WOJEWODA LUBUSKI

Władysław Dajczak

Gorzów Wlkp., 24 sierpnia 2018 r.

NK-II.431.1.1.2018.MWoł

Pan
**Andrzej Kamyszek**
Burmistrz Jasienia

**Wystąpienie pokontrolne**
**z kontroli przeprowadzonej w Urzędzie Miejskim w Jasieniu**

Na podstawie art. 28 ust.1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz.U.2015.525 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 Wydziału Nadzoru i Kontroli oraz Biura Obsługi Urzędu i Rozwoju Systemów Informatycznych Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp. w składzie:
- Małgorzata Wołejko – starszy inspektor wojewódzki – przewodnicząca zespołu,
- Izabela Okonek – inspektor wojewódzki,
- Michał Piaskowski – kierownik Oddziału Informatyki,
- Izabela Milczarek – informatyk ds. administrowania systemami informatycznymi

na podstawie pisemnych upoważnień do przeprowadzenia kontroli nr: 46-1/2018, 46-2/2018, 46-3/2018, 46-4/2018 z dnia 9 marca 2018 r., w dniach od 14 marca do 30 kwietnia 2018 r. przeprowadzili kontrolę problemową w trybie zwykłym w Urzędzie Miejskim w Jasieniu. Kontrola została odnotowana w książce kontroli pod pozycją nr 5/2018.

Przedmiotem kontroli było: realizacja zadań administracji rządowej wynikających z ustawy - Prawo o aktach stanu cywilnego oraz działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.

Okres objęty kontrolą, w zakresie:

1. realizacji zadań administracji rządowej wynikających z ustawy - Prawo o aktach stanu cywilnego - od 1 stycznia 2017 r. do 31 grudnia 2017 r.,
2. działania systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej – kontrola sprawdza stan obecny w obszarze objętym kontrolą.

Do 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:

Burmistrzem Jasienia od dnia 30 listopada 2014 r. jest Pan Andrzej Roman Kamyszek. Jak wynika z Regulaminu Organizacyjnego Urzędu Miejskiego w Jasieniu wprowadzonego Zarządzeniem Nr 120.2.2013 Burmistrza Jasienia z dnia 31 stycznia 2013 r. zadania z zakresu rejestracji stanu cywilnego należały do Urzędu Stanu Cywilnego. Od dnia 24 lutego 2017 r. zadania te przypisane są do Referatu Spraw Obywatelskich, Obronnych i Urzędu Stanu Cywilnego, co jest zgodne z § 27 Zarządzenia Nr 120/13/2017 Burmistrza Jasienia. Osobą odpowiedzialną za wykonywanie ww. zadań jest pani Iwona Rafalska – kierownik Referatu Spraw Obywatelskich, Obronnych i Urzędu Stanu Cywilnego.

Pracownicy urzędu wykonujący zadania z kontrolowanego obszaru posiadają upoważnienia do przetwarzania danych osobowych zgromadzonych w rejestrze PESEL, Rejestrze Dowodów Osobistych i Rejestrze Stanu Cywilnego oraz w systemach teleinformatycznych, w których prowadzone są przedmiotowe rejestry.

## 1. Akty stanu cywilnego.

W 2017 r. zarejestrowano 6 aktów urodzeń, 40 aktów małżeństwa oraz 37 aktów zgonu, oddzielnie dla każdego zdarzenia. Szczegółowym badaniem objęto wybrane losowo 51 aktów. Zgodnie z art. 2 ustawy z dnia 28 listopada 2014 r. - Prawo o aktach stanu cywilnego (Dz.U.2014.1741 ze zm.) rejestracji stanu cywilnego dokonuje się w rejestrze stanu cywilnego w formie aktów stanu cywilnego. Dokonując rejestracji za pośrednictwem systemu teleinformatycznego, dokonywano sprawdzenia danych zawartych w PESEL.

