WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 2 sierpnia 2018 r.

FK-IV.431.11.2018

Szanowny Pan
Andrzej Bondaruk
Wójt Gminy Godkowo
Godkowo 14
14-407 Godkowo

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092), zwanej dalej „ustawą o kontroli w administracji rządowej", przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Gminy w Godkowie, Godkowo 14, 14-407 Godkowo, NIP: 582-10-01-575, REGON: 000532837.

W okresie objętym kontrolą oraz w okresie prowadzenia kontroli stanowiska pełnili:

1. Pan **Andrzej Bondaruk** - Wójt, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu30 listopada 2014 r. (*kierownik jednostki kontrolowanej*)
2. Pani **Izabela Charmuszko** - Sekretarz, zatrudniona podstawie umowy o pracę od dnia 01 marca 2015 r. (*nadzorująca bezpośrednio pracowników realizujących zadania objęte kontrolą poz. 7 i 8*)
3. Pani **Bożena Maria Makuch** - Skarbnik, powołana na stanowisko w dniu 01.07.2010 r. Uchwałą Nr XLV/189/2010 Rady Gminy Godkowo z dnia 01.07.2010 r. (*nadzorująca bezpośrednio pracowników realizujących zadania objęte kontrolą poz. 4-6*)
4. Pani **Anna Mindza** – inspektor, zatrudniona na podstawie umowy o pracę od dnia 26.04.2004 r. (*pracownik realizujący zadania objęte kontrolą*)
5. Pani **Ewelina Olejniczak** – podinspektor, zatrudniona na podstawie umowy o pracę od dnia 03.06.2013 r. (*pracownik realizujący zadania objęte kontrolą*)
6. Pani **Jadwiga Turowska** – inspektor, zatrudniona na podstawie umowy o pracę od dnia 15.09.1979 r. (*pracownik realizujący zadania objęte kontrolą*)
7. Pani **Danuta Dzika** – inspektor, zatrudniona na podstawie umowy o pracę od dnia 01.02.1979 r. (*pracownik realizujący zadania objęte kontrolą*)
8. Pan **Eugeniusz Karpiński** - Kierownik USC, zatrudniony na podstawie umowy o pracę od dnia 11.06.1984 r. (*pracownik realizujący zadania objęte kontrolą*)

[akta kontroli str. 51-52]

Kontrolę przeprowadził pracownik Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie, Radosław Gazda – inspektor wojewódzki; legitymacja służbowa nr 21/2014, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienie do kontroli nr FK-IV.0030.456.2018 z 4 czerwca 2018 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 17]

Kontrolę przeprowadzono w dniach 20-21 czerwca 2018 r., co zostało odnotowane w książce kontroli Urzędu Gminy w Godkowie 0911 pod pozycją Nr 2/2018.

Przedmiotem była kontrola systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2017 r. poz. 570 ze zm.). Pierwotnie okres objęty kontrolą wyznaczono na 2017 rok. Pismem z dnia 18 czerwca 2018 r. rozszerzono okres objęty kontrolą na: od dnia 1 stycznia 2017 r. do dnia 20 czerwca br. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1-2, 30-31]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. Nr 185, poz. 1092) oraz art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (t.j. Dz. U. z 2017 r., poz. 2234) w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2017 r. poz. 570 ze zm.) zwanej dalej „ustawą" oraz rozdziału III i IV 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 (Dz.U. z 2017 r. poz. 2247 j.t.) zwanego dalej „rozporządzeniem KRI", jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 32-47]

W czasie trwania czynności kontrolnych w Urzędzie Gminy w Godkowie informacji i wyjaśnień udzielała Sekretarz Gminy. Bieżąca kontrola była pierwszą kontrolą zewnętrzną z tego zakresu przeprowadzaną w Urzędzie Gminy w Godkowie.

Na podstawie ustaleń kontroli, realizację zadań z zakresu wykorzystania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z nieprawidłowościami.**

Ocena działalności jednostki kontrolowanej wynika z następujących ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez UG w Godkowie przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w kontrolowanej jednostce do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **4** systemy teleinformatyczne oraz prowadzone są **2** rejestry publiczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie Gminy w Godkowie:

1) **SYGNITY**, który dzieli się na moduły:
   - **Oprogramowanie do Obsługi Świadczeń Rodzinnych (SR)** ma na celu wspomaganie pracowników w realizacji zadań wynikających z ustawy o świadczeniach rodzinnych oraz towarzyszących ustawie aktów prawnych. Zadaniem oprogramowania SR jest obsługa rejestracji i przetwarzania danych związanych z procesem przyznawania i wypłaty świadczeń rodzinnych, windykacji świadczeń nienależnie pobranych oraz monitorowania stanu realizacji zadań. Zarejestrowane dane wykorzystywane są w obligatoryjnej sprawozdawczości statystycznej.
   - **Oprogramowanie do obsługi Funduszu Alimentacyjnego (FA)** ma na celu wspomaganie pracowników w realizacji zadań wynikających z ustawy o pomocy osobom uprawnionym do alimentów oraz towarzyszących ustawie aktów prawnych. Zadaniem oprogramowania FA jest obsługa rejestracji i przetwarzania danych związanych z procesem przyznawania i wypłaty świadczeń, obsługą świadczeń nienależnie pobranych, zadłużeń dłużników alimentacyjnych oraz monitorowania stanu realizacji zadań. Zarejestrowane dane wykorzystywane są w obligatoryjnej sprawozdawczości statystycznej.
   - **Oprogramowanie do obsługi Stypendiów (ST)** jest systemem informatycznym mającym za zadanie wspierać i usprawniać pracę użytkownikom w realizacji zapisów ustawy o systemie oświaty z dnia 7 września 1991r., a także windykacji należności na poziomie gminy.
   - **Oprogramowanie do Obsługi Świadczeń Wychowawczych (SW)** zapewnia pracownikom pomoc w realizacji podstawowych zadań wynikających z ustawy o pomocy państwa w wychowywaniu dzieci.

