WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 13 września 2018 r.

FK-IV.431.15.2018

Szanowna Pani
Bożena Grochala
Wójt Gminy
Janowiec Kościelny 62
13-111 Janowiec Kościelny

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 Pani treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Gminy w Janowcu Kościelnym, Janowiec Kościelny 62, 13-111 Janowiec Kościelny, NIP: 7450005521, REGON: 000532808 oraz Gminnym Ośrodku Pomocy Społecznej w Janowcu Kościelnym, Janowiec Kościelny 148, 13-111 Janowiec Kościelny, NIP: 9840055692, REGON: 004457676.

W okresie objętym kontrolą oraz w okresie prowadzenia kontroli stanowiska pełnili:
Pracownicy Urzędu Gminy w Janowcu Kościelnym:

1. **Pani Bożena Grochala** - Wójt Gminy, wybrana na stanowisko w wyniku wyborów bezpośrednich w dniu 02.12.2010 roku (*kierownik jednostki kontrolowanej*),
2. **Pani Zofia Wielgus** - Sekretarz, zatrudniona na podstawie umowy o pracę od dnia 14.02.2011 roku (*nadzorująca bezpośrednio pracowników objętych kontrolą*),
3. **Pan Piotr Szempliński** - St. Informatyk, zatrudniony na podstawie umowy o pracę od dnia 01.09.1999 roku (*realizujący zadania objęte kontrolą*),
4. **Pani Ewelina Mierzejewska** - Kierownik USC, zatrudniona na podstawie umowy o pracę od dnia 23.10.2007 roku (*realizująca zadania objęte kontrolą*).

Pracownicy Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym:

1. **Pan Leszek Stryjewski** - Główny specjalista pracy socjalnej, zatrudniony na podstawie umowy o pracę od dnia 02.12.2004 roku (*pełni zastępstwo podczas nieobecności Kierownika GOPS Janowiec Kościelny*),
2. **Pani Anna Szczecińska** - Referent ds. świadczenia wychowawczego, zatrudniona na podstawie umowy o pracę od dnia 02.03.2016 roku (*realizująca zadania objęte kontrolą*),

3. **Pan Piotr Rakoczy** - Inspektor, zatrudniony na podstawie umowy o pracę od dnia 16.04.2012 roku (*realizujący zadania objęte kontrolą*),
4. **Pani Anna Figurska** - Stażysta - pomoc administracyjna, zatrudniona na podstawie umowy o odbyciu stażu podpisanej z Powiatowym Urzędem Pracy w Nidzicy na okres od 02.07.2018 do 30.11.2018 roku (*realizująca zadania objęte kontrolą*).

[akta kontroli str. 60-61]

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.0030.618.2018 z 10 sierpnia 2018 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 59]

Kontrolę przeprowadzono w dniach 13-14 sierpnia 2018 r., co zostało odnotowane w książce kontroli Urzędu Gminy w Janowcu Kościelnym pod pozycją Nr 14/2018, w książce kontroli Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym pod pozycją Nr 5/2018.

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.). Okres objęty kontrolą: od dnia 1 stycznia 2017 r. do dnia 13 sierpnia br. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1-2, 32-41]

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, 32-41]

W czasie trwania czynności kontrolnych informacji i wyjaśnień udzielali pracownicy upoważnieni przez Wójta Gminy, tj.: Sekretarz Gminy, Kierownik USC, Starszy informatyk oraz Inspektor GOPS. Bieżąca kontrola była pierwszą kontrolą zewnętrzną z tego zakresu przeprowadzaną w Urzędzie Gminy w Janowcu Kościelnym.

[akta kontroli str. 62]

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 uchybieniami.**

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

Z informacji przekazanych przez UG oraz GOPS w Janowcu Kościelnym przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w kontrolowanej jednostce do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywanych jest **5** systemów teleinformatycznych oraz prowadzone są **2** rejestry publiczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie Gminy w Janowcu Kościelnym:

1) **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. **Moduł Wyborcy** – kompleksowa obsługa wyborów. Moduł Wyborcy umożliwia obsługę kart dodatkowych rejestru wyborców (tzw. kart zielonych, różowych oraz kart niebieskich) i pozwala m.in. na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców w gminie lub mieście na podstawie bazy danych ewidencyjnych.

2) **ŹRÓDŁO** - bezpłatna aplikacja, która 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).

