetelności i legalności przeprowadzanych naborów. W kontrolowanej jednostce nabór do służby cywilnej odbywa się w oparciu o uregulowania zawarte w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej. Informacje o wolnych stanowiskach są publikowane w Biuletynie Informacji Publicznej Kancelarii Prezesa Rady Ministrów oraz BIP Komendy Wojewódzkiej PSP w Gorzowie Wlkp. oraz zamieszczane na tablicy ogłoszeń w siedzibie Komendy.
Nie ma stworzonej wewnętrznej procedury naboru do służby cywilnej z uwagi na bardzo małą ilość stanowisk cywilnych, które mają charakter pomocniczy w stosunku do wiodących stanowisk mundurowych.
W okresie objętym kontrolą przeprowadzono 5 naborów do służby cywilnej – 4 w 2017 r. i jeden w 2018 roku.
Na podstawie skontrolowanych dokumentów stwierdzono, że nabory do służby cywilnej zostały przeprowadzane zgodnie z ustawą o służbie cywilnej. Prawidłowo dokonano formalnej weryfikacji ofert pracy, wymagania związane ze stanowiskiem wskazane w ogłoszeniu są zgodne z opisem danego stanowiska. Informacje o naborach oraz wynikach naborów zostały upowszechnione zgodnie z zapisami art. 28 oraz art. 31 ustawy z dnia 21 listopada 2008 roku o służbie cywilnej (Dz.U.2016.1345 j.t).

Przestrzeganie przepisów ustawy o dostępie do informacji publicznej.

Na podstawie § 8 pkt 5 Regulaminu organizacyjnego KW PSP w Gorzowie Wlkp. stanowiącego załącznik do decyzji nr 5/2018 Lubuskiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej w Gorzowie Wlkp. z dnia 27 listopada 2018 r. do wspólnych zadań wszystkich komórek organizacyjnych Komendy Wojewódzkiej należy w szczególności opracowywanie materiałów do udostępniania jako informacji publicznej.

W toku kontroli ustalono, iż w latach 2017 i 2018 do jednostki wpłynęło 8 wniosków o udostępnienie informacji publicznej. Kontrolą objęto wszystkie wnioski.

Podczas wykonywania czynności kontrolnych ustalono, że jednostka była właściwa do załatwienia wszystkich skontrolowanych wniosków. Kontrolujący stwierdzili, iż wszystkie wnioski o udostępnienie informacji publicznej zostały załatwione prawidłowo.

W trakcie kontroli poddano również analizie informacje zamieszczane na stronie Biuletynu Informacji Publicznej Komendy Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wlkp. BIP jednostki kontrolowanej w dniu kontroli spełniała wszystkie wymogi ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Sposób i zakres udostępniania informacji w BIP, w tym terminy publikacji danych, uprawniają do wydania pozytywnej oceny, a działania zmierzające do wyjścia naprzeciw potrzebom klientów przez publikację w BIP dodatkowych, przydatnych informacji są dobrą praktyką.

Dokonywanie zamówień publicznych.

KW PSP jako jednostka sektora finansów publicznych zobowiązana jest przy udzielaniu zamówień publicznych do stosowania przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U.2015.2164). Oceniono zgodność udzielania zamówień publicznych (dostaw) podmiotom zewnętrznym, z przepisami prawa powszechnie obowiązującego i regulacjami wewnętrznymi. W okresie objętym kontrolą przeprowadzono 13 postępowań z zastosowaniem przepisów ustawy Prawo zamówień publicznych, w trybie przetargu nieograniczonego, z czego kontrolą objęto 8, na dostawę:

- kontenerów do transportu środka pianotwórczego, gdzie wartość zamówienia wynosiła 2546100,00 zł;
- spektrometrów, gdzie wartość zamówienia wyniosła 230000,00 zł;
- średniego samochodu ratowniczo-gaśniczego, gdzie wartość zamówienia wyniosła 898884,00 zł;
- średniego samochodu ratowniczo-gaśniczego, gdzie wartość zamówienia wyniosła 888921,00 zł;
- namiotów pneumatycznych, gdzie wartość zamówienia wyniosła 300000,00 zł;
- zestawów do prania i konserwacji ubrań specjalnych, gdzie wartość zamówienia wyniosła 280440,00 zł;
- ubrań specjalnych 146 kompletów, gdzie wartość zamówienia wyniosła 475887,00 zł;
- urządzeń sieciowych, gdzie wartość zamówienia wyniosła 271986,00 zł.

