Gorzów Wlkp., dnia 19 grudnia 2018r.

WOJEWODA LUBUSKI

Władysław Dajczak

NK-II.431.1.5.2018RKam

Pan
Henryk Janowicz
Starosta Żagański

Wystąpienie pokontrolne
z kontroli przeprowadzonej w Starostwie Powiatowym w Żaganiu

Na podstawie art. 6 ust. 4 pkt 2 ustawy o kontroli w administracji rządowej (Dz. U. 2011.185.1092) w dniach od 27 czerwca do 31 sierpnia 2018 r. pracownicy Wydziału Nadzoru i Kontroli Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp., :

- Robert Kamiński – inspektor wojewódzki – przewodniczący zespołu,
- Mariola Żurawska – st. inspektor wojewódzki – członek zespołu,
- Michał Piaskowski – kierownik Oddziału Informatyki – członek zespołu,
- Izabela Milczarek – informatyk ds. administrowania systemami informatycznymi – członek zespołu,

stosownie do pisemnych upoważnień nr: 144-1/2018, 144-2/2018, 144-3/2018, 144-4/2018 z dnia 26 września 2018 r., przeprowadzili kontrolę problemową w Starostwie Powiatowym w Żaganiu.

Przedmiotem kontroli była ocena prawidłowości i rzetelności wykonywanych zadań z zakresu administracji rządowej realizowanych na podstawie ustawy o odpadach w okresie od 1 stycznia 2016 r. do 26 czerwca 2018 r. oraz działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej - stan obecny w obszarze objętym kontrolą.

Do otrzymanego projektu wystąpienia pokontrolnego pismem z dnia 15 listopada 2018 r. znak: S.1710.13.2018 złożył Pan zastrzeżenia. Po ich rozpatrzeniu, pismem znak: NK-II.431.1.5.2018RKam z dnia 6 grudnia 2018 r. został Pan poinformowany o uwzględnieniu zastrzeżeń dotyczących zawiadamiania stosownie do art. 61§ 4 k.p.a. właścicieli nieruchomości o wszczęciu postępowań administracyjnych i oddaleniu pozostałych zastrzeżeń.

W związku z powyższym stosownie do art. 47 ustawy o kontroli w administracji rządowej przekazuję niniejsze wystąpienie pokontrolne.

Ustalenia kontroli.

Starostą Żagańskim jest pan Henryk Andrzej Janowicz wybrany na tę funkcję przez Radę Powiatu Żagańskiego w dniu 1 grudnia 2014 r. Wicestarostą jest pan Marek Kopta.

1. **Ocena prawidłowości i rzetelności wykonywanych zadań z zakresu administracji rządowej realizowanych na podstawie ustawy o odpadach.**

Zadania z zakresu administracji rządowej określone w ustawie z dnia 14 grudnia 2012r. o odpadach (Dz.U.2016.1987 j.t.), stosownie do Regulaminu Organizacyjnego Starostwa Powiatowego, uchwalonego przez Zarząd Powiatu Uchwałą Nr 172.2016 z dnia 23 września 2016 r., wykonuje Wydział Rolnictwa, Ochrony Środowiska i Budownictwa z filią w Szprotawie. Naczelnikiem Wydziału jest pan Piotr Pietraszkiewicz.

Na podstawie zakresów czynności oraz opisów stanowisk pracy ustalono, że w okresie objętym kontrolą pracownikiem odpowiedzialnym za prowadzenie postępowań w zakresie udzielania, odmowy udzielenia, zmiany, cofnięcia i stwierdzenia wygaśnięcia zezwoleń na prowadzenie działalności w zakresie zbierania odpadów, przetwarzania odpadów oraz zbierania i przetwarzania odpadów była pani inspektor w Wydziale Rolnictwa, Ochrony Środowiska i Budownictwa Renata Gmińska.