3) **AW_USC** - moduł wspomagający w zakresie kompleksowej obsługi stanu cywilnego. Migracja danych do systemu Źródło. Producent Technika Gliwice/ZETO Białystok.

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.

Systemy teleinformatyczne wykorzystywane w GOPS w Janowcu Kościelnym:

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. .
- **Oprogramowanie do Obsługi Świadczeń Wychowawczych (SW) + Dobry Start**, zapewnia pracownikom pomoc w realizacji podstawowych zadań wynikających z ustawy o pomocy państwa w wychowywaniu dzieci. Zadaniem Oprogramowania SW + Dobry Start jest obsługa rejestracji i przetwarzania danych związanych z procesem przyznawania i wypłaty świadczenia Dobry Start, windykacji świadczeń nienależnie pobranych, monitorowania stanu realizacji zadań oraz wykorzystaniu danych zarejestrowanych w systemie w obligatoryjnej sprawozdawczości statystycznej.

Rejestry publiczne prowadzone w Urzędzie Gminy w Janowcu Kościelnym:

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. 30-31, 53-55, 560-565]

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 Janowcu Kościelnym 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 e-PUAP, zawarto na stronie internetowej Urzędu, w prawym panelu ekranu w zakładce – KONTAKT oraz bezpośrednio w lewym panelu ekranu – zakładka e-PUAP, gdzie znajduje się również menu przedmiotowe. GOPS w Janowcu Kościelnym posiada również 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 e-PUAP, zawarto na stronie internetowej GOPS w prawym panelu ekranu w zakładce Menu główne.

Zarówno Urząd Gminy jaki i GOPS w Janowcu Kościelnym udostępniały oraz świadczyły 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 odnośniki do stron:

- OBYWATEL.GOV.PL administrowanej przez Ministerstwo Cyfryzacji, za pomocą której jest możliwość realizacji usług drogą elektroniczną (np. dowód osobisty, paszport),
- CEiDG - portal ten ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności,
- BIZNES.gov.pl - serwis informacyjno-usługowy dla przedsiębiorcy nadzorowany przez Ministerstwo Przedsiębiorczości i Technologii.

Zarówno na stronie UG jak i GOPS w Janowcu Kościelnym istniała możliwość złożenia wniosku elektronicznego za pomocą portalu informacyjno-usługowego Ministerstwa Rodziny Pracy i Polityki Społecznej EMP@TIA.
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 BIP Urzędu Gminy w Janowcu Kościelnym 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. Strona GOPS w Janowcu Kościelnym, zawierała w menu przedmiotowym *Poradnik interesanta*, w którym zawarte zostały dane dotyczące: podstawy prawnej, wymaganych dokumentów, wysokości opłaty, terminu i sposobu realizacji, trybu odwoławczego oraz dodatkowych informacji i uwag.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 63-78]

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 oraz GOPS w Janowcu Kościelnym 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 zarówno Urząd Gminy jak i GOPS 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. 20, 43, 64, 77]

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://janowiec.warmia.mazury.pl, a strona internetowa BIP Urzędu – pod adresem http://bip.janowieckoscielny.warmia.mazury.pl. Strona internetowa GOPS w Janowcu Kościelnym działa pod adresem http://www.gops.janowieckoscielny.info.

Na stronie internetowej Urzędu zamieszczono link do strony BIP. W prawym panelu ekranu w zakładce – KONTAKT oraz bezpośrednio w lewym panelu ekranu – zakładka e-PUAP, zamieszczono link do skrzynki podawczej na platformie ePUAP. GOPS w Janowcu Kościelnym posiada również aktywną Elektroniczną Skrzynkę Podawczą. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej GOPS w prawym panelu ekranu w zakładce Menu główne. Zarówno Urząd Gminy jaki i GOPS wykorzystywały 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 odnośniki do stron: OBYWATEL.GOV.PL administrowanej przez Ministerstwo Cyfryzacji, za pomocą której jest możliwość realizacji usług drogą elektroniczną (np. dowód osobisty, paszport), CEiDG - portal ten ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności, BIZNES.gov.pl - serwis informacyjno-usługowy dla przedsiębiorcy nadzorowany przez Ministerstwo Przedsiębiorczości i Technologii. Zarówno na stronie UG jak i GOPS w Janowcu Kościelnym istniała możliwość złożenia wniosku elektronicznego za pomocą portalu informacyjno-usługowego Ministerstwa Rodziny Pracy i Polityki Społecznej EMP@TIA. W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

W Urzędzie Gminy oraz GOPS w Janowcu Kościelnym brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt, że instytucje te nie świadczyły usług elektronicznych na zewnątrz, oprócz usługi „Pismo ogólne do urzędu" świadczonej na platformie ePUAP. Dla poszczególnych referatów na stronie Urzędu oraz GOPS załączone są jedynie pliki stanowiące wzory dokumentów do pobrania.