Po analizie przedłożonej dokumentacji kontrolujący nie stwierdzili żadnych nieprawidłowości w zakresie przeprowadzenia postepowania jak i wyborze najkorzystniejszej oferty.

Badaniem objęto również przeprowadzone postępowania o udzielanie zamówień publicznych o wartości nieprzekraczającej równowartości kwoty 30 000 euro. LKW PSP nie wprowadził do stosowania zarządzenia wewnętrznego w sprawie jednolitej procedury wydatkowania środków finansowych w zakresie udzielania przez zamówień publicznych o wartości nieprzekraczającej równowartości kwoty 30 000 euro.
W okresie objętym kontrolą przeprowadzono 54 postępowania w zakresie kwot od 10 000,00 zł do 30 000 euro. Prawidłowość udzielania przez jednostkę tych zamówień oceniono w oparciu o 26 przeprowadzonych postępowań. Wydatki publiczne w badanym okresie pokrywały zakup m.in. samochodu osobowego, telefonów komórkowych, mebli, opon, tarczy pirotechnicznej, zestawu do symulacji skażeń, zestawów do dekontaminacji, sprzętu komputerowego, urządzeń klimatyzacji.
Badanie spraw wykazało, że:
- w 14 przypadkach zastosowano druk zapotrzebowania na dostawy lub usługi wraz z uzasadnieniem wykonania zamówienia, opisem przedmiotu zamówienia i zatwierdzeniem przez LKW PSP tego wydatku,
- do każdego zamówienia sporządzono zapytania ofertowe i dokonano analizy otrzymanych ofert, dokonując wyboru najkorzystniejszej oferty,
- w uzasadnionych przypadkach sporządzano protokoły odbioru faktycznego dostaw lub robot budowlanych,
- faktury zawierały m.in. opis wydatku oraz były sprawdzone pod względem merytorycznym, formalnym i rachunkowym,
- w 6 przypadkach podpisano umowy z wykonawcami zamówień, które właściwie zabezpieczały interes zamawiającego.
Pomimo braku uregulowań wewnętrznych w przedmiotowym zakresie, kontrolujący nie wnosi uwag do zastosowanej procedury w realizacji ocenianych zamówień publicznych.

Zawieranie umów cywilno-prawnych.
Zawieranie umów cywilnoprawnych i prowadzenie rejestru umów w KW PSP nie zostało uregulowane w Regulaminie Organizacyjnym, jak również żadnym aktem kierownictwa wewnętrznego.
Rejestr umów o dzieło i umów zleceń prowadzi pracownik zatrudniony na stanowisku ds. kadr. W kontrolowanym okresie, tj. w 2017 r. zawarto jedną umowę zlecenia, a w 2018 r. zawarto 3 umowy o dzieło oraz jedną umowę zlecenia, którą to podpisano z pracownikiem cywilnym KW PSP. Przedmiot umowy nie pokrywał się z zakresem obowiązków zatrudnionego pracownika, a umowa była realizowana po godzinach pracy i w dni wolne od pracy. Umowy zostały podpisane przez LKW PSP. W jednostce nie zostały określone procedury postępowania dotyczące rozliczania umów cywilno-prawnych w aspekcie finansowym. Nie stwierdzono nieprawidłowości w zakresie gospodarności i celowości zawierania umów cywilnoprawnych.

Gospodarowanie mieniem ruchomym, w tym środkami transportu samochodowego.
Na podstawie Regulaminu Organizacyjnego KW PSP ustalono, że prowadzenie ewidencji mienia ruchomego, jego inwentaryzację i prowadzenie spraw związanych z rozliczeniem transportu

samochodowego oraz dbałość o środki transportu należy do zakresu działania Wydziału Kwatermistrzowsko-technicznego, w skład którego wchodzi Sekcja do spraw kwatermistrzowskich i Sekcja ds. technicznych.