Upoważnienie Starosty do wydawania w jego imieniu decyzji w indywidualnych sprawach z zakresu administracji publicznej oraz podpisywania pism dotyczących działania ww. wydziału posiadają: Wicestarosta Żagański, etatowy Członek Zarządu, Naczelnik Wydziału oraz inspektor.

W kontrolowanym okresie na wniosek przedsiębiorców wydano 32 decyzje, z czego 17 zezwoleń na zbieranie odpadów, 9 zezwoleń na przetwarzanie odpadów, 5 zezwoleń na przetwarzanie odpadów i zbieranie odpadów oraz 1 zezwolenie na składowanie odpadów. Ponadto w ww. sprawach zmieniono 11 decyzji i uchylono 2 decyzje. Nie rozpoznano 6 wniosków przedsiębiorców z powodu braku uzupełnienia dokumentacji wymaganej przepisami prawa. Skontrolowano wszystkie prowadzone postępowania.

W trzech postępowaniach - sprawy nr ROŚiB.6233.2.2017; ROŚiB.6233.27.2017; ROŚiB.6233.8.2018, wnioskodawcy terminowo nie uiścili należnej opłaty skarbowej. Z wyjaśnień inspektora Wydziału ROŚiB wynika, że wniesiono opłaty po wezwaniu starosty

o uzupełnienie dokumentacji bądź po szczegółowej analizie stwierdzono, że osoba wstępnie, która nie miała obowiązku wnoszenia opłaty skarbowej, została poproszona aby wniosła opłatę skarbową. Składane wnioski spełniały wymogi formalne określone w art. 42 u.o.o.

W 6 sprawach ROŚiB.6233.10.2016; ROŚiB.6233.13.2016; ROŚiB.6233.4.2017; ROŚiB.6233.14.2017; ROŚiB.6233.15.2017; ROŚiB.6233.4.2018; nie rozpoznano wniosków przedsiębiorców z powodu braku uzupełnienia dokumentacji wymaganej przepisami prawa, ale wcześniej przedsiębiorcy dokonali zapłaty opłaty skarbowej do Urzędu Miejskiego w Żaganiu. Z wyjaśnień inspektora Wydziału ROŚiB wynika, że Starosta przesyła wniosek o zwrot opłaty skarbowej wraz z dokumentacją do UM Żagań, który zobowiązany jest, zgodnie z par. 6 ust. 1 rozporządzenia Ministra Finansów z dnia 28 września 2007 r. w sprawie zapłaty opłaty skarbowej, zwrócić dokonaną opłatę.

Jeżeli organ stwierdził brak dokumentów potwierdzających posiadanie tytułu prawnego do terenu prowadzenia działalności wzywał wnioskodawcę na podstawie art. 64 § 2 k.p.a. do ich uzupełnienia oraz pouczał, że ich nieusunięcie w terminie spowoduje pozostawienie wniosku bez rozpoznania.

Decyzje objęte kontrolą zawierały wszystkie elementy decyzji administracyjnej określone przepisem art. 107 § 1 k.p.a. , informacje, o których mowa w art. 43 ust. 1 i ust. 2 u.o.o., i podpisane zostały przez upoważnione osoby. Kopie decyzji zostały przekazane podmiotom określonym w art. 238 ust. 6 u.o.o. Jak wynika z wyjaśnień inspektora od dnia 21 stycznia 2018r. Starosta Żagański zgodnie z art. 80 ust. 4 ustawy o odpadach przesyła kopie decyzji drogą elektroniczną. Jako dowód przedłożono UPP. Do tej daty kopie decyzji były przekazywane drogą pocztową – listem zwykłym.

W decyzjach organ zamieścił adnotację, o której mowa w § 4 ust. 1 pkt 1 rozporządzenia w sprawie zapłaty opłaty skarbowej. W wyjaśnieniach podano, że nie praktykowano zamieszczania w decyzji informacji o zwolnieniu z opłaty.

