WOJEWODA LUBUSKI

Władysław Dajczak

Gorzów Wlkp., 30 maja 2019 r.

NK-II.431.1.8.2018.HKam

Pan
Jacek Wójcicki
Prezydent Miasta
Gorzowa Wielkopolskiego

Wystąpienie pokontrolne

z kontroli przeprowadzonej w trybie zwykłym w Urzędzie Miasta w Gorzowie Wlkp.

Na podstawie art. 28 ust.1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz.U.2017.2234 ze zm.), art. 2 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U.2011.185.1092) pracownicy Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp.:

- Hanna Kamińska – starszy inspektor wojewódzki w Wydziale Nadzoru i Kontroli – przewodnicząca zespołu,
- Robert Burek – starszy inspektor wojewódzki w Wydziale Nadzoru i Kontroli,
- Michał Piaskowski – kierownik Oddziału Informatyki w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych,
- Izabela Milczarek – informatyk ds. administrowania systemami informatycznymi w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych,

w dniach od 15 listopada 2018r. do 28 lutego 2019 r. stosownie do pisemnych upoważnień nr: 262-1/2018, 262-2/2018, 262-3/2018, 262-4/2018r. z dnia 7 listopada 2018 r. przeprowadzili kontrolę problemową w trybie zwykłym w Urzędzie Miasta w Gorzowie Wlkp.

Kontrola została odnotowana w książce kontroli.

Przedmiotem kontroli było sprawdzenie prawidłowości wykonywania zadań z zakresu administracji rządowej realizowanych na podstawie ustawy o dowodach osobistych, ewidencji ludności oraz działanie systemów teleinformatycznych oraz rejestrów publicznych.

Kontrolą objęto okres od 1 stycznia 2018 r. do 30 czerwca 2018 r., natomiast w zakresie działania systemów teleinformatycznych oraz rejestrów publicznych - stan obecny.

Wykonywanie zadań z zakresu administracji rządowej realizowanych na podstawie ustawy o dowodach osobistych i ewidencji ludności oceniono pozytywnie z uchybieniami, natomiast w obszarze bezpieczeństwa informacji – pozytywnie z nieprawidłowościami.

Do otrzymanego dnia 26 kwietnia br. projektu wystąpienia pokontrolnego zastrzeżenia nie zostały wniesione. Wobec powyższego stosownie do art. 47 ustawy o kontroli w administracji rządowej przekazuję Panu niniejsze wystąpienie pokontrolne.

W wyniku przeprowadzonej kontroli dokonano następujących ustaleń:

Prezydentem Miasta Gorzowa Wielkopolskiego jest Pan Jacek Wójcicki od dnia 16 listopada 2014 r.

Wykonywanie zadań z zakresu administracji rządowej realizowanych na podstawie ustawy o dowodach osobistych, ewidencji ludności

Jak wynika z Regulaminu Organizacyjnego Urzędu Miasta Gorzowa Wlkp. wprowadzonego zarządzeniem Nr 101/WI/2017 Prezydenta Miasta Gorzowa Wlkp. z dnia 29 maja 2017 r. zadania z zakresu ustaw o dowodach osobistych oraz ewidencji ludności przypisane są do Wydziału Spraw Obywatelskich. Wydziałem kieruje Dyrektor Pani Sylwia Bagińska, a funkcję kierownika Referatu Ewidencji Ludności i Dowodów Osobistych pełni Pan Adam Stańczuk. Ww. posiadają upoważnienia Prezydenta Miasta do wydawania decyzji administracyjnych zakresu ewidencji ludności i dowodów osobistych.

Od dnia 1 marca 2015 r. zadania z zakresu wydawania dowodów osobistych oraz ewidencji ludności realizowane są przy pomocy jednej wspólnej dla wszystkich gmin w Polsce aplikacji Źródło. Pracownicy urzędu wykonujący ww. zadania posiadają karty dostępowe do przetwarzania danych osobowych zgromadzonych w rejestrze PESEL, Rejestrze Dowodów Osobistych oraz w systemach teleinformatycznych, w których prowadzone są rejestry.