Korzystanie z telefonów służbowych. W kontrolowanym okresie jednostka posiadała 21 numerów abonenta sieci komórkowej. Korzystanie przez pracowników KW PSP ze służbowych telefonów, w ramach zasady oszczędnego, celowego i efektywnego gospodarowania środkami finansowymi nie zostały określone w żadnym akcie kierownictwa wewnętrznego, a jedynie przyjęto dobrą praktykę rozliczania kwot przekraczających ustalony abonament dla danego nr telefonu. Pracowników Komendy zobowiązano do wykonywania połączeń bezpłatnych ujętych w abonamencie miesięcznym w celu załatwiania spraw związanych z wykonywaną pracą. Natomiast w przypadku przekroczenia opłacanego abonamentu, pracownikom potrąca się z poborów całość kwoty przekroczenia. Co miesiąc sporządzano następujący dokument: „Obciążenia za rozmowy prywatne przeprowadzone ze służbowych telefonów komórkowych pracowników cywilnych powyżej przyznanych limitów na kwoty:…". Zestawienie zawiera następujące dane: imię i nazwisko; nr telefonu; abonament w kwocie 40 zł; dopłata do abonamentu; połączenia sms i inne; razem: netto, vat, do zapłaty brutto; treść: „Wyrażam zgodę na potrącenie poniższej należności z mojego wynagrodzenia"; podpis.
Łącznie wystawiono 5 not obciążeń na kwotę 202,75 zł. Ustalono również, że w 8 przypadkach nie potrącono pracownikom należności za przekroczenie abonamentu na łączną kwotę 665,17 zł. Jak wynika ze złożonych wyjaśnień, osoby, którym nie dokonano potrąceń wykorzystały płatny transfer danych na telefonie służbowym oraz połączenia głosowe do wykonywania zadań służbowych.

Ewidencjonowanie środków trwałych. W KW PSP nie funkcjonują uregulowania dotyczące przekazywania pracownikom w użytkowanie środków trwałych. Wszystkie nabywane środki trwałe są ewidencjonowane, a kartoteki środków trwałych są przypisane konkretnym użytkownikom tych środków. W kartotekach środków trwałych wykazano m.in. defibrylatory, ekrany projekcyjne, dalmierz laserowy, radiotelefony z akumulatorami, notebooki, telefony komórkowe, dyski zewnętrzne, dron, baterie i ładowarki do drona oraz zestawy do programowania. Zakres zadań, uprawnień i odpowiedzialności pracowników KW PSP obwarowany jest obowiązkiem dbania o powierzony sprzęt i mienie, za które pracownik jest odpowiedzialny materialnie.

Likwidacja składników majątku KW PSP odbywa się w oparciu i na zasadach określonych w zarządzeniu nr 24/2017 LKW PSP z dnia 20 marca 2017 r. w sprawie: oceny, wybrakowania i likwidacji składników majątku w KW PSP w Gorzowie Wlkp. W okresie objętym kontrolą przeprowadzono dwie takie likwidacje, po jednej w każdym roku. Przedłożona do kontroli dokumentacja zawierała:
- wniosek o likwidację, kasację wybrakowanych lub zużytych składników majątku trwałego,
- Protokół wybrakowania, który został przedstawiony do zatwierdzenia LKW PSP,

- Protokół oceny stanu składników majątku KW PSP,
- Protokół fizycznej likwidacji składników majątku KW PSP,
- Karta przekazania odpadów do zakładu utylizacji,
- Karta likwidacji środka trwałego/nietrwałego.

Kontrolujący nie wnosi uwag do kontrolowanego zakresu.