Ustalono, że nie wszyscy przedsiębiorcy ubiegający się o wydanie zezwoleń na gospodarowanie odpadami są właścicielami nieruchomości wskazanych, jako miejsce ich magazynowania. Nieruchomościami dysponowali na podstawie umów zawartych z ich właścicielami.

W podstawie prawnej decyzji ROŚiB.606.2.2017. nie powołano się na art. 155 k.p.a., który daje organowi, który wydał decyzję prawo do jej uchylenia po spełnieniu przesłanek w nim wskazanych. Brak podstawy prawnej wg wyjaśnień pani inspektor wynikał z kwalifikacji decyzji dotyczącej cofnięcia bez odszkodowania, a nie uchylenia lub zmiany dlatego powołano się na art. 104 Kpa i przepis szczegółowy tj. art. 47 ust. 2 ustawy o odpadach.

Ustalono, że na trzydzieści dwie prowadzone sprawy, dwadzieścia osiem załatwiono w terminie. W sprawach ROŚiB.6233.2.2016; ROŚiB.6233.7.2016; ROŚiB.6233.16.2016; ROŚiB.6233.12.2017 organ nie dotrzymał miesięcznego terminu na załatwienie sprawy. Nie zawiadomiono strony stosownie art. 36 § 1 k.p.a. o przedłużeniu terminu załatwienia sprawy i jej

przyczynie. Obowiązek ten spoczywa na organie również w przypadku zwłoki w załatwieniu sprawy z przyczyn niezależnych od organu. Udzielono wyjaśnień, że przedłużające się postepowania nie następowały z winy organu, lecz z powodu niekompletnie złożonych wniosków i wymaganych opinii.

W wyniku kontroli ustalono, że w badanym okresie przeprowadzono 3 kontrole w ramach postepowań o przestrzeganie zezwoleń na zbieranie odpadów. W 2018 zaplanowano 4 kontrole przedsiębiorców, którzy uzyskali zezwolenia Starosty Żagańskiego na zbieranie i przetwarzanie odpadów na rok 2018. Kontroli w 2016 i 2017 r. nie planowano i nie przeprowadzano.

We wszystkich kontrolowanych decyzjach ważność zezwolenia na okres 10 lat był zapisany prawidłowo.

W kontrolowanym okresie do Starostwa Powiatowego w Żaganiu nie wpływały i nie były rejestrowane wnioski i skargi z zakresu ustawy o odpadach.

Wykonywanie zadań z zakresu administracji rządowej realizowanych na podstawie ustawy o odpadach oceniono **pozytywnie z nieprawidłowościami.**

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

2.1. Usługi elektroniczne.

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Starostwo Powiatowe w Żaganiu dla wybranych usług publikuje na stronach BIP sposób załatwienia spraw. Na stronie głównej jest przekierowanie na platformę ePUAP, gdzie wystawiona jest jedna usługa elektroniczna – „Skargi, wnioski, zapytania do urzędu".

2.2. Centralne repozytorium wzorów dokumentów elektronicznych.

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

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

2.3. Model usługowy

Podstawa prawna

§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

W Starostwie Powiatowym w Żaganiu zamieszczone są na stronie BIP karty informacyjne usług świadczonych w urzędzie, zawierające także dokumenty do pobrania. Elektroniczne załatwienie sprawy kończy się na etapie urzędu, gdzie dokumenty są drukowane i podlegają papierowemu obiegowi wewnątrz instytucji. Brakuje formalnych procedur zarządzania usługami.

2.4.Współpraca systemów teleinformatycznych z innymi systemami

Podstawa prawna

§ 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.

§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Interoperacyjność systemów informatycznych dobrze funkcjonuje na poziomie Wydziałów Komunikacji i Geodezji. W pozostałych wydziałach systemy informatyczne są wdrożone na poziomie szczątkowym i trudno ocenić ich interoperacyjność i zgodność z systemami referencyjnymi.

2.5.Obieg dokumentów w Urzędzie.

Podstawa prawna

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, nun. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu. jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

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.

Podstawa prawna

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. .