2) **PUMA - Moduł Ewidencja Ludności** posiada homologację MSW DEP, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności (KEL). Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca (KOM).
   Program automatyzuje prace i drukuje zawiadomienia w zakresie: meldowania,

wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego, gromadzenia i dostępu do danych historycznych mieszkańców.
Pierwotne ładowanie LBD (Lokalnego Banku Danych – tzn. Bazy w KEL) jest dokonywane danymi pobranymi z TBD/WBD lub CBD (Terenowego/Wojewódzkiego lub Centralnego Banku Danych). Aplikacja udostępnia funkcjonalność rejestru wniosków o udostępnienie danych osobowych oraz umożliwia wymianę informacji z Centralnym, Wojewódzkim i Terenowym Bankiem Danych.

3) **ŹRÓDŁO** - bezpłatna aplikacja tworzona w ramach programu pl.ID obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych i stanu cywilnego. Dodatkowo umożliwia również realizację zadań Systemu Odznaczeń Państwowych oraz Centralnego Rejestru Sprzeciwów. W efekcie ŹRÓDŁO to uniwersalne narzędzie obsługujące m.in.: Rejestr PESEL, Rejestr Bazy Usług Stanu Cywilnego (BUSC), Rejestr Dowodów Osobistych (RDO), System Odznaczeń Państwowych (SOP), Centralny Rejestru Sprzeciwów (CRS).

4) **CEIDG** jest to elektroniczny rejestr przedsiębiorców działających na terenie kraju. Portal ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności.

Rejestry publiczne prowadzone w Urzędzie Gminy w Godkowie:
1) Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości (podstawa prawna - art. 9b ust. 2-3 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, t. j. Dz. U. z 2017 r., poz. 1289 ze zm.),
2) Rejestr decyzji zezwalających na prowadzenie działalności gospodarczej w zakresie opróżniania zbiorników bezodpływowych i transportu nieczystości ciekłych (podstawa prawna - art. 7 ust. 6b ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, t. j. Dz. U. z 2017 r., poz. 1289 ze zm.).

[akta kontroli str. 28, 88-92, 397-409]

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

1.1. Usługi elektroniczne

Z art. 16 ust. 1a ustawy wynika, że *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 KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:
a) 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;

b) *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 Godkowie posiada aktywną Elektroniczną Skrzynkę Podawczą znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę ePUAP, zawarto na stronie internetowej Urzędu w prawym panelu ekranu, gdzie znajduje się menu przedmiotowe. Urząd Gminy w Godkowie udostępniał oraz świadczył usługę elektroniczną, z wykorzystaniem ePUAP, tj. „Pismo ogólne do urzędu". Usługa ta umożliwia złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie, co do której nie mają zastosowania inne formularze. W menu przedmiotowym na stronie głównej Urzędu zawarto również odnośnik do strony OBYWATEL.GOV.PL administrowanej przez Ministerstwo Cyfryzacji, za pomocą której jest możliwość realizacji usług drogą elektroniczną (np. dowód osobisty, paszport).

Na dzień przeprowadzenia czynności kontrolnych strona internetowa Urzędu posiadała bezpośrednie połączenie z BIP Urzędu. Opis procedur obowiązujących przy załatwianiu spraw w Urzędzie został opublikowany na stronie Urzędu Gminy Godkowo i zawierał dane dotyczące: właściciela usługi (komórka organizacyjna), podstawy prawnej, wymaganych dokumentów, wysokości opłaty, terminu i sposobu realizacji, trybu odwoławczego oraz dodatkowych informacji i uwag. W przypadku wyodrębnionych usług (np. karta dużej rodziny, 500+), istniała możliwość złożenia wniosku elektronicznego za pomocą portalu informacyjno-usługowego Ministerstwa Rodziny Pracy i Polityki Społecznej EMP@TIA, o czym zamieszczona została stosowna informacja na stronie www U.G. Godkowo.
Jednocześnie należy nadmienić, że na stronie internetowej Urzędu (przy procedurze dot. karty dużej rodziny) zamieszczona została szczegółowa instrukcja dotycząca możliwości założenia profilu zaufanego on-line, który jest niezbędny przy składaniu wniosków drogą elektroniczną.

[akta kontroli str. 93-113]

Z § 5 ust. 2 pkt 4 rozporządzenia KRI wynika, że kontrolowany podmiot powinien publikować i uaktualniać w Biuletynie Informacji Publicznej opisy procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną. Kontrolujący stwierdził, że w BIP Urzędu są wymienione rodzaje załatwianych spraw, jednakże większość z nich nie zawiera opisanych procedur obowiązujących przy ich realizacji. Powyższe procedury są opisane na stronie www Urzędu. Mając powyższe na uwadze, jak również to, że strona internetowa Urzędu posiadała bezpośrednie połączenie z BIP Urzędu, przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

Przyczyną powstania uchybienia był brak publikacji w BIP opisów procedur obowiązujących przy załatwianiu spraw z zakresu właściwości Urzędu drogą elektroniczną, co skutkowało naruszeniem § 5 ust. 2 pkt 4 rozporządzenia KRI. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b 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 kwalifikowanym podpisem elektronicznym.*

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.

