Gorzów Wlkp., 05 marca 2018r.

WOJEWODA LUBUSKI

Władysław Dajczak

NK-II.431.1.7.2017.RKam

Pani
Krystyna Pławska
Wójt Gminy Bogdaniec

Wystąpienie pokontrolne
z kontroli przeprowadzonej w trybie zwykłym w Urzędzie Gminy Bogdaniec, 66-450 Bogdaniec, ul. Mickiewicza 45.

Na podstawie art. 28 ust.1 pkt. 2 ustawy z dnia 23 stycznia 2009r. o wojewodzie i administracji rządowej w województwie (Dz.U. 2015.525 ze zm.) oraz art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011r. o kontroli w administracji rządowej (Dz.U. Nr 185, poz. 1092) w dniach od 29 września 2017 r. do 17 listopada 2017 r. zespół kontrolny w składzie:

- Robert Kamiński – inspektor wojewódzki w Wydziale Nadzoru i Kontroli - przewodniczący zespołu,
- Michał Piaskowski – Kierownik Oddziału Informatyki w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych członek zespołu,
- Izabela Milczarek – informatyk ds. administrowania systemami informatycznymi w Biurze Obsługi Urzędu i Rozwoju Systemów Informatycznych – członek zespołu,

przeprowadził kontrolę w trybie zwykłym w kierowanym przez Panią Urzędzie Gminy Bogdaniec.
Kontrolą objęto okres od 1 stycznia 2016 r. do dnia kontroli.
Funkcję Wójta Gminy Bogdaniec w okresie objętym kontrolą pełniła Pani Krystyna Pławska

Działając zgodnie z art. 46 ustawy z dnia 15 lipca 2011r. o kontroli w administracji rządowej przekazuję Pani wystąpienie pokontrolne zawierające ustalenia i ocenę kontrolowanej działalności.

Zakres działalności Urzędu Gminy w Bogdańcu objęty kontrolą.

Kontrola obejmowała swym zakresem realizację zadań z zakresu administracji rządowej w przedmiocie wydawania, odmowy wydania oraz cofania zezwoleń na detaliczną sprzedaż napojów

alkoholowych przeznaczonych do spożycia w miejscu lub poza miejscem sprzedaży w świetle ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz.U.2016.487), zwanej dalej ustawą oraz działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.

Zakres odpowiedzialności.

Na podstawie Regulaminu Organizacyjnego Urzędu Gminy w Bogdańcu wprowadzonego zarządzeniem Wójta Gminy Bogdaniec nr KS.120.18.2012 z dnia 23 lipca 2012 r. sprawami dotyczącymi wydawania zezwoleń na sprzedaż napojów alkoholowych zajmuje się Referat Infrastruktury Technicznej, Ochrony Środowiska i Rolnictwa.

Z przedstawionego zakresu czynności oraz opisu stanowiska pracy wynika, że osobą odpowiedzialną za przygotowanie dokumentacji z zakresu wydawania, cofania i wygaszania zezwoleń w okresie objętym kontrolą była pani Kamila Bednarska.

Upoważnienia Burmistrza do wydawania decyzji z ww. zakresu w kontrolowanym okresie posiadał pan Jan Arcab – Kierownik Infrastruktury Technicznej, Ochrony Środowiska i Rolnictwa.

Za sprawy związane z systemami teleinformatycznymi odpowiadał Pana Marek Trusiński zatrudniony w Urzędzie Gminy Bogdaniec na stanowisku informatyka.

Ustalenia kontroli.

1. **Realizacja zadań z zakresu administracji rządowej w przedmiocie wydawania, odmowy wydania oraz cofania zezwoleń na detaliczną sprzedaż napojów alkoholowych przeznaczonych do spożycia w miejscu lub poza miejscem sprzedaży**

Rada Gminy w Bogdańcu w uchwale nr XXXVI/221/2002 z dnia 17 września 2002 r. ustaliła liczbę punktów sprzedaży napojów alkoholowych zawierających powyżej 4,5% alkoholu (z wyjątkiem piwa) przeznaczonych do spożycia poza miejscem sprzedaży (30) jak i w miejscu sprzedaży (15). Kontrolującym przedstawiono dokumentację, z której wynika, że ilość funkcjonujących punktów sprzedaży alkoholu w roku 2016 jak i 2017 do dnia kontroli nie przekraczała liczby punktów sprzedaży ustalonych w uchwale.