Rejestracji stanu cywilnego dokonywano zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych z dnia 9 lutego 2015 w sprawie sposobu prowadzenia rejestru stanu cywilnego oraz akt zbiorowych rejestracji stanu cywilnego (Dz.U.2016.1904) na podstawie dowodów

potwierdzających prawdziwość zgłoszonych danych zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych z dnia 29 stycznia 2015 r. w sprawie wzorów dokumentów wydawanych z zakresu rejestracji stanu cywilnego (Dz.U.2015.194 ze zm.).

Wpis wpływający na treść lub ważność aktu stanu cywilnego dołączano do aktu stanu cywilnego w formie wzmianki dodatkowej. W kontrolowanym okresie sporządzono 49 wzmianek dodatkowych. Informacje o innych aktach stanu cywilnego dotyczących tej samej osoby oraz informacje wpływające na stan cywilny tej osoby zamieszcza się przy akcie stanu cywilnego w formie przypisków. W kontrolowanym okresie zamieszczono 85 przypisków.

Akta zbiorowe zawierały wszystkie wymagane prawem dokumenty. I tak, akta zbiorowe małżeństwa zawierały pisemne zapewnienie o braku okoliczności wyłączających zawarcie małżeństwa podpisane przez osoby zamierzające zawrzeć małżeństwo oraz kierownika urzędu stanu cywilnego. Akty zawarte w sposób określony w art. 1 § 2 i 3 Kodeksu rodzinnego i opiekuńczego, sporządzane były na podstawie zaświadczenia stwierdzającego brak okoliczności wyłączających zawarcie małżeństwa oraz zaświadczenia stwierdzającego, że oświadczenia o wstąpieniu w związek małżeński zostały złożone w obecności duchownego.

W aktach zbiorowych do aktów zgonu dołączane były karty zgonu wypełnione zgodnie z rozporządzeniem Ministra Zdrowia z dnia 11 lutego 2015 r. w sprawie wzoru karty zgonu (Dz.U.2015.231) oraz protokoły zgłoszenia zgonu.

Akta zbiorowe prowadzone były oddzielenie dla każdego rodzaju aktu stanu cywilnego, oznaczano je numerem nadanym aktowi stanu cywilnego oraz datą sporządzenia aktu. W rejestrze stanu cywilnego dokonywano w formie czynności materialno – technicznej rejestracji urodzeń, zawarcia małżeństw oraz zgonów, które nastąpiły poza granicami Rzeczypospolitej Polskiej. Do wniosku dołączono wydany przez właściwy podmiot zagraniczny dokument potwierdzający to zdarzenie wraz z tłumaczeniem urzędowym na język polski. W formie transkrypcji dokonano rejestracji 5 aktów urodzenia.

Z urzędu, lub na wniosek przeniesiono do rejestru stanu cywilnego łącznie 774 akty stanu cywilnego sporządzone w księgach stanu cywilnego zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych z dnia 5 lutego 2015 w sprawie przenoszenia aktów stanu cywilnego do rejestru stanu cywilnego (Dz.U.2015.204). Przeniesienie to umożliwia uzyskanie odpisu aktu stanu cywilnego, w tym jego elektronicznej wersji w dowolnym urzędzie na terenie całego kraju. Kontroli poddano 464 zdarzenia, w których proces migracji zasadniczej części aktu i wzmianek dodatkowych odbywał się zgodnie z prawem.

Wydano 817 odpisów aktów stanu cywilnego (skróconych, zupełnych, na drukach wielojęzycznych) z urzędu po sporządzeniu aktu oraz na wniosek. W teczkach aktowych zgodnie z JRWA „5362 – odpisy zupełne, skrócone i wielojęzyczne aktów stanu cywilnego" odnotowano 301 pozycji zarejestrowanych spraw. Szczegółowym badaniem objęto 181 spraw. Wnioski o wydanie odpisu aktu w formie odrębnie stworzonego formularza, składały osoby, których akt dotyczył, bądź osoby do tego uprawnione, ponosząc opłatę skarbową w zależności od rodzaju odpisu aktu i jego przeznaczenia.