W trakcie kontroli ustalono, że Urząd Gminy w Godkowie w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE. Jednocześnie Urząd Gminy w Godkowie świadczył usługę elektroniczną, z wykorzystaniem platformy ePUAP, tj. „Pismo ogólne do urzędu", która umożliwia złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie, co do której nie mają zastosowania inne formularze. W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 114, 397]

1.3. Model usługowy

Z § 15 ust. 2 rozporządzenia KRI wynika, że *zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.*

Strona internetowa Urzędu działa pod adresem http://www.godkowo.pl/, a strona internetowa BIP Urzędu – pod adresem http://www.bip.godkowo.pl. Na stronie internetowej Urzędu zamieszono link do strony BIP oraz w prawym panelu ekranu, gdzie znajduje się menu przedmiotowe, zamieszczono link do skrzynki podawczej na platformie ePUAP. Urząd wykorzystywał platformę ePUAP, jako główne narzędzie do świadczenia usług elektronicznych poprzez automatyczną integrację ePUAP z usługą „Pismo ogólne do urzędu" umożliwiającą złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie. W menu przedmiotowym na stronie głównej Urzędu zawarto również odnośnik do strony OBYWATEL.GOV.PL administrowanej przez Ministerstwo Cyfryzacji, za pomocą której jest możliwość realizacji usług drogą elektroniczną w innych jednostkach. W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

W Urzędzie Gminy w Godkowie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt że Urząd nie świadczy takich usług na zewnątrz, oprócz usługi „Pismo ogólne do urzędu" świadczonej na platformie ePUAP. Dla poszczególnych referatów na stronie Urzędu załączone są jedynie pliki stanowiące wzory dokumentów do pobrania. Ewentualne elektroniczne załatwienie sprawy kończy się na etapie urzędu, gdzie dokumenty są drukowane i podlegają papierowemu obiegowi wewnątrz instytucji.

[akta kontroli str. 114-119]

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

- § 5 ust. 3 pkt 3 rozporządzenia KRI *interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;*
- § 16 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w 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.*

Wiele rejestrów w urzędach administracji publicznej przechowuje i przetwarza identyczne informacje, np. o obywatelu/podmiocie, takie jak PESEL, REGON, NIP, dane adresowe itp. Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu będzie sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

Z informacji uzyskanych z Urzędu Gminy w Godkowie wynika, że kontrolowane systemy współpracują z innymi systemami publicznymi, tj. między systemami PUMA - ŹRÓDŁO następuje wymiana danych, ponadto poprzez system SYGNITY następuje również wymiana danych z systemem EMP@TIA. Również z systemu SYGNITY generowane są dokumenty przelewów do systemu HOME BANKING.
Prowadzone rejestry publiczne odwoływały się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne (np. PUMA → ŹRÓDŁO), w zakresie niezbędnym do realizacji zadań. Współpraca pomiędzy systemami Urzędu była możliwa jedynie dzięki wyposażeniu w odpowiednie składniki sprzętowe oraz oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących. Systemy informatyczne spełniały minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu, jak również systemami innych jednostek administracji publicznej. W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 400]

1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególność 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 Gminy w Godkowie 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 rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67).
Zarządzeniem nr 19/2011 Wójta Gminy Godkowo z dnia 4 kwietnia 2011 r. w sprawie sposobu wykonywania czynności kancelaryjnych określono, że w Urzędzie Gminy Godkowo obowiązuje tradycyjny (papierowy) system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji wytworzonej i przyjętej do Urzędu Gminy w Godkowie.
Jednocześnie należy zwrócić uwagę, iż w wewnętrznych procedurach Urzędu dotyczących wykonywania czynności kancelaryjnych nie określono zasad obiegu dokumentów wpływających drogą elektroniczną (skrzynka podawcza na platformie ePUAP), co powoduje naruszenie § 20 ust. 2 pkt 9 rozporządzenia KRI. Niewskazanie sposobu postępowania z dokumentami przyjmowanymi w postaci elektronicznej może prowadzić do narażenia na utratę autentyczności, integralności oraz poufności informacji zawartych w sprawie, której dokument dotyczy. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.
Przyczyną powstania uchybienia był brak w procedurach wewnętrznych zapisów w zakresie sposobu postępowania z dokumentami przyjmowanymi w postaci elektronicznej, co

skutkowało naruszeniem § 20 ust. 2 pkt 9 rozporządzenia KRI. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 120]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI k*odowanie 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/IEC 10646 wraz ze zmianami lub normę ją zastępującą;*
- § 18 ust. 1 rozporządzenia KRI *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 *KRI 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.*

Istotą współdzielenia informacji w urzędach jest stworzenie możliwości wymiany danych pomiędzy różnymi systemami informatycznymi oraz umożliwienie odbiorcom swobodnego dostępu do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików. Systemy informatyczne użytkowane w Urzędzie Gminy w Godkowie posiadały możliwość generowania zasobów informacyjnych oraz przyjmowanie elektronicznych dokumentów w formatach danych zawartych w załączniku nr 2 do rozporządzenia KRI, tj. np. pdf, xls, odt, html. Wymiana znaków odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 121-122, 400]

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI p*odmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;*

- § 20 ust. 2 rozporządzenia KRI *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 KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*

Podmiot publiczny 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. Wymaga to opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym możliwości skutecznego zarządzania bezpieczeństwem informacji w podmiocie.
Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji.