Gminny program profilaktyki i rozwiązywania problemów alkoholowych jest opracowywany cyklicznie na dany rok kalendarzowy.

W 2016r. pracownicy gminy skontrolowali 9 przedsiębiorców prowadzących działalność gospodarczą w zakresie sprzedaży napojów alkoholowych, zgodnie z harmonogramem kontroli zatwierdzonym przez Wójta Gminy Bogdaniec. W 2017 r. zgodnie z planem przeprowadzono 2 kontrole.

Ustalono, że na terenie gminy Bogdaniec nie są rozmieszczone jednostki wojskowe.

Łącznie kontrolą objęto 37 zezwoleń na sprzedaż napojów alkoholowych (wydanych na detaliczną sprzedaż alkoholu jak i na sprzedaż alkoholu w punktach gastronomicznych), w tym 17 zezwoleń jednorazowych, tj. skontrolowano 100% zezwoleń wydanych w okresie objętym kontrolą.

Wszystkie skontrolowane zezwolenia na sprzedaż napojów alkoholowych wydane zostały na podstawie pisemnego wniosku przedsiębiorcy. Zezwolenia wydawano oddzielnie na następujące rodzaje napojów alkoholowych:

1) do 4,5% zawartości alkoholu oraz na piwo,
2) powyżej 4,5% do 18% zawartości alkoholu (z wyjątkiem piwa),
3) powyżej 18% zawartości alkoholu

oraz na czas oznaczony nie krótszy niż 4 lata, w przypadku sprzedaży napojów alkoholowych przeznaczonych do spożycia w miejscu sprzedaży i nie krótszy niż 2 lata, w przypadku sprzedaży napojów alkoholowych przeznaczonych do spożycia poza miejscem sprzedaży.

Skontrolowane zezwolenia na sprzedaż napojów alkoholowych wydane zostały po uzyskaniu pozytywnej opinii komisji rozwiązywania problemów alkoholowych o zgodności lokalizacji punktu sprzedaży z uchwałami rady gminy.

Wniosek o wydanie zezwolenia na sprzedaż napojów alkoholowych udostępniany w Urzędzie Gminy w Bogdańcu zawiera wszystkie wymagane ustawą elementy. Wszystkie składane przez przedsiębiorców wnioski wypełnione zostały prawidłowo.

Przedsiębiorcom posiadającym zezwolenia oraz jednostkom Ochotniczych Straży Pożarnych wydawano jednorazowe zezwolenia na sprzedaż napojów alkoholowych. Łącznie kontrolą objęto 17 zezwoleń jednorazowych.

Skontrolowane jednorazowe zezwolenia na sprzedaż napojów alkoholowych wydane zostały na podstawie pisemnego wniosku przedsiębiorcy. Do 8 zezwoleń jednorazowych w latach 2016-2017 do dnia kontroli nie zostały wniesione opłaty. Powyższe opłaty dotyczyły BOSS Browaru Witnica S.A, który uiścił opłatę wraz z odsetkami 17 października 2017 r. Powyższa opłata została dokonana po audycie wewnętrznym w firmie i stwierdzeniu, że z dniem 1 stycznia 2016 r. BOSS Browar Witnica S.A utracił status zakładu pracy chronionej.

Zezwolenia jednorazowe wydawano na napoje alkoholowe do 4,5 zawartości alkoholu oraz na piwo.

Skontrolowane jednorazowe zezwolenia na sprzedaż napojów alkoholowych wydane zostały po uzyskaniu pozytywnej opinii komisji rozwiązywania problemów alkoholowych o zgodności lokalizacji punktu sprzedaży z uchwałami rady gminy. Od 1 stycznia 2016 r. w związku z wejściem w życie ustawy z dnia 25 czerwca 2015 r. o zmianie ustawy o samorządzie gminnym oraz o zmianie niektórych innych ustaw (Dz.U.2015.1045), na gminnej komisji rozwiązywania problemów alkoholowych nie ciąży obowiązek opiniowania zezwoleń jednorazowych (art. 18^1 ust. 1 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi).