Ewentualne elektroniczne załatwienie sprawy kończy się na etapie urzędu, gdzie dokumenty w formie elektronicznej są weryfikowane (podpis elektroniczny, oddzielenie spamu), drukowane i podlegają papierowemu obiegowi wewnątrz instytucji.

[akta kontroli str. 63, 64, 69, 72, 77]

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 w wyniku kontroli wynika, że kontrolowane systemy Urzędu Gminy współpracują z innymi systemami publicznymi. Wymiana danych odbywa się pomiędzy systemami **PUMA - ŹRÓDŁO** oraz **AW_USC – ŹRÓDŁO**. Na wymianę danych w powyższych systemach nie podpisywano umów gdyż obowiązek ten wynika z uregulowań odgórnych na szczeblu ministerialnym.
W GOPS Janowiec Kościelny zapewniana jest komunikacja, poprzez projekt emp@tia, z systemami: PESEL, Centralna Aplikacja Rynku Pracy, EKSMOoN, ZUS, CEIDG, KRS, KRUS, oraz systemem Ministerstwa Finansów, z których pobierane są dane dla celów realizacji złożonych wniosków o przyznanie świadczenia. Wykorzystywane przez GOPS systemy firmy Sygnity automatycznie przekazują dane do centralnej bazy beneficjenta CBB. Na wymianę danych nie ma podpisanych umów, obowiązek ten wynika bezpośrednio z ustaw, tj.: ustawa z dnia z dnia 28 listopada 2003 roku o świadczeniach rodzinnych, ustawa z dnia z dnia 7 września 2007 roku o pomocy osobom uprawnionym do alimentów oraz ustawy z dnia 11 lutego 2016 roku o pomocy państwa w wychowywaniu dzieci.
Współpraca pomiędzy systemami była możliwa 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. 555-559]

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 Janowcu Kościelnym 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 roku 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 10/2011 Wójta Gminy Janowiec Kościelny z dnia 15 lutego 2011 roku, w sprawie instrukcji kancelaryjnej i rzeczowego wykazu akt określono, że w Urzędzie Gminy w Janowcu Kościelnym obowiązuje tradycyjny nieelektroniczny z możliwością korzystania z narzędzi informatycznych do wspomagania obiegu dokumentacji system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji wytworzonej i przyjętej do Urzędu.
W wewnętrznych procedurach Urzędu dotyczących wykonywania czynności kancelaryjnych określono zasady obiegu dokumentów wpływających drogą elektroniczną (skrzynka podawcza na platformie ePUAP oraz gmina@janowiec.com.pl), zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, co zapobiega narażeniu dokumentów elektronicznych na utratę autentyczności, integralności oraz poufności informacji w nich zawartych.

Zarządzeniem Nr 3/2015 Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 14 maja 2015 roku, w sprawie wprowadzenia zmian w instrukcji określającej czynności kancelaryjne w Gminnym Ośrodku Pomocy Społecznej w Janowcu Kościelnym określono, że w GOPS obowiązuje tradycyjny nieelektroniczny z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentacji system wykonywania czynności kancelaryjnych. W wewnętrznych procedurach GOPS dotyczących wykonywania czynności kancelaryjnych określono zasady obiegu dokumentów wpływających drogą elektroniczną.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 79-110]

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.

Z informacji uzyskanych w wyniku kontroli wynika, że systemy teleinformatyczne w Urzędzie Gminy umożliwią dwukierunkową wymianę danych. W ramach systemu AW_USC dane generowane są do plików XML, za pomocą aplikacji narzędziowej dostarczonej przez producenta, które następnie można zaimportować w systemie ŹRÓDŁO. Kodowanie plików XML odbywa się według standardu Unicode UTF-8. W przypadku systemu PUMA jest on zasilany bezpośrednio z systemu ŹRÓDŁO za pomocą aplikacji narzędziowej dostarczonej przez producenta oprogramowania. Format przekazywanych danych to XML. Kodowanie plików XML odbywa się według standardu Unicode UTF-8.