1. **Dowody osobiste.**

Kontrolą objęto wydawanie, wymianę i unieważnianie dowodów osobistych, zasady prowadzenia Rejestru Dowodów Osobistych oraz zasady postępowania z dokumentacją związaną z dowodami osobistymi.

W kontrolowanym okresie wydano 8442 dowody osobiste. Skontrolowano 136 kopert dowodowych. Dokumentację przechowywano w prawidłowo oznaczonych kopertach dowodowych. Wnioski o wydanie dowodu osobistego oraz formularze zgłoszenia utraty lub uszkodzenia dowodu osobistego składane były bezpośrednio u prowadzącego sprawę pracownika, który ustalał tożsamość osoby ubiegającej się o wydanie dowodu osobistego, weryfikował wniosek w oparciu o posiadane dokumenty i rejestry, a następnie wprowadzał dane do Rejestru Dowodów Osobistych. W okresie objętym kontrolą zgłoszono utratę 950 dowodów osobistych, z których skontrolowano 122 zgłoszenia. Wszystkie skontrolowane wnioski złożono na właściwych formularzach i zostały prawidłowo wypełnione.

Do urzędu wpłynęło 267 wniosków o wydanie dowodu osobistego za pomocą platformy e-PUAP. Wnioskodawca otrzymywał potwierdzenie złożenia wniosku o wydanie dowodu osobistego z wydrukowaną przewidywaną datą odbioru oraz zaświadczenie o utracie lub uszkodzeniu dowodu osobistego ważne do czasu wydania nowego dowodu osobistego, nie dłużej jednak niż przez 2 miesiące.

Dowody osobiste wydawane były nie później niż w terminie 30 dni od dnia złożenia wniosku. Odbiór dowodu osobistego był każdorazowo potwierdzany na formularzu odbioru dowodu osobistego, lecz stwierdzono pojedyncze przypadki braku formularza odbioru. Zgodnie z wyjaśnieniami kierownika referatu, wynika to z reorganizacji pracy wydziału w okresie objętym kontrolą, tj. miejsca obsługi interesanta i miejsca przechowywania kopert dowodowych. W trakcie trwania kontroli formularze dołączono do właściwych kopert.

Po wprowadzeniu z formularza do Rejestru Dowodów Osobistych daty odbioru przez wnioskodawcę dowodu osobistego dane przekazywane były do rejestru PESEL. Osoba, która odbierała nowy dowód osobisty przedkładała dotychczasowy. W przypadku wyrażenia woli zachowania dokumentu, dokument unieważniano w systemie i po fizycznym uszkodzeniu przekazywano właścicielowi.

W imieniu osoby nieposiadającej zdolności do czynności prawnych lub posiadającej ograniczoną zdolność do czynności prawnych ubiegającej się o wydanie dowodu osobistego wniosek składał rodzic, opiekun prawny lub kurator.

W okresie objętym kontrolą unieważniono 989 dowodów osobistych. Powodami unieważnienia były:

- zgony - 703,
- zmiana danych – 155,
- zmiany wizerunku twarzy – 64,
- odnalezienie dowodu osobistego przez osoby trzecie – 33,
- reklamacje – 8,
- inne – 26.

W przypadku unieważniania utraconych dowodów, zgłaszanych przez właścicieli, jako datę unieważnienia utraconych dowodów rejestrowano datę zgłoszenia do organu utraty dowodu.

Nie stwierdzono przypadków wydania decyzji administracyjnej w sprawie odmowy wydania dowodu osobistego.

2. Ewidencja ludności.

Kontrolując realizację zadań z zakresu ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz.U.2017.657 ze zm., Dz.U.2018.1382 ze zm.) sprawdzano prawidłowość i terminowość wykonywania obowiązku meldunkowego przez obywateli polskich i cudzoziemców. Rejestr mieszkańców jest prowadzony w programie ASTER wersja 32.19, której administratorem jest firma Mistar z Gorzowa Wielkopolskiego. Zgodnie z wyjaśnieniami złożonymi przez Kierownika Referatu Ewidencji Ludności i Dowodów Osobistych, ww. firma dokonuje codziennie aktualizacji (transportu danych) z systemu Źródło do rejestru mieszkańców.