Opłaty za wydanie zezwoleń jednorazowych wnoszone były na rachunek gminy w wysokości odpowiadającej 1/12 rocznej opłaty za dany rodzaj zezwolenia, co jest zgodne z art. 18^1 ust. 3 ustawy.
Nie stwierdzono złożenia przez przedsiębiorców wniosków o wydanie nowego zezwolenia przed upływem 6 miesięcy od dnia wydania decyzji o wygaśnięciu zezwolenia z powodu nie złożenia oświadczenia lub niedokonania opłaty za korzystanie z zezwoleń.

Opłata za wydanie zezwolenia w roku jego nabycia była pobierana w wysokości proporcjonalnej do okresu jego ważności.

Wszyscy przedsiębiorcy, prowadzący sprzedaż napojów alkoholowych w roku poprzednim, złożyli do dnia 31 stycznia, pisemne oświadczenia o wartości sprzedaży poszczególnych rodzajów napojów alkoholowych w danym punkcie sprzedaży za rok poprzedni. W 3 przypadkach na oświadczeniach brak było daty wpływu. Z wyjaśnienia wynika, że w dniu złożenia oświadczenia od ręki było wydane rozliczenie opłaty za dany rok i data wpływu oświadczenia jest datą odebrania powyższego rozliczenia. Daty odebrania rozliczenia mieszczą się w ustawowym terminie.

W przypadkach, gdy roczna wartość sprzedaży napojów alkoholowych w roku poprzednim przekraczała ustalone w ustawie progi, pobierano prawidłowo procentową opłatę od ogólnej wartości sprzedaży poszczególnych rodzajów napojów alkoholowych naliczaną oddzielnie dla każdego rodzaju zezwolenia.

Opłata za korzystanie z zezwoleń na sprzedaż napojów alkoholowych w okresie kontrolowanym była wnoszona na rachunek gminy w każdym roku kalendarzowym objętym zezwoleniem w trzech równych ratach w terminach do 31 stycznia, 31 maja i 30 września danego roku kalendarzowego.

W okresie objętym kontrolą nie wpłynął żaden wniosek od przedsiębiorców, którym zezwolenia wygasły z przyczyn wymienionych w art. 18 ust. 12 ustawy. Wobec powyższego nie wydawano zezwoleń z określeniem terminu na wyprzedaż posiadanych, zinwentaryzowanych zapasów napojów alkoholowych.

Nie stwierdzono odmowy wydania zezwolenia na sprzedaż napojów alkoholowych.
W okresie objętym kontrolą wydano 14 decyzji wygaszających zezwolenia na sprzedaż napojów alkoholowych z powodu złożenia pisemnej rezygnacji, likwidacji punktu sprzedaży i wygaśnięcia zezwolenia.

Nie stwierdzono złożenia przez przedsiębiorców wniosków o wydanie nowego zezwolenia przed upływem 6 miesięcy od dnia wydania decyzji o wygaśnięciu zezwolenia z powodu nie złożenia oświadczenia lub niedokonania opłaty za korzystanie z zezwoleń.
W okresie objętym kontrolą nie została wniesiona do Urzędu Gminy Bogdaniec żadna skarga, wniosek lub petycja związana z podawaniem lub sprzedażą napojów alkoholowych.

Działalność urzędu w zakresie wydawania oraz wygaszania zezwoleń na detaliczną sprzedaż napojów alkoholowych **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.*

§ 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 Gminy w Bogdańcu 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 Obieg dokumentów w Urzędzie.

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.*

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, który został ustalony zarządzeniem nr RG.0050.9.2011 Wójta Gminy Bogdaniec z dnia 21 stycznia 2011r.

2.4 Formaty danych udostępniane przez systemy teleinformatyczne.

Zgodnie z § 17 ust. 1 rozporządzenia: *Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także* w *odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normą ISO/1EC 10646 wraz ze zmianami lub normę ją zastępującą. .*

§ 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.*

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**.