§ 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.

§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

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.

Podstawa prawna

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 informacji16 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.

§ 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.*

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Zarządzenie Nr 14.2016 Starosty Żagańskiego z dnia 14 marca 2016 r. w sprawie aktualizacji „Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi, w których przetwarzane są dane osobowe. Polityka bezpieczeństwa informacji odnosi się w głównej mierze do zakresu danych osobowych, a nie do wszystkich informacji przetwarzanych w urzędzie. Dotychczas nie przeprowadzano działań związanych z przeglądem polityk i zasad, a w dokumentach istnieje wiele rozbieżności ze stanem rzeczywistym.

W trakcie kontroli stwierdzono niżej wymienione nieprawidłowości:

- w Urzędzie nie wdrożono kompleksowo Polityki Bezpieczeństwa Informacji, która jest elementem systemu zarządzania bezpieczeństwem informacji w zakresie określonym w § 20 ust. 1 zarządzenia. Opracowano „Politykę Bezpieczeństwa Ochrony Danych Osobowych" oraz Instrukcję zarządzania systemem informatycznym. Dokumenty te formalnie nie dotyczyły wszystkich danych, jakie są przetwarzane w Urzędzie.
- „Polityka Bezpieczeństwa" oraz „Instrukcji zarządzania systemem informatycznym" zostały

opracowane jedynie na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, co oznacza nieujęcie w ustanowionej dokumentacji ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz 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. Powyższym naruszono § 20 ust. 1 rozporządzenia.

- od dnia ustanowienia w Urzędzie „Polityki bezpieczeństwa" i „Instrukcji zarządzania systemem informatycznym", nie zostały przeprowadzone ustanowione przeglądy dokumentacji, co stanowiło naruszenie wymogu z § 20 ust. 2 pkt 1 zarządzenia, mówiącego o aktualizacji regulacji wewnętrznych w zakresie zmieniającego się otoczenia. Przy dzisiejszym postępie technologicznym należy przyjąć, że SZBI powinien być poddawany przeglądom oraz modyfikowany każdorazowo w wyniku zmian infrastruktury technicznej, nie rzadziej niż raz na rok i zawierać plan, listę sprawdzającą, sprawozdanie z przeglądu dokumentacji. Można przyjąć że dokumentacja jest została ustanowiona w początku 2017 r., ale zawiera liczne odstępstwa od rzeczywistości.

3.2 Analiza zagrożeń związanych z przetwarzaniem informacji

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Przedstawiony dokument „Sprawozdanie z analizy funkcjonowania kontroli zarządczej w Starostwie Powiatowym w Żaganiu w 2017r. z dnia 22.02.2018 r. nie zawiera analizy ryzyka z zakresu bezpieczeństwa informacji.

W czasie wykonywania czynności kontrolnych nie przedstawiono dokumentów potwierdzających wykonywanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co stanowi naruszenie § 20 ust. 2 pkt 3 rozporządzenia.

3.3 Inwentaryzacja sprzętu i oprogramowania informatycznego.

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

W wyniku kontroli ustalono, że inwentaryzacja zasobów informatycznych w Urzędzie nie jest prowadzona. Dane z ewidencji środków trwałych nie zawierają bardziej szczegółowych danych odnośnie konfiguracji sprzętowej oraz zainstalowanego oprogramowania. Stwierdzono brak aktualnej inwentaryzacji oprogramowania w ewidencji, co narusza § 20 ust. 2 pkt 2 rozporządzenia

3.4 Zarządzanie uprawnieniami.

Podstawa prawna

Zgodnie z § 20 ust. 2 pkt 4 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, nun. 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.

§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

W trakcie kontroli stwierdzono, że ewidencja uprawnień jest prowadzona na zasadzie wystawiania pracownikom upoważnień do systemów informatycznych. Prowadzony jest także rejestr zbiorczy wystawionych upoważnień. Brakuje formalnych procedur nadawania i odbierania uprawnień. Wnioskowanie o nadanie uprawnień często przekazywane jest tylko w formie ustnej.