W przypadku systemu SYGNITY użytkowanego przez GOPS w Janowcu Kościelnym, to Minister właściwy do spraw zabezpieczenia społecznego, w porozumieniu z Ministrem właściwym do spraw informatyzacji, określa w drodze rozporządzenia opis systemów teleinformatycznych stosowanych w urzędach administracji publicznej realizujących zadania zlecone (m.in. ŚR, FA, ŚW, ST) zawierający strukturę systemu, wymaganą minimalną funkcjonalność systemu oraz zakres komunikacji między elementami struktury systemu, w tym zestawienie struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących, o których mowa w art. 13 ust. 2 pkt 2 lit. a ustawy.

Zarówno systemy teleinformatyczne używane w Urzędzie Gminy jak i GOPS w Janowcu

Kościelnym umożliwiają udostępnianie danych w powszechnie dostępnych formatach plików tj.: XML, PDF, TXT, RTF, ODT, DOC.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 555-559]

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 20/2013 Wójta Gminy Janowiec Kościelny z dnia 19 marca 2013 roku, w sprawie powołania Administratora Bezpieczeństwa Informacji, ustanowiono osobę do pełnienia obowiązków ABI, w Urzędzie Gminy Janowiec Kościelny.

- Zarządzeniem Nr 25/2013 Wójta Gminy Janowiec Kościelny z dnia 19 marca 2013

roku, w sprawie ustalenia „Dokumentacji ochrony danych osobowych w Urzędzie Gminy Janowiec Kościelny", (uaktualnionej w dniu 15 marca 2016 roku), wprowadzono między innymi politykę bezpieczeństwa w zakresie danych osobowych przetwarzanych w Urzędzie oraz instrukcję zarządzania systemem informatycznym - zgodnie z obowiązującą w tym okresie ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2002 nr 101, poz. 926 ze zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku 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). Wszyscy pracownicy Urzędu, którzy przetwarzają dane osobowe zostali zobowiązani do przestrzegania jego treści.

- Zarządzeniem Nr 13/2017 Administratora Danych Osobowych – Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 11 września 2017 roku, w sprawie zasad ochrony danych osobowych w GOPS w Janowcu Kościelnym. wprowadzono do stosowania „*Politykę Bezpieczeństwa przetwarzania danych osobowych w GOPS w Janowcu Kościelnym*" oraz ustalono „*Instrukcję zarządzania systemem informatycznym przeznaczonym do przetwarzania danych osobowych w GOPS w Janowcu Kościelnym"*- zgodnie z obowiązującą w tym okresie ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2014, poz. 1182 ze zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku, 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). Wszyscy pracownicy GOPS, którzy przetwarzają dane osobowe zostali zobowiązani do przestrzegania jego treści.

Powyższe dokumenty, a w szczególności instrukcja zarządzania systemem informatycznym przeznaczonym do przetwarzania danych osobowych w Urzędzie Gminy oraz GOPS w Janowcu Kościelnym, 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.

Zgodnie z § 20 ust. 1 i ust. 2 pkt 1-2 rozporządzenia KRI, jak również mając na względzie wprowadzenie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, 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 46/2018 Wójta Gminy Janowiec Kościelny z dnia 24 maja 2018 roku, w sprawie wprowadzenia polityki ochrony danych w Urzędzie Gminy Janowiec

Kościelny, przekazano do stosowania założenia polityki ochrony danych między innymi:

- instrukcję gromadzenia i przetwarzania danych osobowych,
- instrukcję wypełniania praw podmiotów danych,
- uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych,
- środki organizacyjne służące bezpieczeństwu danych osobowych,
- środki techniczne służące bezpieczeństwu danych osobowych,
- bezpieczeństwo (analiza ryzyka),
- incydenty bezpieczeństwa ochrony danych osobowych,
- inspektor ochrony danych (wybór, pozycja, zadania).

Wszyscy pracownicy Urzędu, którzy przetwarzają dane osobowe zostali zobowiązani do przestrzegania jego treści.

– Zarządzeniem Nr 48/2018 Wójta Gminy Janowiec Kościelny z dnia 24 maja 2018 roku, w sprawie wyznaczenia Inspektora Ochrony Danych, wskazano osobę (przedstawiciela firmy zewnętrznej) do pełnienia obowiązków Inspektora Ochrony Danych.