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 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.*

Zarządzenie Nr KS.120.2.2017 z dnia 07 lutego 2017 r. w sprawie wprowadzenia i wdrożenia do stosowania Instrukcji zarządzenia systemem informatycznym służącym do przetwarzania danych osobowych oraz polityki bezpieczeństwa danych osobowych. Do zapoznania się z powyższymi dokumentami zobowiązano pracowników i odbyli oni szkolenia z tego zakresu. 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 planie audytów wewnętrznych nie ma pozycji związanej z bezpieczeństwem informacji.

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

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.*

Zarządzenie nr KS.120.27.2012 Wójta Gminy Bogdaniec z dnia 04 września 2012 r. w sprawie wprowadzenia polityki zarządzania ryzykiem w Gminie Bogdaniec.

W wyniku przeglądu rejestru ryzyk w latach 2016 i 2017 w znikomym zakresie odnosi się do bezpieczeństwa informacji, a co za tym idzie można uznać, że szacowanie ryzyka w tym obszarze nie identyfikuje podatności i zagrożeń w system przetwarzających informacje.

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.

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.*

Ustalono, że inwentaryzacja zasobów informatycznych w Urzędzie prowadzona jest, w formie elektronicznej - plik Excel - zestawienie zawiera informację o użytkowniku, imię i nazwisko, nazwie stacji roboczej, systemie operacyjnym oraz zainstalowanego oprogramowania.

Stwierdzono, że informacje o przypisanych sprzęcie informatycznym do pracowników są prowadzone prawidłowo, natomiast ewidencja zainstalowanego oprogramowania jest nieaktualna.

Stwierdzono brak aktualnej inwentaryzacji oprogramowania w ewidencji, 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, 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.*

W trakcie kontroli wprowadzono zarządzenie nr. KS.120.29.2017 Wójta Gminy Bogdaniec z dnia 25 października 2017 r. w sprawie ewidencji użytkowników i uprawnień w systemie informatycznym Urzędu Gminy Bogdaniec. Zarządzenie to formalizuje i porządkuje sposób zarządzania uprawnieniami, a także wprowadza rejestr użytkowników i ich uprawnień w systemach informatycznych. Rejestr ten został wypełniony danymi i zatwierdzony.

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.

W badanym okresie Urząd zapewnił szkolenia pracowników zaangażowanych w procesie przetwarzania informacji. Zakres szkolenia obejmował obszary dotyczące zagrożenia bezpieczeństwa informacji, odpowiedzialności prawnej za naruszenie bezpieczeństwa informacji oraz stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich. Szkolenie było prowadzone przez firmę zewnętrzną, a dla pracowników, którzy nie mogli uczestniczyć w tych szkoleniach instruktaż przeprowadziła Pani Krystyna Breń.

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 nie są przechowywane na nich żadne dane. Wynoszone poza urząd są tylko za zgodą kierownictwa. Pracownicy nie posiadają opcji zdalnego dostępu do danych, a zdalny dostęp jest wykorzystywany jedynie przy pracach serwisowych w jednym systemie za pomocą zestawionego bezpiecznego połączenia.

3.7 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

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

Podczas kontroli pracownicy urzędu wyjaśnili, że incydenty nie występują. 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.

3.8 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.*

Ustalono, że w planie audytów wewnętrznych na rok 2017 nie ma pozycji związanej z bezpieczeństwem informacji.

Audyt wewnętrzny ma za zadanie dostarczyć informację czy posiadany SZBI jest zgodny z własnymi wymaganiami i przepisami prawa oraz czy jest skutecznie wdrożony i utrzymany. Przeprowadzenie audytu wewnętrznego związane jest z:

- zaplanowaniem, ustanowieniem, wdrożeniem i utrzymaniem programu audytów. Program audytów powinien zawierać wyniki poprzednich audytów,;
- zdefiniowaniem kryteriów audytu i zakresu;
- wybraniem audytora i prowadzeniem audytu w sposób zapewniających obiektywność i bezstronność procesu audytu;
- przedstawieniem wyników audytu kierownikowi jednostki

Audyt wewnętrzny systemu zarządzania bezpieczeństwem informacji powinien być wykonywany przynajmniej raz w roku.

Przedstawiony plan audytów wewnętrznych nie zawierał pozycji związanych z bezpieczeństwem informacji, co jest naruszeniem § 20 ust. 2 pkt 14 rozporządzenia.