3.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Starostwo Powiatowe w Żaganiu przeprowadziło szkolenia z zakresu bezpieczeństwa informacji. W lutym 2016 roku przeprowadzono szkolenie z zakresu ochrony danych osobowych, a w październiku 2017 roku z zakresu bezpieczeństwa informacji. Szkolenia objęły wszystkich pracowników Urzędu. Pracownicy mają także szkolenia stanowiskowe przeprowadzane przez informatyka, jednak brakuje potwierdzenia tego faktu w dokumentach.

3.6 Praca na odległość i mobilne przetwarzanie danych.

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Urządzenia mobilne nie są szyfrowane i są wynoszone poza siedzibę Urzędu. Brakuje formalnych procedur dotyczących zasad użytkowania sprzętu mobilnego poza siedzibą urzędu. Poza pocztą elektroniczną nie ma zdalnego dostępu do zasobów Starostwa Powiatowego w Żaganiu. Niewłaściwe zarzadzanie urządzeniami podczas pracy poza siedzibą Urzędu stanowi naruszenie § 20 ust. 2 pkt 8 rozporządzenia KRI.

3.7 Serwis sprzętu informatycznego i oprogramowania

Podstawa prawna

§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Starostwo Powiatowe w Żaganiu posiada dwie umowy serwisowe oprogramowania. W obu umowach brakuje zapisów związanych z powierzeniem przetwarzania danych osobowych. Serwis sprzętu informatycznego jest prowadzony w serwisach zewnętrznych bez nośników danych.

3.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Podstawa prawna

Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, tzn. in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określonym i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Podczas kontroli pracownicy urzędu wyjaśnili, że incydenty prawie nie występują. Rejestr incydentów zawiera dwa wpisy. 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.

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

W maju 2018 roku firma LanCenter stworzyła dokumentację wdrożeniową. Dokumentacja ta zawiera elementy podstawowego audytu z zakresu bezpieczeństwa informacji podatności na zagrożenia w oparciu o wymagania normy ISO27001. Jest to zbiór zaleceń wynikających z obserwacji podczas wdrożenia oprogramowania. W dokumencie tym brakuje rzetelnej analizy audytowej, a podane zalecenia mają charakter ogólny.

3.10 Kopie zapasowe.

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Brakuje formalnych procedur wykonywania kopii zapasowych. W wyniku kontroli stwierdzono, że kopie bezpieczeństwa są wykonywane codziennie na serwerach produkcyjnych. W każdy piątek tygodniowa kopia zostaje zgrana na dysk przenośny. Kopie zapasowe powinny być testowo odtwarzane, ale brak na to jednoznacznych dowodów. Niewłaściwe sporządzanie kopii zapasowych stanowi naruszenie § 20 ust. 2 pkt 12 lit. B rozporządzenia KRI.

3.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Podstawa prawna

§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Starostwo Powiatowe w Żaganiu. 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

Podstawa prawna

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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

W Starostwie Powiatowym w Żaganiu istnieją zabezpieczenia fizyczne minimalizujące wystąpienie ryzyka kradzieży informacji i środków przetwarzania informacji. Dostęp do pomieszczenia serwerowni jest ograniczony, ale brakuje wykazu osób uprawnionych do wejścia. Przebywanie osób nieuprawnionych jest nadzorowane, ale wejścia nie są rejestrowane wpisem do dziennika wejść. Do stacji komputerowych pracowników założone są loginy i hasła dostępu, ale brakuje mechanizmu wymuszenia zmiany haseł. Dotyczy to także dostępu do poczty elektronicznej.