Wykorzystanie samochodów służbowych. W celu zapewnienia prowadzenia właściwej gospodarki transportowej oraz organizacji funkcjonowania Krajowego Systemu Ratowniczo – Gaśniczego na terenie Województwa Lubuskiego wydano do stosowania zarządzenie wewnętrzne nr 49/08 LKW PSP w Gorzowie Wlkp. z dnia 13 sierpnia 2008 r. w sprawie wykorzystania pojazdów służbowych PSP oraz zasad obowiązujących przy wyjazdach tymi pojazdami poza teren działania. Zarządzenie wprowadza obowiązek prowadzenia ewidencji i wydawania zezwoleń na wyjazd pojazdami w celach administracyjno-gospodarczych realizowanych na terenie działania Komendy. Wprowadzono również obowiązek prowadzenia ewidencji wyjazdów poza teren województwa lub poza granice Rzeczypospolitej Polskiej.
W okresie objętym kontrolą pozostających w ewidencji i użytkowanych było 11 pojazdów osobowych, w tym 6 pojazdów operacyjnych, 2 pojazdy rozpoznawczo ratownicze oraz 3 pojazdy do przewozu osób. Kontrolą objęto łącznie 4 pojazdy, tj. dwie Skody Octavie o nr rejestracyjnych FG 5112H, FG 4444E, Isuzu D-Max nr rej. FG 0927J, Mercedes Vito o nr rej. FG 68112.
Wszystkie ww. ewidencje wyjazdów pojazdów służbowych prowadzone są w jednym programie komputerowym pn. „System wspomagania decyzji – ST3" opracowanym przez firmę Abakus Systemy Teleinformatyczne.
Dla każdego pojazdu zakładane są „Okresowe karty pracy pojazdu", obejmujące miesięczny cykl rozliczeniowy. Sprawdzono przestrzeganie obowiązku prowadzenia ewidencji i wydawania zezwoleń na wyjazd pojazdami w celach administracyjno-gospodarczych. Kontrolującym okazano zezwolenia za miesiąc listopad i grudzień roku 2017 oraz za okres od stycznia do listopada 2018 r. Zastępca Naczelnika Wydziału Kwatermistrzowsko-technicznego wyjaśnił, że nie posiada pełnego udokumentowania wydanych zezwoleń z okresu objętego kontrolą, tj. za lata 2017-2018, ponieważ część tej dokumentacji została zarchiwizowana poprzez fizyczne zniszczenie, a żaden akt kierownictwa wewnętrznego nie określa jak długo przedmiotowe zezwolenia powinny być przechowywane w jednostce oraz co należałoby z nimi zrobić po upływie wyznaczonego okresu przechowywania.

Ochrona danych osobowych, w tym przygotowanie do wdrożenia rozporządzenia Unii Europejskiej o ochronie danych osobowych.

Kontrola obejmowała analizę dokumentacji systemu ochrony danych osobowych. Komendant Wojewódzki Państwowej Straży Pożarnej w Gorzowie Wielkopolskim wprowadził w Komendzie „Politykę ochrony danych osobowych" (Zarządzenie nr 50/2018 z dnia 25 maja 2018 r. w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych). Dokumentacja zawiera m. in. określenie zakresu

stosowania Polityki Ochrony Danych Osobowych, zasady zarządzania przetwarzaniem danych osobowych, zasady polecania przetwarzania danych, zasady przetwarzania zgodnego z prawem, tryb realizacji obowiązku informacyjnego, zasady realizacji praw osoby, której dane dotyczą, wskazuje obszary przetwarzania, zasady przetwarzania danych w systemach informatycznych i na nośnikach papierowych, zasady postępowania w sytuacji naruszenia ochrony danych osobowych, zasady monitorowania przestrzegania RODO, metodę oceny ryzyka naruszenia praw lub wolności osób fizycznych.

W Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wielkopolskim prowadzony jest rejestr czynności przetwarzania oraz rejestr kategorii przetwarzania. Przedstawiony rejestr czynności przetwarzania zawiera 67 pozycji, dla których sformułowano cele przetwarzania, opis kategorii danych, opis kategorii osób oraz opis kategorii odbiorców, którym dane zostały lub zostaną ujawnione, wskazano metodę umożliwiającą ustalenie terminu usunięcia danych oraz zamieszczono ogólny opis techniczny i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE). Rejestr kategorii przetwarzania zawierał 3 pozycje.