W okresie objętym kontrolą dokonano łącznie 5264 zameldowań, wymeldowań, zgłoszeń wyjazdu na pobyt czasowy i stały oraz zgłoszeń powrotu z pobytu czasowego poza granicami RP. Skontrolowano 135 zgłoszeń. Zgłoszenia składane były bezpośrednio u prowadzącego sprawę pracownika, który ustalał tożsamość wnioskodawcy, weryfikował zgłoszenie w oparciu o posiadane dokumenty i rejestry, a następnie wprowadzał dane do rejestru.

Zgłaszanie i przyjmowanie danych do zameldowania i wymeldowania odbywało się zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych z dnia 13 grudnia 2017 r. w sprawie określenia wzorów i sposobu wypełniania formularzy stosowanych przy wykonywaniu obowiązku meldunkowego (Dz.U.2017.2411). Formularze zgłoszeń w zdecydowanej większości przypadków są wypełniane pismem odręcznym przez osobę dokonującą zgłoszenia.

W pojedynczych przypadkach formularze zgłoszeń meldunkowych są drukowane przez pracownika, w obecności osoby dokonującej zgłoszenia, na podstawie danych zawartych

w rejestrze PESEL oraz podanych przez tę osobę. Czynność zameldowania następuje po wykazaniu, przez osobę meldującą się, wymaganych danych w tym dot. potwierdzenia faktu pobytu osoby pod zgłaszanym do zameldowania adresem oraz po potwierdzeniu przez osobę meldującą się wiarygodności wskazanych danych. Formularze zgłoszeń opatrzone są datą przyjęcia (stanowiącą jednocześnie datę rejestracji zdarzenia) i podpisem pracownika przyjmującego zgłoszenie. W skontrolowanych formularzach stwierdzono pojedyncze przypadki nieprawidłowości i uchybień, są one jednak sporadyczne i nie mają wpływu na kontrolowaną działalność.

W przypadku meldunku niepełnoletnich dzieci zgłoszenia meldunkowego dokonywał jeden z rodziców. Dokonywane były również czynności meldunkowe przez pełnomocnika, a w przypadkach gdzie powstawał obowiązek zapłaty opłaty skarbowej była ona uiszczana w prawidłowej stawce. Stwierdzono, że okresy zameldowania cudzoziemców nie przekraczają okresu określonego dokumentem, legalizującym jego pobyt na terytorium RP.

W okresie objętym kontrolą zarejestrowane zostały 51 zgłoszenia meldunkowe dokonane drogą elektroniczną. Wymeldowania dotyczyło 16 zgłoszeń, wyjazdu za granicę 3 zgłoszenia, a 32 zgłoszenia dotyczyły zameldowania na pobyt stały. Wszystkie zgłoszenia są przechowywane w systemie teleinformatycznym kontrolowanej jednostki.
Osobom dokonującym zameldowania na pobyt stały z urzędu są wydawane zaświadczenia o zameldowaniu, natomiast osobom meldującym się na pobyt czasowy – zaświadczenia o zameldowaniu wydawane są na wniosek.

W drukach meldunkowych wszystkie rubryki wypełniano prawidłowo, a w miejscu przeznaczonym na potwierdzenie pobytu osoby w lokalu znajdował się podpis osoby posiadającej tytuł prawny do lokalu. W sprawach dotyczących zgłoszenia pobytu cudzoziemców pracownik Referatu Ewidencji Ludności i Dowodów Osobistych dokonuje adnotacji o przedstawionych przez wnioskodawcę dokumentach legalizujących jego pobyt na terenie Polski (wiza, decyzja wojewody). Na każdym zgłoszeniu widniał podpis osoby przyjmującej zgłoszenie. Dokonując zameldowania na pobyt stały wydawano z urzędu zaświadczenie o zameldowaniu.