Ponadto wydano łącznie 67 zaświadczeń, zezwoleń oraz przyjęto oświadczenia dotyczące: braku okoliczności wyłączających zawarcie małżeństwa (art. 41 kro), stwierdzających, że obywatel polski może zawrzeć małżeństwo za granicą (art. 83 pasc), o zamieszczonych lub niezamieszczonych w RSC danych dotyczących osoby (art.44 pasc), o stanie cywilnym (art.44 pasc), o nieposiadaniu księgi stanu cywilnego (art.133 pasc), w sprawie skrócenia terminu do zawarcia małżeństwa (art.76 pasc).

Wnioski o wydanie zaświadczeń i odpisów aktów z rejestru stanu cywilnego, nie były opatrywane, stosownie do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U.2011.14.67) pieczęcią wpływu, co w konsekwencji powodowało, że nie zawierały informacji o dacie ich wpływu do Urzędu. Data ta stanowi zgodnie z przepisem art. 61 § 3 k.p.a. datę wszczęcia postępowania administracyjnego i podstawę prawidłowego obliczenia terminu załatwienia sprawy.

Stwierdzone uchybienie nie miało wpływu na sposób realizacji kontrolowanych zadań, miało natomiast charakter powtarzalny.

Wykonywanie zadań administracji rządowej wynikających z ustawy - Prawo o aktach stanu cywilnego oceniono pozytywnie.

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

### 2.1. 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.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych: 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.

Urząd Miejski w Jasieniu dla wybranych usług publikuje na stronach BIP sposób załatwienia spraw. Na stronie głównej jest przekierowanie na platformę ePUAP, gdzie wystawiona jest jedna usługa elektroniczna – „Pismo ogólne do Urzędu".

### 2.2. 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 Urząd w badanym okresie do centralnego repozytorium wzorów dokumentów ePUAP nie przekazywał wzorów dokumentów elektronicznych.

### 2.3. 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.

W Urzędzie Miejskim w Jasieniu brak formalnych procedur opisujących obsługę oraz monitorowanie usług. Na stronach internetowych urzędu opublikowano jedynie karty usług z załącznikami dokumentów do pobrania. Elektroniczne załatwienie sprawy kończy się na etapie urzędu, gdzie dokumenty są drukowane i podlegają papierowemu obiegowi wewnątrz instytucji.

### 2.4. 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.

Według § 16 ust. 1 rozporządzenia: Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

Z uwagi na jednego dostawcę systemów merytorycznych w jednostce interoperacyjność systemów jest na wysokim poziomie. Jednak trwają prace nad zastąpieniem kilku modułów oprogramowaniem od innego dostawcy, co może znacząco obniżyć poziom interoperacyjności systemów informatycznych.

### 2.5. Obieg dokumentów w Urzędzie.

Zgodnie z § 20 ust. 2 pkt 9 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

W Urzędzie 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 Urzędzie obowiązuje tradycyjny („papierowy") system wykonywania czynności kancelaryjnych jako podstawowy sposób dokumentowania spraw w Urzędzie.

### 2.6. 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 normę

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.

Wg § 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.

W obszarze wymiany informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną działalność urzędu oceniono pozytywnie z uchybieniami.

## 3. System zarządzania bezpieczeństwem informacji w systemach informatycznych.

### 3.1. 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.

Dokumentem z zakresu bezpieczeństwa informacji jest Zarządzenie Nr 120/19a/2017 Burmistrza Jasienia z dnia 10 kwietnia 2017r. w sprawie wprowadzenia do użytku

służbowego polityki bezpieczeństwa informacji w Urzędzie Miejskim w Jasieniu. Do zapoznania się z powyższym zobowiązano pracowników, którzy odbyli szkolenia z tego zakresu. Dotychczas nie przeprowadzano działań związanych z przeglądem polityk i zasad, a w dokumentach istnieje wiele rozbieżności ze stanem rzeczywistym. Od momentu wdrożenia dokumentu nie podjęto zbyt wielu konkretnych działań zmierzających do dostosowania stanu faktycznego do zapisów polityki, co znajduje potwierdzenie w raporcie z audytu przeprowadzonego w grudniu 2017r. Dokumentacja, która jest zgodna z Krajowymi Ramami Interoperacyjności w znacznym stopniu odbiega od faktycznego stanu zastanego podczas kontroli. Oznacza to brak wdrożenia zapisów dokumentacji. Późniejsze działania w postaci analizy ryzyka i audytu nie przekładają się na wzrost bezpieczeństwa informacji w jednostce.