Zarządzeniem Nr 79/2015 z dnia 3 listopada 2015 r. Wójt Gminy Godkowo wprowadził do stosowania w Urzędzie Politykę Bezpieczeństwa Informacji - zgodnie z obowiązującą w tym okresie ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2014 poz. 1182) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024). W skład PBI wchodziły:
- Zał. 1 - Instrukcja ochrony danych osobowych w Urzędzie Gminy w Godkowie;
- Zał. 2 - Instrukcja eksploatacji systemów informatycznych, w których przetwarzane są dane osobowe w Urzędzie Gminy w Godkowie.

Przedmiotowym zarządzeniem wszyscy pracownicy Urzędu, którzy przetwarzają dane osobowe zostali zobowiązani do przestrzegania jego treści.

Powyższe dokumenty, a w szczególności Instrukcja eksploatacji systemów informatycznych, w których przetwarzane są dane osobowe w Urzędzie Gminy w Godkowie, stanowią dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (…). Służą one zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

Mając na względzie wprowadzenie rozporządzenia KRI, zgodnie z § 20 ust. 2 i ust. 2 pkt 1

przedmiotowego rozporządzenia oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) – RODO, Zarządzeniem Nr 81/2017 Wójta Gminy Godkowo z dnia 29 grudnia 2017 r., przyjęto System Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy w Godkowie. W ramach SZBI zostały opracowane następujące polityki i procedury:
Polityka bezpieczeństwa informacji w zakresie danych osobowych oraz:

- Procedura stosowania SZBI;
- Procedura w zakresie analizy ryzyka bezpieczeństwa informacji;
- Procedura w zakresie planowania i ciągłości działania;
- Procedura w zakresie klasyfikacji informacji;
- Procedura w zakresie nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych;
- Procedura w zakresie zarzadzania bezpieczeństwem fizycznym i dostępem do pomieszczeń;
- Procedura w zakresie bezpieczeństwa fizycznego sprzętu i nośników;
- Procedura w zakresie użytkowania stanowiska komputerowego;
- Procedura w zakresie zarządzania incydentami i słabościami w SZBI;
- Procedura w zakresie zarządzania kluczami do pomieszczeń.

Dokumentacja SZBI dotyczyła wszystkich danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych); zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa informacji.

Jednocześnie należy zaznaczyć, że Urząd Gminy Godkowo nie przeprowadzał do dnia kontroli żadnych audytów oraz jakichkolwiek przeglądów Polityki Bezpieczeństwa Informacji, jak również całego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z § 20 ust. 1 rozporządzenia KRI, co stanowi nieprawidłowość. W zakresie audytów – szczegółowo w pkt 2.9.
Z wyjaśnienia Wójta Gminy w powyższej sprawie wynika, że: „*w związku z tym, że SZBI weszło w życie pod koniec roku ubiegłego, audyty, o których mowa nie zostały ujęte w planach wydatków na rok bieżący. Jednak Urząd Gminy planuje podjąć rozmowy z audytorem wiodącym normy ISO 27001, celem wykonania takiego audytu. Jeśli okaże się, że Urząd Gminy nie będzie w stanie własnymi siłami przeprowadzić analizy, dokonamy jej zlecenia:*.
Odnosząc się do powyższych wyjaśnień należy stwierdzić, że Polityka Bezpieczeństwa Informacji została wprowadzona do stosowania w Urzędzie dnia 3 listopada 2015 r. Od tego momentu należało podejmować działania w celu doskonalenia bezpieczeństwa informacji przetwarzanych w Urzędzie poprzez organizację ich przeglądów. Jedocześnie należy stwierdzić, że System Zarządzania Bezpieczeństwem Informacji (SZBI) został opracowany

w Urzędzie i wymaga jak najszybszego sprawdzenia (audytu) w zakresie dopasowania jego procesów do realiów pracy, w celu ewentualnych zmian dokumentacji SZBI.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.
Przyczyną powstania nieprawidłowości było nieprzeprowadzanie okresowych przeglądów bezpieczeństwa informacji w Urzędzie, co skutkowało naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 123-181, 182-307]

Na stronie internetowej BIP UG w Godkowie zawarto zapis: *Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) informuję, iż Administratorem Pani/Pana danych osobowych jest Gmina Godkowo z siedzibą Godkowie nr 14, 14-407 Godkowo, reprezentowana przez: Wójta Gminy Godkowo. Administrator wyznaczył Inspektora Ochrony Danych, kontakt: tel. (55) 249-72-10, e-mail: sekretariat.godkowo@gmail.com.*

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Z § 20 ust. 2 pkt 3 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu. Zgodnie z Zarządzeniem Nr 81/2017 Wójta Gminy Godkowo z dnia 29 grudnia 2017 r. przyjęto System Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy w Godkowie. W przedmiotowym dokumencie została opracowana *metodyka oszacowania ryzyka dla bezpieczeństwa informacji w Urzędzie*. Dokument ten nakładał na Wójta Gminy obowiązek powołania Zespołu ds. Bezpieczeństwa Informacji, który przeprowadziłby oszacowanie ryzyka dla bezpieczeństwa informacji oraz określiłby planu postępowania z ryzykiem. Na pytanie kontrolującego dotyczące przeprowadzania analizy ryzyka w związku z przyjęciem dokumentacji SZBI, Wójt Gminy wyjaśnił, że: „*w związku z tym, że SZBI weszło w życie pod koniec roku ubiegłego, audyty o których mowa nie zostały ujęte w planach wydatków na rok bieżący. Jednak Urząd Gminy planuje podjąć rozmowy z audytorem wiodącym normy ISO 27001, celem wykonania takiego audytu. Jeśli okaże się, że Urząd Gminy nie będzie w stanie własnymi siłami przeprowadzić analizy, dokonamy jej zlecenia:*.