Czynności meldunkowe wykonywano z zachowaniem zasad określonych rozporządzeniem Ministra Spraw Wewnętrznych z dnia 16 lutego 2012 r. w sprawie trybu rejestracji danych w rejestrze PESEL oraz rejestrach mieszkańców i rejestrach zamieszkania cudzoziemców (Dz.U.2015.1290), i znalazły odzwierciedlenie w rejestrze PESEL oraz w rejestrach mieszkańców.

Dokumentacja, na podstawie której pracownik referatu dokonywał zameldowania lub wymeldowania gromadzona jest w miesięcznych plikach oddzielnie dla każdego rodzaju meldunku:

– zameldowanie na pobyt stały,

– zameldowanie na pobyt czasowy,

– wymeldowania.

Skontrolowano wszystkie postępowania administracyjne w przedmiocie wymeldowania z pobytu stałego i zameldowania na pobyt stały (129). O wymeldowaniu z pobytu stałego orzeczono w 79 przypadkach, a ponadto:

– w 21 sprawach wydano decyzje umarzające postępowanie,

– w 8 przypadkach odmówiono wymeldowania,

– wydano 2 decyzje uchylające czynność materialno-techniczną,

– w 1 decyzji orzeczono o wymeldowaniu i umorzeniu,

– w 1 decyzji orzeczono o wymeldowaniu i odmowie umorzenia,

– w 4 przypadkach odmówiono wszczęcia postępowania,

– 9 spraw po zakończeniu okresu objętego kontrolą pozostawało w toku,

– wydano 4 decyzje o zameldowaniu.

Wnioski o wymeldowanie były składane przez osoby do tego upoważnione. Postępowania administracyjne były prowadzone prawidłowo, jednak w zawiadomieniach o wszczęciu postępowania, w wezwaniach oraz w zawiadomieniach, o których mowa w art. 10 k.p.a. (wysyłanych w formie jednego pisma) w nagłówku zamiast oznaczenia organu (Prezydent Miasta), wskazywano oznaczenie aparatu pomocniczego (Urząd Miasta). Zawiadomienia były podpisywane przez pracowników wydziału, a nie przez uprawnioną osobę, tj. z upoważnienia Prezydenta. Powyższe stanowi uchybienie formalne niepowodujące negatywnych następstw dla kontrolowanej działalności.

Organ prawidłowo zawiadamiał strony o wszczęciu postępowania oraz o przedłużeniu terminu, lecz nie we wszystkich przypadkach decyzje były wydane w wyznaczonym terminie. Wszystkie decyzje administracyjne posiadają prawidłowe oznaczenia, zawierają uzasadnienie faktyczne i prawne, podpisywane są przez uprawnione osoby, zawierają pouczenie o środkach odwoławczych. Pisma w sprawie oraz decyzje doręczano za zwrotnym potwierdzeniem odbioru. Pobierano opłatę skarbową w prawidłowej wysokości w przypadku postępowania wszczętego na wniosek.

3. Nadanie i zmiana numeru PESEL

W uzasadnionych przypadkach zameldowanie połączone jest z nadaniem z urzędu numeru PESEL osobie wykonującej obowiązek meldunkowy. W okresie objętym kontrolą z urzędu nadano 488 numerów PESEL. Skontrolowano 109 przypadków.

W sytuacji ubiegania się o nadanie numeru PESEL na wniosek osoby zainteresowanej (art. 18 ustawy o ewidencji ludności) każdorazowo weryfikowana jest wskazana przez wnioskodawcę podstawa prawna. Numer PESEL jest nadawany na wniosek tylko w uzasadnionych przypadkach, kiedy z przepisów odrębnych wynika konieczność jego posiadania – zarejestrowano 25 takich przypadków. Wszystkie wnioski spełniały wymogi ustawowe.

W kontrolowanym okresie nie było przypadków zmiany numeru PESEL.