**3.2 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 Miejski w Jasieniu przedstawił dokument analizy ryzyka przeprowadzony przez Centrum Bezpieczeństwa Informatycznego z dnia 21.01.2018 r. Zawiera on ocenę szeregu zagrożeń i podatności systemów informatycznych. Do tego dokumentu dołączona jest metodologia analizy ryzyka, a także opracowany przez pracowników Urzędu plan zmniejszenia ryzyk. Jest to szczegółowy plan naprawczy połączony z harmonogramem czasowym.

**3.3 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 postaci arkusza Excel. Stwierdzono brak przypisania sprzętu informatycznego do użytkowników, a także brak szczegółowego wykazu zainstalowanego oprogramowania, co narusza § 20 ust. 2 pkt 2 rozporządzenia.

**3.4 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 m.in. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Zgodnie z polityką bezpieczeństwa i jej załącznikiem nr 7 sporządzany jest wniosek o nadanie uprawnień do przetwarzania danych osobowych. Na podstawie tego wniosku informatyk nadaje uprawnienia w systemach informatycznych. Natomiast niejasne są zasady odbierania uprawnień w systemach informatycznych i brak jest dokumentów potwierdzających ten fakt.

**3.5 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 Miejski w Jasieniu przeprowadził szkolenia z zakresu bezpieczeństwa informacji w momencie wdrożenia polityki bezpieczeństwa informacji. Szkolenie było prowadzone przez firmę zewnętrzną. Poświadczenia tego faktu są w teczkach osobowych pracowników znajdujących się w dziale kadr. Z uwagi na krótki okres czasu, który upłynął do ustanowienia polityki bezpieczeństwa, nie wiadomo czy szkolenia odbywały się cyklicznie.

**3.6 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 nie są szyfrowane i według przedstawionych informacji nie są wynoszone poza siedzibę Urzędu. Firmy zewnętrzne mają dostęp do systemów za pomocą specjalistycznych narzędzi do zdalnej pomocy (np. TeamViewer) pod nadzorem informatyka.

**3.7 Serwis sprzętu informatycznego i oprogramowania.**

Wg § 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 Miejski w Jasieniu posiada dwie umowy outsourcingowe dotyczące opieki nad oprogramowaniem. Obie firmy mają zawarte w umowie klauzule powierzenia przetwarzania danych osobowych. Dodatkowo zawarto umowę z przedstawicielem firmy Centrum Bezpieczeństwa Informatycznego dotyczącą pełnienia funkcji Administratora Bezpieczeństwa Informacji.

**3.8 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 określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Podczas kontroli pracownicy urzędu wyjaśnili, że incydenty nie występują. Rejestr incydentów nie zawiera żadnych wpisów. W wyniku działań kontrolnych ujawniono co najmniej kilka incydentów. Pracownicy nie mają zdefiniowanego pojęcia incydentu i brak procedury zachowania się w przypadku jego wystąpienia.

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 § 20 ust. 2 pkt 13 rozporządzenia.

**3.9 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.

Przed wdrożeniem polityki bezpieczeństwa przeprowadzono audyt bezpieczeństwa informacji zakończony rzetelnym raportem z audytu. Zawarte w nim informacje przedstawiają stan rzeczywisty (zgodny ze stanem zastanym podczas kontroli) oraz rekomendacje. Większość rekomendacji nie została dotychczas zrealizowana, ale została ujęta w planie zmniejszenia ryzyka.

**3.10 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. 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 § 20 ust. 2 pkt 12 lit. B rozporządzenia KRI.

**3.11 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 Miejski w Jasieniu nie posiada żadnych formalnych regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych, co stanowi naruszenie § 15 ust. 1 rozporządzenia KRI.

**3.12 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 Miejskim w Jasieniu 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, ale nie prowadzi się żadnych rejestrów wejść i wyjść.