Załącznik numer 5 do Polityki ochrony danych osobowych stanowi Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Instrukcja zawiera m.in. metody i środki uwierzytelniające oraz procedury związane z ich zarządzeniem użytkowaniem, procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, procedurę wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Załącznik numer 16 do Polityki ochrony danych osobowych stanowi instrukcja postępowania w sytuacjach naruszenia. Załącznik nr 17 do Polityki ochrony danych osobowych stanowi Plan działań związanych z monitoringiem przestrzegania przepisów w zakresie ochrony danych osobowych.

Komendant Wojewódzki Państwowej Straży Pożarnej w Gorzowie Wielkopolskim wyznaczył Inspektora Ochrony Danych Osobowych (Zarządzenie nr 49/2018 z dnia 25 maja 2018 r. w sprawie wyznaczania Inspektora Ochrony Danych Osobowych) oraz wyznaczył specjalistę ochrony danych w Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wielkopolskim.

Ponadto w KW PSP w Gorzowie Wielkopolskim przeprowadzono ocenę skutków przetwarzania dla ochrony danych w związku z monitoringiem wizyjnym oraz wdrożono Regulamin monitoringu wizyjnego w pojazdach oraz obiektach Komendy Wojewódzkiej Państwowej Straży Pożarnej w Gorzowie Wielkopolskim (załącznik nr 1 do Decyzji nr 1/2019 Lubuskiego Komendanta Wojewódzkiego PSP z 24 kwietnia 2019 r.).

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

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

Usługi elektroniczne. Zgodnie z § Art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne: Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.

§ 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: Interoperacyjność na poziomie organizacyjnym osiągana 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.

Komenda Wojewódzka PSP nie publikuje usług elektronicznych z uwagi na charakter działalności jednostki. Na platformę ePUAP wystawiona jest jedna usługa elektroniczna – „Pismo ogólne do Urzędu".

Centralne repozytorium wzorów dokumentów elektronicznych. Zgodnie z 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.

W trakcie kontroli ustalono, że komenda nie przekazywała wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów ePUAP.

Model usługowy. Zgodnie z § 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.

Z uwagi na charakter prowadzonej działalności jednostka nie posiada wdrożonego modelu usługowego. Elektroniczne załatwienie sprawy kończy się na etapie urzędu, gdzie dokumenty są drukowane i podlegają papierowemu obiegowi wewnątrz instytucji.

Współpraca systemów teleinformatycznych z innymi systemami. Zgodnie z § 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.
Zgodnie z § 16 ust. 1 rozporządzenia: Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się składniki sprzętowe łub 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.
Interoperacyjność systemów jest zachowana dla głównego systemu informatycznego SWD.

Obieg dokumentów w KWPSP. Zgodnie z § 20 ust. 2 pkt 9 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest szczególność przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizacją i egzekwowanie, min. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
W jednostce w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do Urzędu 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. W Komendzie obowiązuje tradycyjny („papierowy") system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania spraw w KWPSP.

Formaty danych udostępniane przez systemy teleinformatyczne. Zgodnie z § 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 normą ISO/1EC 10646 wraz ze zmianami lub normę ją zastępującą.
Zgodnie z § 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.
Zgodnie z § 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.
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.

System zarządzania bezpieczeństwem informacji w systemach informatycznych.

Dokumenty z zakresu bezpieczeństwa informacji. Zgodnie z § 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.

Zgodnie z § 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.

Zarządzenie nr 50/2018 Lubuskiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej w Gorzowie Wielkopolskim z dnia 25 maja 2018r. w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych.

Polityka bezpieczeństwa informacji odnosi się w głównej mierze do zakresu danych osobowych, a nie do wszystkich informacji przetwarzanych w komendzie.

Analiza zagrożeń związanych z przetwarzaniem informacji. Zgodnie z § 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.

W maju 2018 roku przeprowadzono analizę ryzyka systemu informatycznego. Wszystkie ryzyka zostały sprowadzone do poziomu akceptowalnego, więc nie było potrzeby konstruowania planów postępowania z ryzykiem. Komenda przedstawiła metodykę analizy ryzyka.

Inwentaryzacja sprzętu i oprogramowania informatycznego. Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia 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.

Inwentaryzacja zasobów informatycznych przeprowadzona jest w systemie NOD.