– Zarządzeniem Nr 6/2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 24 maja 2018 roku, w sprawie wprowadzenia polityki ochrony danych w GOPS w Janowcu Kościelnym, przekazano do stosowania założenia polityki ochrony danych. Wszyscy pracownicy GOPS, którzy przetwarzają dane osobowe zostali zobowiązani do przestrzegania jego treści

Dokumentacja w zakresie bezpieczeństwa informacji dotyczyła wszystkich danych przetwarzanych w Urzędzie oraz GOPS w Janowcu Kościelnym 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 w Janowcu Kościelnym, zgodnie z opracowanym planem sprawdzeń bezpieczeństwa informacji na dany rok, przeprowadzał cyklicznie sprawdzenia (wewnętrzne) funkcjonowania bezpieczeństwa informacji - szczegółowo w pkt 2.9, jak również przeprowadził niezwłocznie po wprowadzeniu zarządzenia Nr 46/2018 analizę i szacowanie ryzyka ochrony danych - szczegółowo w pkt 2.2. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 111-318, 348-443, 508-513, 566-590]

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.
Aktualizację Polityki Bezpieczeństwa Informacji dokonano Zarządzeniem Nr 46/2018 Wójta Gminy Janowiec Kościelny z dnia 24 maja 2018 roku, w sprawie wprowadzenia polityki ochrony danych w Urzędzie Gminy Janowiec Kościelny. W przedmiotowym dokumencie zawarto zapis, że analiza ryzyka ochrony danych przeprowadzana jest nie rzadziej niż raz na rok. Dokument zawiera również opracowaną metodykę przeprowadzania analizy ryzyka.
Mając na względzie zapisy wprowadzonej powyższym zarządzeniem polityki ochrony danych w Urzędzie Gminy Janowiec Kościelny, niezwłocznie, tj. w dniu 25 maja 2018 r. przeprowadzona została analiza ryzyka według opracowanej metodyki. Przeprowadzona analiza zidentyfikowała zagrożenia i podatności w obszarze przetwarzania danych osobowych realizowanych przez Urząd i wyznaczyła terminy na wyeliminowanie zagrożeń, jak również proponowane rozwiązania.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 111, 144-145, 308-318]

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 inwentaryzacja sprzętu komputerowego i oprogramowania odbywa się w ramach inwentaryzacji majątku gminy zgodnie z corocznie wydawanymi Zarządzeniami Wójta Gminy. Bieżące zmiany ewidencjonowane są w module „Środki trwałe" systemu „PUMA" . W GOPS Janowiec Kościelny, inwentaryzacja sprzętu komputerowego odbywa się na podstawie corocznego spisu z natury zarządzonego przez Głównego Księgowego, dodatkowo na podstawie zarządzenia Nr 12/2017 Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 11 września 2017 roku w sprawie: polityki zarządzania sprzętem i oprogramowaniem komputerowym w Gminnym Ośrodku Pomocy Społecznej w Janowcu Kościelnym. Prowadzone są metryki sprzętu komputerowego przekazanego na stanowiska pracy".*
Zarządzenie Nr 46/2018 Wójta Gminy Janowiec Kościelny z dnia 24 maja 2018 roku w sprawie wprowadzenia polityki ochrony danych w Urzędzie Gminy Janowiec Kościelny określa sposób prowadzenia ewidencji sprzętu i oprogramowania. Ewidencja oprogramowania prowadzona jest w formie elektronicznej lub papierowej.
Zasady inwentaryzacji sprzętu i oprogramowania w GOPS zawarte są w Zarządzeniu Nr

12/2017 Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 11 września 2017 roku w sprawie: polityki zarządzania sprzętem i oprogramowaniem komputerowym w Gminnym Ośrodku Pomocy Społecznej w Janowcu Kościelnym.
Kontrolującemu przedstawiono aktualną (sporządzoną na dzień 24.05.2018 r.) inwentaryzację oprogramowania oraz sprzętu komputerowego. Inwentaryzacja sporządzona została zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja obejmowała rodzaj i konfigurację sprzętu oraz dodatkowo informację dotyczącą użytkownika. Ponadto kontrolującemu okazana została coroczna inwentaryzacja w ramach spisu majątku z natury, w zakresie sprzętu komputerowego.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 142, 277-295, 319-324, 334-335]

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 z*arządzanie 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.