3.13 Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Podstawa prawna

*§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

Na komputerach jest zainstalowane oprogramowanie antywirusowe. Systemy posiadają bieżące aktualizacje systemowe, poza kilkoma komputerami z systemem Windows XP, które są przeznaczone do wymiany. Użytkownicy na stanowiskach pracy mają uprawnienia administracyjne, co znacznie utrudnia nadzorowanie instalowanego oprogramowania. Poświadczenia administracyjne do serwerów i systemów, znane są jedynie informatykowi i nie są nigdzie zapisane. Z uwagi na niewystarczającą analizę ryzyka, nie istnieją plany postępowania z ryzykiem, a także dokumentacja zabezpieczeń. Nie są prawidłowo badane podatności systemów informatycznych. Stanowi to naruszenie § 20 ust. 4 rozporządzenia KRI.

3.14 Rozliczalność działań w systemach informatycznych

Podstawa prawna

§ 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.

§ 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.

§ 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

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

W obszarze bezpieczeństwa informacji działalność urzędu **oceniono negatywnie**.

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

Podstawa prawna

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.*

Ustalenie stanu faktycznego, stanowiące podstawę do oceny

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. Obie strony nie zawierają błędów niezgodności ze standardem WCAG 2.0. a także posiadają elementy zmiany kontrastu oraz wielkości czcionki.

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

Przedstawiając powyższe ustalenia, ***zalecam :***

1. przestrzegać terminów załatwiania spraw oraz w każdym przypadku niezałatwienia sprawy w terminie zawiadamiać strony z podaniem przyczyny zwłoki i wskazaniem nowego terminu jej załatwienia oraz pouczeniem o prawie do wniesienia ponaglenia – art. 36 k.p.a.,
2. wydawać decyzje administracyjne w terminach wynikających z Kodeksu postępowania administracyjnego, a w razie przedłużenia terminu poinformować stronę postępowania o tym fakcie,

3. dokonać kompleksowego wdrożenia Systemu zarządzania bezpieczeństwem informacji, uwzględniając wszystkie informacje przetwarzane oraz przechowywane w Urzędzie,
4. przeprowadzać okresową aktualizację dokumentacji SZBI, w tym „Polityki Bezpieczeństwa", „Instrukcji zarządzania systemem informatycznym" oraz innych dokumentów stanowiących SZBI zgodnie z wymogami wskazanymi w § 20 ust. 2 pkt 1 rozporządzenia KRI,
5. badać podatności systemów informatycznych np. na postawie występujących incydentów i określać zagrożenia. Przeprowadzać okresowe udokumentowane analizy ryzyka i przedstawiać sposób postępowania z ryzykiem,
6. wykonywać audyty wewnętrzne przynajmniej raz w roku,
7. wdrożenie procedur zarządzania uprawnieniami,
8. właściwie zarządzać urządzeniami mobilnymi podczas pracy poza siedzibą urzędu,
9. uaktualnić ewidencję sprzętu i oprogramowania,
10. dokumentować inwentaryzację zasobów teleinformatycznych,
11. prowadzić rejestr incydentów. Opracować procedurę zgłaszania incydentów oraz przeszkolić pracowników w tym zakresie,
12. stworzyć procedurę wykonywania kopii zapasowych. Testować i dokumentować okresowe odtwarzanie danych. Dostosować rozwiązania teleinformatyczne dla użytkowników przy wykonywaniu kopii zapasowych stacji roboczych. Opracować plany zapewnienia ciągłości działania.
13. wdrożyć rozwiązania teleinformatyczne zapewniające możliwość przechowywania logów systemowych przez okres minimum 2 lat.
14. wdrożyć regulacje wewnętrzne dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych.
15. wdrożyć procedury umożliwiające zarządzanie usługami realizowanymi przez systemy teleinformatyczne, stosować szczegółowe opisy usług na stronach internetowych urzędu.

W terminie 30 dni liczonym od daty otrzymania niniejszego wystąpienia pokontrolnego, proszę o pisemną informację o sposobie wykonania zaleceń i wykorzystaniu wniosków, a także o podjętych działaniach lub przyczynach ich niepodjęcia.

WOJEWODA LUBUSKI

Władysław Dajczak