Brak przeprowadzonej analizy ryzyka dla bezpieczeństwa informacji w Urzędzie należy uznać za nieprawidłowość. Przyczyną nieprawidłowości jest niepowołanie Zespołu ds. Bezpieczeństwa Informacji i nieprzeprowadzenie oszacowania ryzyka dla bezpieczeństwa informacji zgodnie z przyjętym SZBI. Skutkiem jest naruszenie § 20 ust. 2 pkt 3 rozporządzenia KRI. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 197-206, 400]

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Z § 20 ust. 2 pkt 2 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

Z wyjaśnienia Wójta Gminy wynika, że: *„W Urzędzie Gminy w Godkowie nie ma dodatkowego dokumentu poza przyjętą Polityką Bezpieczeństwa Informacji oraz Systemem Zarządzania Bezpieczeństwem Informacji. Inwentaryzacja sprzętu komputerowego jest przeprowadzana corocznie łącznie z inwentaryzacją majątku, a w przypadku zakupu nowego sprzętu i oprogramowania w ciągu roku, ewidencje sprzętu i oprogramowania aktualizowane są na bieżąco przez informatyka."*
Kontrolującemu przedstawiono aktualną (na dzień 20.06.2018 r.) inwentaryzację oprogramowania oraz sprzętu komputerowego użytkowanego w Urzędzie.
Jednocześnie należy stwierdzić, że przedmiotowa inwentaryzacja nie zawierała m.in. informacji o osobie, która obsługuje komputer, adresie IP, zainstalowanym oprogramowaniu, systemie operacyjnym, parametrach technicznych (m.in. ilość pamięci, rodzaj i wielkość dysku twardego, typie procesora). Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.
Przyczyną stwierdzonego uchybienia było przeprowadzanie inwentaryzacji z pominięciem elementów w zakresie rodzaju i konfiguracji inwentaryzowanego sprzętu. Skutkiem stwierdzonego uchybienia było naruszenie § 20 ust. 2 pkt 2 rozporządzenia KRI. Odpowiedzialnym jest osoba wyznaczona do przeprowadzenia inwentaryzacji sprzętu.

[akta kontroli str. 308-309, 401]

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: 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 KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Istotnym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zgodnie z zarządzeniem Nr 79/2015 z dnia 3 listopada 2015 r. Wójta Gminy Godkowo w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Godkowie zasady nadawania zmiany i cofania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych określa Rozdział VIII Polityki Bezpieczeństwa Informacji (PBI).
Polityka bezpieczeństwa informacji w zakresie ochrony danych osobowych zawarta jest w załączniku nr 11 Zarządzenia Nr 81/2017 Wójta Gminy Godkowo z dnia 29 grudnia 2017 r. w sprawie przyjęcia SZBI w Urzędzie Gminy w Godkowie.
W Urzędzie Gminy w Godkowie prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych wg. załącznika nr 5 do Polityki Bezpieczeństwa Informacji. Każdy z pracowników, który pracował w systemach teleinformatycznych posiadał stosowne upoważnienie do przetwarzania danych osobowych, jak również w zależności od użytkowanego systemu teleinformatycznego, stosowne pisemne zgłoszenie do zarejestrowania użytkownika w aplikacji lub usłudze systemu teleinformatycznego, zgodnie z załącznikiem nr 2 do Polityki Bezpieczeństwa Informacji. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 164-165, 264-298, 310-348]

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: 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 pracownicy Urzędu Gminy w Godkowie, zaangażowani w proces przetwarzania informacji, zostali przeszkoleni w przedmiotowej tematyce. Zakres szkolenia obejmował obszary dotyczące zagrożenia bezpieczeństwa informacji, odpowiedzialność prawną za naruszenie bezpieczeństwa informacji oraz stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko

błędów ludzkich. Na szkoleniu w dniu 15 czerwca 2018 roku omówione zostały główne założenia dotyczące RODO. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 349-351]

2.6. Praca na odległość i mobilne przetwarzanie danych

Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Zarządzeniem Nr 79/2015 z dnia 3 listopada 2015 r. Wójta Gminy Godkowo w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Godkowie wprowadzone zostały *zasady korzystania z komputerów przenośnych* (zał. nr 4). Zarządzeniem Nr 81/2017 Wójta Gminy Godkowo z dnia 29 grudnia 2017 r. w sprawie przyjęcia SZBI w Urzędzie Gminy w Godkowie, określono rejestr osób uprawnionych do wykorzystywania sprzętu mobilnego poza obszarem Urzędu, którym Wójt Gminy wyraził zgodę na korzystanie z tego sprzętu. Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 139, 246]

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii oraz gwarantującymi bezpieczeństwo informacji (BI) dla informacji uzyskanych przez wykonawców w związku z ich realizacją. W Urzędzie Gminy w Godkowie użytkowane są 2 systemy teleinformatyczne do realizacji zadań publicznych zakupione u zewnętrznego dostawcy, tj. Sygnity i Puma. W związku z zakupem obydwu systemów podpisane zostały umowy licencyjne z firmami: Sygnity S.A. oraz ZETO SOFTWARE Sp. z o.o.