Serwerownia jest miejscem pracy informatyka. W celu ograniczenia dostępu osób nieuprawnionych do serwerowni warto rozważyć zmianę miejsca jego pracy. Drzwi serwerowni nie spełniają wymogów bezpieczeństwa informacji ani przepisów ppoż. Brakuje elementów nadzorujących temperaturę w serwerowni. Brakuje procedur związanych z zarządzaniem nośnikami zewnętrznymi. Powszechnie używane są pendrive'y bez opcji szyfrowania. W jednostce wykonano analizę podatności systemów informatycznych w postaci testów penetracyjnych wewnętrznych i zewnętrznych. Wyniki dołączone są do raportu z audytu z 12 stycznia 2018 r

### 3.13 Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Wg § 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.

§ 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. Pozostałe systemy operacyjne posiadają bieżące aktualizacje systemowe. Dostęp do systemów jest zabezpieczony loginem i hasłem. Podczas kontroli ujawniono fakt pracy użytkownika na nie swoich uprawnieniach. Brakuje planów zabezpieczenia ciągłości działania. W szczególności nie są rozpatrywane scenariusze związane z nieobecnością służb informatycznych.

### 3.14 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 Miejskim w Jasieniu posiadają logi systemowe. Nie są one jednak nigdzie kopiowane i niektóre ulegają nadpisaniu, narusza to § 21 ust. 4 rozporządzenia KRI.

W obszarze bezpieczeństwa informacji działalność urzędu oceniono pozytywnie z nieprawidłowościami.

## 4. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów 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 Urzędu oraz BIP Urzędu ze standardem WCAG 2.0 poprzez wykorzystanie narzędzi dostępnych na stronie internetowej https://validator.w3.org. W przypadku strony urzędu walidacja wykazała 2 błędy, jednak nie miały one istotnego wpływu na prezentowanie treści dla osób

niepełnosprawnych. Strona BIP nie zawierała błędów niezgodności ze standardem WCAG 2.0. Strona BIP zawiera elementy zmiany kontrastu oraz wielkości czcionki. W przypadku strony jasien.com.pl brakuje możliwości pracy w zwiększonym kontraście. Istnieje możliwość tylko zmiany wielkości czcionki. Rozwiązanie wymaga dopracowania.

W obszarze dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych oceniono pozytywnie z uchybieniami.

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) rejestrowanie wpływającej korespondencji zgodnie z zasadami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych,
2) doprowadzenie do zgodności zapisów polityki z rozwiązaniami teleinformatycznymi w jednostce,
3) przeprowadzenie okresowej aktualizacji dokumentacji SZBI, w tym „Polityki Bezpieczeństwa Informacji" w § 20 ust. 2 pkt 1 rozporządzenia KRI,
4) wykonanie zaleceń z audytu zgodnie z raportem z 12.01.2018 r.,
5) uaktualnienie ewidencji sprzętu i oprogramowania, dokumentowanie inwentaryzacji zasobów teleinformatycznych,
6) prowadzenie rejestru incydentów, opracowanie procedury zgłaszania incydentów oraz przeszkolenie pracowników w tym zakresie,
7) stworzenie procedury i poprawienie rozwiązania wykonywania kopii zapasowych, testowanie i dokumentowanie okresowego odtwarzania danych, dostosowanie rozwiązania teleinformatycznego dla użytkowników przy wykonywaniu kopii zapasowych stacji roboczych, opracowanie planu zapewnienia ciągłości działania,
8) wdrożenie rozwiązania teleinformatycznego zapewniającego możliwość przechowywania logów systemowych przez okres minimum 2 lat,
9) wdrożenie regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych,

10) wdrożenie procedury umożliwiającej zarządzanie usługami realizowanymi przez systemy teleinformatyczne, stosowanie szczegółowych opisów usług na stronach internetowych urzędu,
11) poprawienie rozwiązań zapewniających dostępność informacji dla osób niepełnosprawnych w obrębie strony jasien.com.pl zgodnie z przepisami,
12) wdrożenie procedury zarządzania zewnętrznymi nośnikami danych.

WOJEWODA LUBUSKI

Władysław Dajczak