3.9 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.*

Szczegółowe zasady tworzenia kopii zapasowych zostały opisane w Instrukcji zarządzania systemami informatycznymi. Zgodnie z tą instrukcją kopie powinny być przechowywane w odrębnym pomieszczeniu. W wyniku kontroli stwierdzono, że kopie bezpieczeństwa są przechowywane w serwerowni na serwerze produkcyjnym urzędu.

Zdaniem kontrolujących kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż dane produkcyjne. Jest to także napisane w wewnętrznych regulacjach Urzędu. Przechowywanie kopii bezpieczeństwa na tym samym serwerze co dane jest dużym zagrożeniem ich bezpieczeństwa i podnosi celowości wykonywania kopii zapasowych. Kopie zapasowe powinny być testowo odtwarzane, a brak na to jednoznacznych dowodów. Brak też rejestru (zestawienia), które dane są poddawana procesowi wykonywania kopii bezpieczeństwa. Niewłaściwe sporządzanie kopii zapasowych stanowi naruszenie § 20 ust. 2 pkt 12 lit. B rozporządzenia KRI.

3.10 Zabezpieczenia techniczno-organizacyjne dostępu do informacji, systemów teleinformatycznych i rozliczalność działań w systemach teleinformatycznych.

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.*

§ 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.*

§ 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 n> *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.*

Zgodnie z Instrukcją zarządzania systemami informatycznymi dostęp do komputera jest wymuszony podaniem identyfikatora i hasła, które jest okresowo zmieniane. Na komputerach jest zainstalowane oprogramowanie antywirusowe. Systemy posiadają bieżące aktualizacje systemowe. Uprawnienia administracyjne są rozproszone. W systemach teleinformatycznych jest jedno konto administracyjne, na które logują się wszystkie osoby posiadające uprawniania. Zgodnie z Załącznikiem 2 Instrukcji zarządzania systemami informatycznymi hasła administracyjne powinny być przechowywane w zapieczętowanej kopercie. W wyniku działań kontrolnych nie udało się tego faktu potwierdzić.

Niewłaściwe zarządzanie uprawnieniami administracyjnymi narusza § 21 ust 2 rozporządzenia, gdyż nie zapewnia rozliczalności działań administracyjnych w systemach informatycznych.

W obszarze systemu zarządzania bezpieczeństwem informacji w systemach informatycznych działalność Urzędu **oceniono negatywnie.**

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 Gminy w Bogdańcu 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 130 błędów, jednak nie miały one istotnego wpływu na prezentowanie treści dla osób niepełnosprawnych. Strona BIP nie zawierała błędów niezgodności ze standardem WCAG 2.0.

Działalność Urzędu w zakresie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych **oceniono pozytywnie.**

W związku z ustaleniami kontroli zaleca się:

- dokonanie kompleksowego wdrożenia Systemu zarządzania bezpieczeństwem informacji, uwzględniając wszystkie informacje przetwarzane oraz przechowywane w Urzędzie,
- przeprowadzenie okresowej aktualizacji 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,
- zbadanie podatności systemów informatycznych np. na podstawie występujących incydentów i określać zagrożenia,
- przeprowadzenie okresowych udokumentowanych analiz ryzyka i przedstawić sposób postępowania z ryzykiem,
- wykonanie okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok,
- uaktualnienie ewidencji sprzętu i oprogramowania,
- dokumentowanie inwentaryzacji zasobów teleinformatycznych,
- prowadzenie rejestru incydentów naruszenia bezpieczeństwa informacji. Należy opracować procedurę zgłaszania incydentów oraz przeszkolić pracowników w tym zakresie,
- przeanalizowanie procedur wykonywania kopii zapasowych. Należy dostosować rozwiązania teleinformatyczne w tym zakresie do ogólnie przyjętych norm i dobrych praktyk oraz opracować plany zapewnienia ciągłości działania,
- przyjęcie rozwiązań organizacyjnych zapewniających rozliczalność czynności administracyjnych.

W terminie do dnia 30 czerwca 2018r., oczekuję informacji o sposobie wykonania zaleceń i wykorzystania wniosków lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

WOJEWODA LUBUSKI

Władysław Dajczak