- W przypadku umowy na opiekę autorską podpisanej z ZETO SOFTWARE Sp. z o.o. na użytkowanie programów pod nazwą PUMA, zawarto zapisy/klauzule dotyczące bezpieczeństwa informacji, w tym zapisy regulujące powierzenie przetwarzania danych osobowych (§4 pkt 8 umowy).
- W przypadku umowy licencyjnej z firmą Sygnity S.A na użytkowanie poszczególnych modułów w ramach systemu, nie zawarto klauzul regulujących powierzenie przetwarzania danych osobowych. W § 4 umowy – Postanowienia końcowe, zawarto jedynie zapisy zobowiązujące strony do zachowania tajemnicy wszelkich informacji dotyczących

warunków umowy oraz innych wiadomości, co do których druga strona poweźmie kroki celem zachowania ich w poufności, co nie gwarantuje odpowiedniego poziomu bezpieczeństwa informacji, w tym bezpieczeństwa przetwarzania danych osobowych. Powyższa sytuacja narusza częściowo zapisy § 20 ust. 2 pkt 10 rozporządzenia KRI i stanowi uchybienie.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

Przyczyną powstania uchybienia było nieprzestrzeganie postanowień § 20 ust. 2 pkt 10 rozporządzenia KRI, co skutkowało podpisaniem umowy niezawierającej w całości zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 352-366]

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określonym i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji został uregulowany w następujących dokumentach:

- Zarządzeniem Nr 79/2015 z dnia 3 listopada 2015 r. Wójta Gminy Godkowo w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Godkowie wprowadzona została *zasada nr 5 Postępowanie w przypadku wykrycia próby nieupoważnionego dostępu do danych* (zał. nr 9).
- Zarządzeniem Nr 81/2017 Wójta Gminy Godkowo z dnia 29 grudnia 2017 r. w sprawie przyjęcia SZBI w Urzędzie Gminy w Godkowie, w procedurze nr 10 *Zarządzanie incydentami i słabościami w SZBI,* określono zasady zgłaszania i rejestracji zaistniałych incydentów.

W badanym okresie stwierdzono jedynie uszkodzenie zasilaczy w serwerze z oprogramowaniem PUMA, na skutek awarii sieci energetycznej. Po wymianie zasilaczy i dokonaniu analizy działania systemy stwierdzono poprawność działania systemu PUMA.
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 149-150, 256-261, 367]

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

Z wyjaśnienia Wójta Gminy wynika, że: „*w związku z tym, że SZBI weszło w życie pod koniec roku ubiegłego, audyty o których mowa nie zostały ujęte w planach wydatków na rok bieżący. Jednak Urząd Gminy planuje podjąć rozmowy z audytorem wiodącym normy ISO 27001, celem wykonania takiego audytu. Jeśli okaże się, że Urząd Gminy nie będzie w stanie własnymi siłami przeprowadzić analizy, dokonamy jej zlecenia”*.
Odnosząc się do powyższych wyjaśnień wskazać należy, iż wymogiem SZBI jest regularne przeprowadzanie audytów wewnętrznych w zakresie BI w systemach informatycznych. Celem audytów jest ewentualne ujawnienie słabości SZBI, a także słabości zabezpieczeń i w wyniku zaleceń poaudytowych doskonalenie SZBI oraz zabezpieczeń. Jedocześnie należy stwierdzić, że System Zarządzania Bezpieczeństwem Informacji (SZBI) został opracowany w Urzędzie i wymaga jak najszybszego sprawdzenia (audytu) w zakresie dopasowania jego procesów do realiów pracy, w celu ewentualnych zmian dokumentacji SZBI. Brak przeprowadzonych audytów SZBI stanowi naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI, co należy uznać za nieprawidłowość.
Przyczyną powstania nieprawidłowości było nieprzeprowadzenie audytów wewnętrznych w celu zapewnienia bezpieczeństwa informacji w Urzędzie. Skutkiem było naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 400-401]

2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.*

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Tworzenie kopi zapasowych jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć wykonując regularnie kopie zapasowe całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

Procedurę tworzenia, przechowywania, przekazywania i wydawania kopii bezpieczeństwa zawarto w Polityce Bezpieczeństwa Informacji przyjętej Zarządzeniem Wójta Gminy Godkowo Nr 79/2015 z dnia 3 listopada 2015 r. w załącznikach:
nr 5 – zasady wykonywania i przechowywania kopii bezpieczeństwa,
nr 6 – zasady przekazywania i wydawania kopii bezpieczeństwa z archiwum oddalonego,
nr 7 – zasady odzyskiwania bazy danych osobowych z kopii bezpieczeństwa.

Z wyjaśnień Wójta Gminy wynika, że: „*w celu zapewnienia ciągłości działania systemów teleinformatycznych w urzędzie obowiązuje plan ciągłości działania na wypadek:*
1. braku dostępu do zasobów sieci komputerowej,
2. zawieszenia pracy systemu,
3. braku zasilania obiektu energią elektryczną.
Kopie bezpieczeństwa wykonywane są codziennie i przechowywane zarówno na serwerze oraz na dysku zewnętrznym (po zaszyfrowaniu)”.