Zasady nadawania zmiany i cofania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy w Janowcu Kościelnym określone są w:

- Zarządzeniu Nr 25/2013 Wójta Gminy Janowiec Kościelny z dnia 19 marca 2013 roku, w sprawie ustalenia „Dokumentacji ochrony danych osobowych w Urzędzie Gminy Janowiec Kościelny”, (uaktualnionej w dniu 15 marca 2016 roku), w rozdziale 6 *Instrukcja zarządzania systemem informatycznym,* zawarto procedurę nadawania uprawnień
- Zarządzeniu Nr 46/2018 Wójta Gminy Janowiec Kościelny z dnia 24 maja 2018 roku, w sprawie wprowadzenia polityki ochrony danych w Urzędzie Gminy Janowiec Kościelny w którym to dokumencie (rozdział 2 i 5) określono nową procedurę nadawania i cofania uprawnień do przetwarzania danych osobowych i pracy w systemach teleinformatycznych,

w związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (…) (RODO). W przedmiotowym zarządzeniu określono nowe wzory wniosków: o nadanie uprawnień (5.3.1), upoważnienia (zał. 5.3.2) oraz ewidencji osób upoważnionych do przetwarzania danych osobowych (zał. 5.3.3).

W Urzędzie Gminy w Janowcu Kościelnym prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych wg. załącznika nr 3 do Zarządzenia Nr 25/2013 Wójta Gminy Janowiec Kościelny z dnia 19 marca 2013 roku, w sprawie ustalenia „Dokumentacji ochrony danych osobowych w Urzędzie Gminy Janowiec Kościelny", (uaktualnionej w dniu 15 marca 2016 roku). 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 upoważnienie do danego systemu teleinformatycznego.

Zasady nadawania zmiany i cofania upoważnień do przetwarzania danych osobowych oraz prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w GOPS w Janowcu Kościelnym określone były Zarządzeniem Nr 13/2017 Administratora Danych Osobowych – Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 11 września 2017 roku, w sprawie zasad ochrony danych osobowych w GOPS w Janowcu Kościelnym. Przedmiotowe zarządzenie wprowadziło do stosowania „*Politykę Bezpieczeństwa przetwarzania danych osobowych w GOPS w Janowcu Kościelnym.*" W dniu 24 maja 2018 r. powyższe zarządzenie w związku z wejściem w życie przepisów RODO, zastąpione zostało Zarządzeniem Nr 6/2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 24 maja 2018 roku w sprawie wprowadzenia polityki ochrony danych w GOPS w Janowcu Kościelnym.
W GOPS w Janowcu Kościelnym prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, ponadto każdy z pracowników, który pracował w systemie teleinformatycznym posiadał stosowne upoważnienie do przetwarzania danych osobowych, jak również upoważnienie do systemu teleinformatycznego.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 118, 133, 246-248, 417, 436-443, 486-507, 508-537]

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 oraz GOPS w Janowcu Kościelnym, zaangażowani w proces przetwarzania informacji, zostali przeszkoleni w przedmiotowej tematyce. Zakres szkolenia obejmował obszary dotyczące podstawowych zasad przetwarzania danych osobowych, prawidłowego gromadzenia i przetwarzania danych osobowych, obowiązków pracownika, w zakresie zasad bezpiecznego przetwarzania danych, zastosowania środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych, postępowania w przypadku naruszenia bezpieczeństwa informacji oraz zgłaszania naruszeń bezpieczeństwa informacji.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 325-329]

2.6. Praca na odległość i mobilne przetwarzanie danych

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

Z wyjaśnienia Wójta Gminy wynika, że: *„W Urzędzie Gminy Janowiec Kościelnym nie są podejmowane działania i nie określono zasad i reguł pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość z uwagi na stacjonarny system pracy. Sprzęt przenośny wykorzystywany jest tylko i wyłącznie w siedzibie Urzędu. Praca zdalna jest tylko do celów serwisowych co opisane jest w pkt 6.7 Polityki Ochrony Danych.*
W GOPS nie przewiduje się pracy zdalnej, jest ona tylko przewidziana dla celów serwisowych co opisane jest w pkt 6.7 polityki ochrony danych. Planuje się natomiast wprowadzenie procedur co do wykorzystywania sprzętu przenośnego przekazanego w ramach projektu emp@tia dla potrzeb pracowników socjalnych tzw. terminale mobilne”.
Zgodnie z Zarządzeniem Nr 25/2013 Wójta Gminy Janowiec Kościelny z dnia 19 marca 2013 roku, w sprawie ustalenia „Dokumentacji ochrony danych osobowych w Urzędzie Gminy Janowiec Kościelny”, (uaktualnionej w dniu 15 marca 2016 roku), w rozdziale *Instrukcja zarządzania systemem informatycznym,* zawarto jedynie zapis (pkt 6.7.5), który stanowi, że *komputery przenośne oraz inne mobilne nośniki danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.*
Przedmiotowe cząstkowe zagadnienie ze względu na wykorzystywanie sprzętu przenośnego tylko w siedzibie jednostki (stacjonarny tryb pracy) nie podlegało ocenie.