4. Usunięcie niezgodności przez ewidencję ludności

Niezgodności danych ujętych w rejestrze PESEL z danymi faktycznymi, stwierdzone w wyniku otrzymania zlecenia z innej jednostki, były wyjaśnianie i usuwane bez zbędnej zwłoki. Prawidłowość danych zarejestrowanych w rejestrze PESEL sprawdzana była również z urzędu podczas pracy bieżącej jednostki w wyniku czego albo były przekazywane, zgodnie z właściwością, innym jednostkom zlecenia usunięcia niezgodności, albo też stwierdzone niezgodności zostały usunięte we własnym zakresie. Zgodnie z wyjaśnieniami Kierownika Referatu, sprawdzenie wykonania tych czynności możliwe jest jedynie w plikach systemowych. Skontrolowano 65 przypadków usunięcia niezgodności ze 123 zarejestrowanych. Wg statystyki sytemu Źródło wszystkie zlecenia z okresu objętego kontrolą posiadały status „zrealizowane". Usuwane niezgodności w zakresie meldunków dotyczyły głównie uzupełnienia kodu pocztowego w adresie zameldowania, doprecyzowania nr domu lub archiwalnych danych dot. pobytu czasowego, a więc tego rodzaju danych, których uzupełnienie w rejestrze PESEL z urzędu nie wymaga powiadamiania osób, których dane dotyczą. W przypadku zaś usuwania niezgodności z inicjatywy osoby, której dane dotyczą, osoba ta jest informowana o dokonanej weryfikacji i aktualizacji jej danych w rejestrze PESEL, lecz w okresie objętym kontrolą nie zaistniały takie sytuacje.

5. Udostępnianie danych oraz wydawanie zaświadczeń

Dokumentacja w teczkach aktowych „5345 – udostępnianie danych i wydawanie zaświadczeń z ewidencji ludności i dowodów osobistych" prowadzona była oddzielnie w podteczkach dla udostępnianej dokumentacji związanej z dowodami osobistymi

i wniosków o udostępnienie danych w trybie jednostkowym z Rejestru Dowodów Osobistych, udostępnianych danych z ewidencji ludności oraz wydawanych zaświadczeń.

W trakcie kontroli stwierdzono, iż w okresie objętym kontrolą do organu wpłynęło łącznie 147 wniosków o udostępnienie dokumentacji związanej z dowodami osobistymi jak i o udostępnienie danych w trybie jednostkowym z Rejestru Dowodów Osobistych. Wnioski były składane dwojako, część na właściwych formularzach, zgodnie z § 1 pkt 1 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 października 2011 r. w sprawie określenia wzorów wniosków o udostępnienie danych z Rejestru Dowodów Osobistych oraz dokumentacji związanej z dowodami osobistymi, a część w innej formie, napisane odręcznie, ale zawsze zawierały informacje o jakie dane wnioskowano. Wnioski, które złożono na niewłaściwych formularzach były rozpatrywane zgodnie z wytycznymi z pisma Ministerstwa Spraw Wewnętrznych i Administracji Departamentu Spraw Obywatelskich z dnia 16 lutego 2018 r. znak DSO-WUI-6174-10.19/17. Skontrolowano 14 wniosków, z czego 7 wniosków dotyczyło udostępnienia danych w trybie jednostkowym, a następne 7 udostępnienia dokumentacji związanej z dowodami osobistymi. Na powyższe wnioski udzielono odpowiedzi zgodnej z zakresem żądania wnioskodawcy i tylko w takim zakresie, w jakim wnioskodawca wykazał uprawnienia do ich otrzymania. Skontrolowano również wszystkie wnioski, które podlegały opłacie zgodnie z rozporządzeniem Rady Ministrów z dnia 21 listopada 2011 r. w sprawie opłat za udostępnienie danych z Rejestru Dowodów Osobistych i dokumentacji związanej z dowodami osobistymi (Dz.U.2016.319) i stwierdzono, że wpłacane kwoty były zgodne z określonymi stawkami.

Udostępniano również dane z rejestru mieszkańców podmiotom publicznym oraz innym osobom i jednostkom organizacyjnym, które wykazały interes faktyczny w otrzymaniu danych, pod warunkiem uzyskania zgody osób, których one dotyczyły. Wniosków o udostepnienie danych jednostkowych wpłynęło 2954, w tym 318 dotyczyło udostępnień na wnioski wpływające z własnych jednostek. Skontrolowano 131 wniosków. Dane były udostępniane prawidłowo: w formie pisemnej i dotyczyły one jednej osoby lub imion i nazwisk wszystkich osób zameldowanych pod jednym adresem.