Zarządzanie uprawnieniami. Zgodnie z § 20 ust. 2 pkt 4 rozporządzenia: 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: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez min. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób o których mowa w pkt 4.
Wniosek o nadanie uprawnień wpływa drogą mailową od przełożonego do Administratora Bezpieczeństwa Systemów (ABS) i Specjalisty Ochrony Danych (SOD). SOD przygotowuje upoważnienie i przeprowadza szkolenie pracownika. Po podpisaniu dokumentów przez Lubuskiego Komendanta Wojewódzkiego ABS nadaje uprawnienia. Odbieranie uprawnień przeprowadzane jest na postawie karty obiegowej. Brakuje spisu uprawnień dla pracowników.

Szkolenia pracowników zaangażowanych w proces przetwarzania informacji. Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia: 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.
Szkolenia z zakresu bezpieczeństwa ochrony danych osobowych przeprowadza Specjalista Ochrony Danych. Szkolenie stanowiskowe prowadzone jest przez pracowników Wydziału Informatyki i Łączności. Brakuje potwierdzeń prowadzenia takich szkoleń w dokumentacji.

Praca na odległość i mobilne przetwarzanie danych. Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
Urządzenia mobilne nie są szyfrowane, a wyniesienie urządzeń poza komendę jest możliwe za zgodą Lubuskiego Komendanta Wojewódzkiego.

Serwis sprzętu informatycznego i oprogramowania. Zgodnie z § 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.
Komenda Wojewódzka posiada umowy outsourcingowe dotyczące opieki nad oprogramowaniem. Sprawdzone umowy posiadały klauzule powierzenia przetwarzania danych osobowych.

Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji. Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
Stwierdzono, że brakuje rejestru incydentów. Jedynie odnotowywane są naruszenia ochrony danych osobowych (jeden wpis).
Zarządzanie incydentami jest bardzo ważnym aspektem systemu zarządzania bezpieczeństwem informacji. Jest to podstawowe narzędzie przy badaniu podatności systemów informatycznych. Brak zarejestrowanych incydentów świadczy o braku monitorowania systemów w kontekście występowania incydentów, a także o niewystarczającej wiedzy pracowników na temat definicji i sposobu zgłaszania incydentu. Nieprawidłowe zarządzanie incydentami narusza zapisy § 20 ust. 2 pkt 13 rozporządzenia.

Audyt wewnętrzny w zakresie bezpieczeństwa informacji. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej jednak, niż raz na rok.
Nie przeprowadzono audytów wewnętrznych z zakresu bezpieczeństwa informacji.

Kopie zapasowe. Zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. minimalizowanie ryzyka utraty informacji w wyniku awarii.
Kopie wykonywane są ręcznie raz w tygodniu. Brakuje jednak szczegółowej procedury wykonywania i testowania kopii zapasowych. Kopie systemów informatycznych tworzone są na urządzeniu QNAP. Jest on umieszczony w tej samej lokalizacji co dane produkcyjne. Brakuje także, potwierdzenia przeprowadzania testowego odtwarzania kopii zapasowych. Niewłaściwe sporządzanie kopii zapasowych stanowi naruszenie zapisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI.

Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych. Zgodnie z § 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.
Komenda Wojewódzka nie posiada żadnych formalnych regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych, co stanowi naruszenie § 15 ust. 1 rozporządzenia KRI.
Zabezpieczenia techniczno-organizacyjne informacji. Zgodnie z § 20 ust. 2 rozporządzenia: 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 środków przetwarzania informacji, w tym urządzeń mobilnych.
W Komendzie Wojewódzkiej istnieją zabezpieczenia fizyczne minimalizujące wystąpienie ryzyka kradzieży informacji i środków przetwarzania informacji. Dostęp do pomieszczenia serwerowni jest ograniczony do wyznaczonych osób. Przebywanie osób nieuprawnionych jest ograniczone i odnotowywane w rejestrze wejść i wyjść. Użytkownicy pracują w domenie posiadając swoje loginy i hasła.