[akta kontroli str. 371, 418, 555-559]

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI z*arządzanie 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 oraz GOPS w Janowcu Kościelnym użytkowane są 3 systemy teleinformatyczne do realizacji zadań publicznych zakupione u zewnętrznego dostawcy, tj.: Puma, AW_USC oraz Sygnity. W związku z zakupem ww. systemów podpisane zostały umowy licencyjne z firmami: ZETO SOFTWARE Sp. z o.o., ZETO SA Białystok, Sygnity S.A.

- 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 na opiekę autorską podpisanej z ZETO SA Białystok na użytkowanie programów pod nazwą AW_USC, zawarto zapisy/klauzule dotyczące bezpieczeństwa informacji, w tym zapisy regulujące powierzenie przetwarzania danych osobowych (§4 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 GOPS.

[akta kontroli str. 591-618]

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że z*arządzanie 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 w przypadku Urzędu Gminy w Janowcu Kościelnym został uregulowany Zarządzeniem Nr 46/2018 Wójta Gminy Janowiec Kościelny z dnia 24 maja 2018 roku, w sprawie wprowadzenia polityki ochrony danych w Urzędzie Gminy Janowiec Kościelny.
Sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji w przypadku GOPS w Janowcu Kościelnym został uregulowany Zarządzeniem Nr 6/2018 Kierownika Gminnego Ośrodka Pomocy Społecznej w Janowcu Kościelnym z dnia 24 maja 2018 roku w sprawie wprowadzenia polityki ochrony danych w GOPS w Janowcu Kościelnym.

W badanym okresie nie stwierdzono incydentów naruszenia BI. Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 145, 510]

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI z*arządzanie 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 Urzędzie Gminy robione były audyty (sprawdzenia) procedur zawartych w PBI i SZSI w ramach własnego zasobu kadrowego (ze względu na brak środków finansowych nie zlecano czynności firmom zewnętrznym)…”*

Odnosząc się do powyższych wyjaśnień wskazać należy, iż wymogiem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) jest regularne przeprowadzanie (raz w roku) 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 jego zabezpieczeń.
Urząd Gminy w Janowcu Kościelnym, nie prowadził w okresie objętym kontrolą audytów wewnętrznych w zakresie bezpieczeństwa informacji w systemach informatycznych (§ 20 ust. 2 pkt 14 rozporządzenia KRI), przeprowadzał natomiast cyklicznie sprawdzenia (wewnętrzne) funkcjonowania bezpieczeństwa informacji zgodnie z opracowanym planem sprawdzeń bezpieczeństwa informacji na dany rok, , tj.:

- na rok 2016 zaplanowano i wykonano 3 sprawdzenia,
- na rok 2017 zaplanowano 1 sprawdzenie całoroczne, w ramach którego dokonano 4 sprawdzeń cząstkowych poprawności działania sprzętu komputerowego i serwera,
- na rok 2018 zaplanowano i wykonano 1 sprawdzenie.