Dnia 30 stycznia 2018 r. na prawidłowym formularzu wpłynął wniosek o udostępnienie danych wraz z opłatą. W związku z brakiem uzyskania zgody osoby, której udostepnienie dotyczyło, zgodnie z art. 46 ust. 2 pkt 3, decyzją z dnia 14 lutego 2018 r. znak WSO.III.5181.1.1.2018 organ odmówił udostępnienia danych z rejestru mieszkańców.

Ponadto do Urzędu złożono 1908 wniosków od zainteresowanych osób o wydanie zaświadczeń o zameldowaniu. Do wydania przedmiotowych zaświadczeń wykorzystywano dane zawarte w Rejestrze Mieszkańców. Skontrolowano 150 wniosków. W przypadkach gdy o zaświadczenie zwracała się osoba, której dane miały być wykorzystane do celów innych niż wynika to z ustawy z dnia 16 listopada 2006 r. o opłatach skarbowych (Dz.U.2016.1827) pobierano opłatę w wysokości 17 zł. Organ kwalifikował te zaświadczenia jako wydane na podstawie art. 45 ustawy o ewidencji ludności, jednak w żadnym z powyższych przypadków nie wydano pełnego odpisu przetwarzanych danych dotyczących tej osoby.

Ponadto organ nie wydawał na wniosek zainteresowanej osoby, złożony w formie pisemnej, zaświadczeń, na podstawie art. 63 ustawy o dowodach osobistych, dotyczących danych z rejestru dowodów osobistych zawierających pełny odpis danych, o których mowa w art. 56 pkt 1, 3, 4, 7 i 8 ww. ustawy, dotyczących tej osoby przetwarzanych przez ten organ w Rejestrze Dowodów Osobistych.

System zarządzania bezpieczeństwem informacji w systemach informatycznych.

1.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu.

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.
Zgodnie z § 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 141/W/I/2018 Prezydenta Miasta Gorzowa Wlkp. z dnia 17 lipca 2018 r. w sprawie wdrożenia do użytku „Polityki bezpieczeństwa danych osobowych

w Urzędzie Miasta Gorzowa Wlkp.”. Pracownicy zostali przeszkoleni z zakresu tego dokumentu. Nowo przyjęci pracownicy są szkoleni przez Inspektora Ochrony Danych Osobowych. Dokument skupia się wyłącznie na ochronie danych osobowych. Ochrona pozostałych, ważnych z punktu widzenia urzędu danych zostały pominięte. Stanowi to naruszenie § 20 ust. 2 pkt 1 rozporządzenia KRI.

1.2 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.

Urząd Miasta Gorzowa Wlkp. przedstawił dokument analizy ryzyka za 2018 rok. Zawiera on ocenę szeregu zagrożeń i podatności systemów informatycznych. Do tego dokumentu dołączona jest metodyka analizy ryzyka. Wszystkie ryzyka zostały oszacowane na poziomie co najwyżej średnim. W wyniku kontroli wykazane zostały zagrożenia, które powinny być szacowane w stopniu wysokim. Brakuje planu postępowania z ryzykiem oraz harmonogramu prac naprawczych.

1.3 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.

W wyniku kontroli ustalono, że inwentaryzacja zasobów informatycznych w Urzędzie prowadzona jest, w formie elektronicznej w systemie IT-Manager. Nie stwierdzono nieprawidłowości w tym zakresie.

1.4 Zarządzanie uprawnieniami.

Zgodnie z § 20 ust. 2 pkt 4 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w, stopniu adekwatnym do

realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.
Zgodnie z § 20 ust. 2 pkt 5 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, nun. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Nadawanie uprawnień przebiega zgodnie z polityką bezpieczeństwa informacji i nie budzi zastrzeżeń kontroli.