Jednocześnie wskazać należy, że z §2 ust. 1 zał. nr 5 do Polityki Bezpieczeństwa Informacji, tj. zasad wykonywania i przechowywania kopii bezpieczeństwa wynika, że *kopia bezpieczeństwa wykonywana jest w cyklu dziennym*.
Z prowadzonego (zgodnie z zał. nr 5 do Polityki Bezpieczeństwa Informacji) rejestru wykonywania kopii bezpieczeństwa wynika, że kopia bezpieczeństwa w zakresie systemów teleinformatycznych wykonywana była w okresie objętym kontrolą maksymalnie 4 razy w miesiącu (np. 4 września, 11 września, 22 września, 30 września 2017 r.), w pozostałych przypadkach wykonywanie kopii bezpieczeństwa odbywało się 1-3 razy w miesiącu. Powyższe odstępstwo od ustalonych w PBI zasad stanowi uchybienie. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.
Przyczyną powstania uchybienia było nieprzestrzeganie §2 ust. 1 zał. nr 5 do Polityki Bezpieczeństwa Informacji - Instrukcja eksploatacji systemów (…), który stanowi, że kopia bezpieczeństwa wykonywana jest w cyklu dziennym. Powyższe uchybienie skutkowało nieterminowym wykonywaniem kopii bezpieczeństwa danych z systemów informatycznych. Osobą odpowiedzialną był informatyk wykonujący kopie bezpieczeństwa.

[akta kontroli str. 141-145, 188, 369-371, 401]

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI s*ystemy 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.*

Rozdział X Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Godkowie – Instrukcja eksploatacji systemów (…), szczegółowo reguluje zagadnienia dotyczące przeglądów i konserwacji sprzętu komputerowego oraz zbioru danych. Zgodnie z zapisami ww. dokumentu, bieżących oraz okresowych przeglądów, konserwacji sprzętu i napraw, niewymagających angażowania firm serwisowych, dokonuje Informatyk. Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Informatyk. Przeglądów i konserwacji zbioru danych osobowych dokonują użytkownicy zgodnie z indywidualnymi zakresami obowiązków. W przypadku korzystania z zewnętrznej firmy serwisującej, przegląd i konserwacja zbioru danych odbywa się pod nadzorem Informatyka lub osoby przez niego wyznaczonej.

W okresie objętym kontrolą nie zidentyfikowano w Urzędzie Gminy w Godkowie systemów będących na etapie projektowania oraz wdrażania, w związku z czym nie było potrzeby posiadania przez jednostkę procedury w powyższym zakresie. Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 132-133]

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI wynika, że z*arządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:*

- 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 *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;*
- pkt 11 *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

Z wyjaśnień Wójta Gminy wynika, że: „*aby zapewnić ochronę informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniem lub zakłóceniem na każdej ze stacji roboczych zostały wydzielone konta użytkowników i administratora, zainstalowano program antywirusowy (ESET NOD32), wykonywane są kopie zapasowe. Logowanie do systemów odbywa się za pomocą uwierzytelnienia. Zablokowano dostęp do stron www z nieodpowiednią treścią*.”

Powyższe zostało sprawdzone przez kontrolującego na 2 stacjach roboczych obsługujących systemy informatyczne służące do realizacji zadań publicznych. Ponadto w Urzędzie Gminy w Godkowie w celu ochrony przetwarzanych danych obowiązuje całkowity zakaz używania nośników pamięci przenośnej, tj. pamięć typu flash, płyty CD, DVD, pochodzących z nieznanych źródeł oraz nie dających się zweryfikować oprogramowaniem antywirusowym. Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 133, 401]

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

- § 20 ust. 2 pkt 12 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: 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, 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 KRI *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.*

Zgodnie z wyjaśnieniami cytowanymi w punkcie 2.12 jednostka przedstawiła stosowane mechanizmy w celu zapewniania ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Odbywa się to m.in. poprzez: działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp oraz kontrolę dostępu do systemów operacyjnych. W systemie PUMA i Sygnity logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga wymiany co 30 dni. W systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe. Ponadto zgodnie z zapisami obowiązującymi w jednostce, systemy informatyczne służące do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:

- poprzez zainstalowanie programu antywirusowego *ESET NOD32*,
- poprzez zablokowanie dostępu do niektórych stron www będących potencjalnymi nośnikami złośliwego oprogramowania,

przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej:

- poprzez stosowanie zasilaczy awaryjnych UPS,
- wykonywanie kopii bezpieczeństwa.

Kontrolowana jednostka zapewnia fizyczne bezpieczeństwo przetwarzanych informacji, m.in. poprzez:

- zainstalowanie elektronicznego systemu alarmowego wewnątrz budynku,
- zawarcie umowy z firmą zewnętrzną na konserwację i obsługę awaryjną systemu alarmowego,
- zamykanie na klucz pokoi, w których przetwarzane są informacje, każdorazowo przy

opuszczeniu przez pracownika stanowiska pracy,
- zabezpieczenie krytycznych pomieszczeń kratami w oknach,
- kontrolę dysponowania kluczami do pomieszczeń.

Bezpieczeństwo działania systemów teleinformatycznych realizowane jest również poprzez okresową aktualizację oprogramowania w zakresie działania poszczególnych systemów do najnowszych wersji.
Urząd Gminy w Godkowie podpisał umowę na świadczenie usług informatycznych, w celu kompleksowej obsługi systemów informatycznych, w tym miedzy innymi administrowanie i zarządzanie siecią teleinformatyczną, sporządzanie i weryfikację kopii zapasowych, modernizację oprogramowania i sprzętu, reakcję na zgłoszona awarię oraz jak najszybsze przywrócenie pełnej sprawności systemów w przypadku wystąpienia awarii. Umowa zawierała zobowiązanie do zachowania przez zleceniobiorcę tajemnicy i nie ujawniania danych osobowych przetwarzanych przez zleceniodawcę.