Zabezpieczenia techniczno-organizacyjne systemów informatycznych. Zgodnie z § 20 ust. 2 pkt 12 rozporządzenia**:** 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.
Zgodnie z § 20 ust. 4 rozporządzenia: 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.
Na komputerach jest zainstalowane oprogramowanie antywirusowe. Systemy operacyjne posiadają bieżące aktualizacje systemowe. Dostęp do systemów jest zabezpieczony loginem i hasłem. Brakuje planów zabezpieczenia ciągłości działania. Jedynie stanowisko w sekretariacie nie posiada poświadczeń imiennych, a jedynie stanowiskowe. Nie zapewnia to pełnej rozliczalności pracy na tym stanowisku.
Rozliczalność działań w systemach informatycznych. Zgodnie z § 21 ust 2 rozporządzenia: IV 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.

Zgodnie z § 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.

Zgodnie z § 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.

Wszystkie systemy informatyczne stosowane w Komendzie Wojewódzkiej posiadają logi systemowe. Nie są one jednak nigdzie kopiowane i niektóre mogą ulegać nadpisaniu.

Zapewnienie dostępności informacji zawartych na stronach internetowych dla osób niepełnosprawnych.

Zgodnie z § 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.

W toku kontroli dokonano weryfikacji zgodności strony internetowej Komendy Wojewódzkiej oraz BIP standardem WCAG 2.0 poprzez wykorzystanie narzędzi dostępnych na stronie internetowej https://validator.w3.org. W przypadku strony Komendy walidacja wykazała 11 błędów i 46 ostrzeżeń. Strona BIP zawierała 3 błędy niezgodności ze standardem WCAG 2.0 i 35 ostrzeżeń. Obie strony zawierają elementy ułatwiające pracę osobom niepełnosprawnym w postaci zmiany wielkości czcionki i zmiany kontrastu. Rozwiązanie wymaga dopracowania.

Przedstawiając powyższe ustalenia, **zalecam**:

1. wdrożenie wewnętrznej procedury ustalania Indywidualnego Programu Rozwoju Zawodowego i przy kolejnych procesach ocen okresowych ustalenie indywidulanie programu rozwoju zawodowego pracownikom Komendy;

2. stworzenie programu zarządzania zasobami ludzkimi dla pracowników służby cywilnej zatrudnionych w Komendzie Wojewódzkiej PSP w Gorzowie Wlkp.;
3. rozszerzenie zakresu dokumentacji bezpieczeństwa ochrony danych osobowych o tematykę bezpieczeństwa informacji, w tym stworzenie systemu zarządzania bezpieczeństwem informacji;
4. wykonywania audytów wewnętrznych z zakresu bezpieczeństwa informacji;
5. prowadzenie rejestru incydentów;
6. opracowanie procedur zgłaszania incydentów oraz przeszkolenie pracowników w tym zakresie;
7. stworzenie procedury wykonywania kopii zapasowych, w tym poprawienie dotychczasowego rozwiązania wykonywania kopii zapasowych;
8. testowanie i dokumentowanie okresowego odtwarzania danych i opracowanie planów zapewnienia ciągłości działania;
9. wdrożenie rozwiązania teleinformatycznego zapewniającego możliwość przechowywania logów systemowych przez okres minimum 2 lat;
10. wdrożenie regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych;
11. zapewnienie zgodności ze standardem WCAG 2.0 strony internetowej Komendy Wojewódzkiej PSP jak również strony BIP Komendy;
12. wprowadzenie takich regulacji, które zapewnią cykliczność szkoleń z zakresu bezpieczeństwa informacji;
13. dokonanie działań zarządczych, które zapewnią szyfrowanie urządzeń mobilnych pracujących poza siedzibą Komendy;
14. wprowadzenie takich regulacji zarządczych, które określą zasady archiwizacji zezwoleń na wyjazd pojazdami w celach administracyjno-gospodarczych;
15. prowadzenia bieżącej, wnikliwej analizy sposobu realizacji kontrolowanych zadań w celu uniknięcia podobnych nieprawidłowości w przyszłości.

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.

wz. WOJEWODY LUBUSKIEGO

Wojciech Perczak
Wicewojewoda Lubuski