1.5 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.

Urząd Miasta Gorzowa Wlkp. przeprowadził szkolenia z zakresu bezpieczeństwa danych osobowych. Procesem szkolenia zajmuje się Inspektor Ochrony Danych Osobowych, a instruktaż stanowiskowy przeprowadzają pracownicy Wydziału Zarządzania Systemami Informatycznymi. Brakuje jedynie potwierdzenia tego instruktażu dokumentami.

1.6 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 są szyfrowane. Użytkownicy mają wyłączone porty USB. Istnieje szereg wyjątków do tej zasady, a przekazane do użytkowania urządzenia wymienne nie są ewidencjonowane. Pracownicy Wydziału Zarządzania Systemami Informatycznymi korzystają z szyfrowanych, zdalnych połączeń VPN do infrastruktury Urzędu.

1.7 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.

Urząd Miasta Gorzowa Wlkp. posiada ponad 30 umów outsourcingowych dotyczących opieki nad sprzętem i oprogramowaniem. W umowach przeważanie widnieją zapisy o powierzeniu przetwarzania danych osobowych, jednak brakuje ich w 2 przypadkach. Jest to naruszenie § 20 ust. 2 pkt 10 rozporządzenia KRI.

1.8 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 określonym i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Podczas kontroli przedstawiono dokument potwierdzający zgłoszenia incydentów naruszenia ochrony danych osobowych. Szczegółowo zostały w nim opisane sytuacje oraz podjęte działania. Brakuje wpisów dotyczących pozostałych incydentów, nie będących naruszeniem ochrony danych osobowych.

1.9 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 niż raz na rok.

W Urzędzie Miasta Gorzowa Wlkp. przeprowadzone są corocznie audyty wewnętrzne z zakresu bezpieczeństwa informacji. W sprawozdaniach końcowych z realizacji zadania audytowego znajduje się szereg szczegółowych zaleceń, zgodnych z obserwacjami z niniejszej kontroli. Podany harmonogram działań naprawczych nie jest realizowany zgodnie z terminami podanymi w załącznikach do sprawozdania.

1.10 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.

Wykonywanie kopii zapasowych reguluje polityka bezpieczeństwa informacji. Kopie zapasowe są realizowane za pomocą wydzielonych zasobów dwóch macierzy w różnych lokalizacjach, gdzie są naprzemiennie składowane. Brakuje formalnych procedur wykonywania oraz odtwarzania kopii zapasowych. Nie jest dokumentowane także testowe lub awaryjne odtwarzanie kopii zapasowych. Stanowi to naruszenie z § 20 ust. 2 pkt 12 lit. B rozporządzenia KRI.

1.11 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.

Urząd Miasta Gorzowa Wlkp. nie posiada żadnych formalnych regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych. Nieformalnie powoływane są interdyscyplinarne zespoły, które najpierw określają wymagania dla systemów, a następnie poszukują produktów spełniających wymogi.

1.12 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 Urzędzie Miasta Gorzowa Wlkp. zabezpieczenia fizyczne stanowią duży problem w bezpieczeństwie informacji. Urząd Miasta posiada wiele lokalizacji, w każdej z nich funkcjonują odrębne, nieformalne zasady zarządzania dostępem do kluczy. Istnieją lokalizacje, które nie posiadają żadnych zabezpieczeń w dostępie do pomieszczeń, a klucze są dostępne dla osób nieuprawnionych. Stanowi to duże zagrożenia w ochronie fizycznej bezpieczeństwa informacji.
Wszystkie pomieszczenia techniczne są zabezpieczone i istnieje wykaz osób uprawnionych do wejścia do tych pomieszczeń. Jednak klucze do tych pomieszczeń posiadają osoby nieuprawnione, pracujące w danej lokalizacji. Trudno stwierdzić, kto faktycznie nadzoruje dostępem do pomieszczeń technicznych, ponieważ pracownicy Wydziału Zarządzania Systemami Informatycznymi nie mają swobodnego dostępu do tych pomieszczeń. Przebywanie osób nieuprawnionych jest ograniczone i prowadzony jest rejestr wejść i wyjść. Systemy informatyczne pracują w środowiskach zwirtualizowanych, w klastrze niezawodnościowym, ale dużym problemem są stosowane rozwiązania związane z zasilaniem (brak agregatów prądotwórczych) i klimatyzacją (redundancja) pomieszczeń serwerowych. Nie ma opracowanych planów zarządzania ciągłością działania, a opisane zagrożenia nie występują w analizie ryzyka.
Brakuje aktualnych, kompleksowych projektów sieci teleinformatycznej, co w sytuacjach awaryjnych może skutkować dodatkowymi problemami z uruchomieniem systemów informatycznych Urzędu.
Opisane powyżej problemy stanowią naruszenie § 20 ust. 2 pkt 7 rozporządzenia KRI.