Podczas kontroli dokonano także oględzin pomieszczenia pełniącego w Urzędzie rolę serwerowni. Pomieszczenie nie posiada klimatyzacji (pomimo wysokiej temperatury panującej wewnątrz) oraz systemów monitorujących parametry środowiskowe (temperatura, wilgotność, zadymienie, wyciek wody), co może mieć negatywny wpływ na znajdujące się w nim urządzenia oraz niesie ryzyko utraty informacji w wyniku awarii. Wejście do pomieszczenia posiada obite blachą drzwi, w których zainstalowano dwa zamki. Okno znajdujące się w pomieszczeniu zabezpieczono metalową kratą, co potwierdza dokumentacja z przeprowadzonych oględzin. Powyższe stanowi uchybienie, które może skutkować utratą informacji w wyniku awarii sprzętu. Przyczyną powstania uchybienia jest niedostosowanie pomieszczenia pełniącego rolę serwerowni do pracy w nim jednostek centralnych, na których opiera się działanie poszczególnych systemów informatycznych. Osobą odpowiedzialną jest kierownik kontrolowanej jednostki.
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

[akta kontroli str. 375-387]

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:
- § 21 ust. 2 rozporządzenia KRI *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;*
- § 21 ust. 3 rozporządzenia KRI *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 KRI *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.*

Z wyjaśnień Wójta Gminy wynika, że cyt.: „*Rozliczalność działań w systemach teleinformatycznych zapewnia się poprzez przechowywanie logów systemowych na dysku zewnętrznym przez okres 3 lat. Ponadto oprogramowanie dziedzinowe gromadzi rejestr czynności, przechowuje dane o wszystkich operacjach wykonywanych w systemie”.*
Mając na uwadze powyższe wyjaśnienia przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 401]

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

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 19 rozporządzenia KRI, 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 KRI.

Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy w Godkowie, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0. W toku kontroli dokonano jednak weryfikacji zgodności ze standardem WCAG 2.0 strony internetowej Urzędu oraz BIP Urzędu, poprzez wykorzystanie narzędzia dostępnego na stronie internetowej http://wave.webaim.org, tj. walidatora WAVE-WCAG 2.0. W przypadku strony www urzędu walidacja wykazała 7 błędów, w przypadku strony BIP walidacja wykazała 12 błędów. Wykazane błędy nie miały jednak istotnego wpływu na prezentowanie treści dla osób niepełnosprawnych.

Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strona internetowa Urzędu oraz BIP Urzędu spełniały poniższe zasady:

- postrzeganie – informacje oraz komponenty interfejsu strony były przedstawione użytkownikom w sposób dostępny dla jego zmysłów,
- funkcjonalność – komponenty interfejsu stron umożliwiały korzystanie z nich,

– zrozumiałość – informacje oraz obsługa interfejsu były zrozumiałe.

Zarówno strona internetowa www Urzędu oraz strona BIP Urzędu zawierały elementy umożliwiające zmiany kontrastu oraz wielkości czcionki. Dostosowanie zostało wykonane z możliwością wyboru 2 kontrastów oraz sześciu rozmiarów czcionki za pomocą ikony (NIEDOWIDZĄCY) oraz (A+ A-) umieszczonej w prawym górnym rogu strony. Powyższe zagadnienie oceniono pozytywnie.

[akta kontroli str. 388-394]

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Opublikowanie i uaktualnianie w BIP opisów procedur obowiązujących przy załatwianiu w Urzędzie spraw drogą elektroniczną, zgodnie z § 5 ust. 2 pkt 4 rozporządzenia KRI.

2. Uzupełnienie wewnętrznych procedur Urzędu dotyczących wykonywania czynności kancelaryjnych, o zasady obiegu dokumentów wpływających drogą elektroniczną (skrzynka podawcza na platformie ePUAP).

3. Przeprowadzenie przeglądów Bezpieczeństwa Informacji w tym Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z § 20 ust. 1 rozporządzenia KRI.

4. Przeprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz przyjętym SZBI.

5. Sporządzanie inwentaryzacji sprzętu zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI tj. utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

6. Uwzględnianie w podpisywanych umowach z firmami dostarczającymi oprogramowanie, zapisów § 20 ust. 2 pkt 10 rozporządzenia KRI, a w szczególności zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

7. Przeprowadzenie audytu wewnętrznego bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI

8. Wykonywanie kopii bezpieczeństwa danych zgodnie z §2 ust. 1 zał. nr 5 do Polityki Bezpieczeństwa Informacji tj. w cyklu dziennym lub zmianę zasad dotyczących częstotliwości wykonywania kopii bezpieczeństwa.

9. Przeprowadzenie w miarę możliwości finansowych Urzędu modernizacji pomieszczenia serwerowni, w zakresie montażu klimatyzacji oraz systemów monitorujących parametry środowiskowe.

Proszę Pana Wójta o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i uchybień oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 30 dni od dnia otrzymania niniejszego wystąpienia, o sposobie wykorzystania uwag i wniosków oraz wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Jednocześnie informuję, że stosownie do art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

WOJEWODA
WARMIŃSKO-MAZURSKI

Artur Chojecki