1.13 Zabezpieczenia techniczno-organizacyjne systemów informatycznych

§ 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. W jednostce znajdują się komputery pod kontrolą systemu operacyjnego Windows XP, dla których nie można już przeprowadzić aktualizacji producenta. Występowały przypadki, w których pozostałe systemy operacyjne nie posiadały bieżących aktualizacji systemowych. Dostęp do systemów jest zabezpieczony loginem i hasłem. Podczas kontroli ujawniono fakt pracy użytkownika na nie swoich uprawnieniach.

1.14 Rozliczalność działań w systemach informatycznych

Zgodnie z § 21 ust 2 rozporządzenia: w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:
1) systemu z uprawnieniami administracyjnymi;
2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
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 Urzędzie Miasta Gorzowa Wlkp. posiadają logi systemowe. Nie są one jednak nigdzie kopiowane i niektóre ulegają nadpisaniu, co narusza § 21 ust. 4 rozporządzenia KRI.
W wyniku przyjętych wyjaśnień i przeglądu zakresów czynności pracowników nie można jednoznacznie wskazać pracownika odpowiedzialnego za wynikłe nieprawidłowości. W związku z powyższym odpowiedzialnym za zaistniała sytuację jest kierownik jednostki.

Przedstawiając powyższe ustalenia, zalecam:

1. wzmożenie nadzoru nad kompletowaniem dokumentacji w kopertach dowodowych,
2. wzmożenie nadzoru nad rzetelnością wypełnianej dokumentacji, dotyczącej zgłoszeń meldunkowych,
3. prowadzenie postępowań administracyjnych dotyczących spraw meldunkowych, szczególnie w zakresie wszczynania postępowań, zgodnie z przepisami Kodeksu postępowania administracyjnego,
4. ujęcie w polityce bezpieczeństwa informacji zagadnień wykraczających poza ochronę danych osobowych gdyż obecne rozwiązania odnoszą się wyłącznie do danych osobowych,
5. dokonanie przeglądu sprawozdań z wcześniejszych audytów wewnętrznych pod kątem realizacji zaleceń poaudytowych,
6. prowadzenie rejestru incydentów dla zagadnień spoza ochrony danych osobowych,
7. stworzenie procedury wykonywania kopii zapasowych; testowanie i dokumentowanie okresowe odtwarzanie danych; opracowanie planów zapewnienia ciągłości działania,
8. wdrożenie rozwiązań teleinformatycznych zapewniających możliwość przechowywania logów systemowych przez okres minimum 2 lat,
9. dokonanie przeglądu umów z podmiotami zewnętrznymi pod kątem zagadnień związanych z powierzeniem przetwarzania danych osobowych,

10. wdrożenie regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych,
11. dokonanie przeglądu komputerów użytkowników pod kątem aktualizacji systemów operacyjnych,
12. aktualizację projektów sieci teleinformatycznej w Urzędzie,
13. wdrożenie procedury zabezpieczeń dostępu do pomieszczeń przetwarzających informacje, w szczególności do pomieszczeń technicznych.

W terminie do dnia **21 czerwca 2019 r**., proszę o pisemną informację o sposobie wykonania zaleceń i wykorzystaniu wniosków lub o przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

WOJEWODA LUBUSKI

Władysław Dajczak