Z każdego sprawdzenia sporządzane było sprawozdanie, które obejmowało przedmiot

i zakres sprawdzenia, opis stanu faktycznego stwierdzonego w toku dokonywanych czynności, ewentualne przypadki naruszenia przepisów o ochronie danych osobowych wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem. W wyniku przeprowadzonych sprawdzeń wewnętrznych nie stwierdzono naruszenia przepisów o ochronie danych osobowych.
W wyniku sprawdzenia przeprowadzonego w dniach 01.02-25.05.2018 roku stwierdzono konieczność dostosowania PBI do przepisów 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. Powyższe zalecenie zostało wykonane.
Zgodnie z przyjętym programem kontroli, nieprzeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, stanowi nieprawidłowość. Jednakże, ze względu na prowadzenie w Urzędzie cyklicznych sprawdzeń wewnętrznych w zakresie bezpieczeństwa informacji, będących narzędziem nadzoru nad BI, brak przeprowadzonego audytu uznaje się za uchybienie.
Przyczyną powstania uchybienia było nieprzeprowadzenie audytu wewnętrznego w celu zapewnienia bezpieczeństwa informacji w Urzędzie. Skutkiem było naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI. Intencją ustawodawcy było zobowiązanie podmiotów realizujących zadania publiczne do realizowania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, bez szczegółowego wskazywania na rodzaj audytu oraz tryb jego przeprowadzania. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki. Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

[akta kontroli str. 555-559, 568-590]

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.

Zgodnie z Zarządzeniem Nr 25/2013 Wójta Gminy Janowiec Kościelny z dnia 19 marca 2013 roku, w sprawie ustalenia „Dokumentacji ochrony danych osobowych w Urzędzie Gminy Janowiec Kościelny", (uaktualnionej w dniu 15 marca 2016 roku), w rozdziale *Instrukcja zarządzania systemem informatycznym* zawarto procedurę tworzenia kopii awaryjnych (zapasowych). Zgodnie z zapisami ww. procedury, kopie baz danych gromadzonych na serwerach wykonywane są przez administratora systemu informatycznego, co najmniej raz w tygodniu. Zgodnie z przedstawionym kontrolującemu raportem z wykonywania kopii bezpieczeństwa, w okresie objętym kontrolą kopie awaryjne z poszczególnych systemów wykonywane były raz w tygodniu do dnia 31 maja 2018 r., a od dnia 1 czerwca 2018 r. w cyklu dziennym, w dwóch lokalizacjach - na dysku lokalnym oraz przenośnym.
Ponadto z wyjaśnienia Wójta Gminy wynika, że: „*W Urzędzie Gminy Janowiec Kościelny kopie zapasowe wykonywane są w trybie dobowym i przechowywane są na serwerze i dysku zewnętrznym. Poza tym Urząd Gminy ma podpisane stosowne porozumienie z Warmińsko-Mazurskim Urzędem Marszałkowskim z dnia 02.01.2017 r. na przechowywanie kopii bezpieczeństwa (backup do 2 GB – wykonywane w cyklu dobowym) na serwerze Urzędu Marszałkowskiego oraz Umowę na powierzenie przetwarzanie danych. Kopie baz danych poddawane są okresowej poprawności odtwarzania.*
Gminny Ośrodek pomocy społecznej wykonuje kopie zapasowe baz danych, systemów informatycznym w cyklu dobowym w dni robocze (poniedziałek-piątek). Bazy danych przechowywane są w wyodrębnionym folderze na serwerze sieciowym oraz dodatkowo na zewnętrznym dysku. Poprawność kopii zapasowych weryfikowana jest w trakcie odtwarzania bazy danych w celu jej uporządkowania co jest wymuszane komunikatami systemu".
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 370, 417, 444-485, 555-559]

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.*

Zgodnie z Zarządzeniem Nr 25/2013 Wójta Gminy Janowiec Kościelny z dnia 19 marca 2013 roku, w sprawie ustalenia „Dokumentacji ochrony danych osobowych w Urzędzie Gminy Janowiec Kościelny", (uaktualnionej w dniu 15 marca 2016 roku), w rozdziale *Instrukcja zarządzania systemem informatycznym* zawarto procedurę przeprowadzania 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 (Administrator Sytemu Informatycznego). Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Informatyk (ASI).

Przeglądów i konserwacji zbioru danych osobowych mogą dokonywać jedynie osoby posiadające upoważnienie Administratora Danych Osobowych. W przypadku korzystania z zewnętrznej firmy serwisującej, przegląd i konserwacja zbioru danych odbywa się pod nadzorem Informatyka (ASI).

W okresie objętym kontrolą nie zidentyfikowano w Urzędzie Gminy oraz GOPS w Janowcu Kościelnym 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. 25, 420]

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.

W Urzędzie Gminy Janowiec Kościelny stosowane są zabezpieczenia typu:

- sieć wewnętrzna LAN na styku z siecią WAN (Internet) zabezpieczona jest FireWall sprzętowym UTM, którego polityki bezpieczeństwa filtrują (monitorują) cały ruch sieciowy w tym pocztę e-mail, ograniczają dostęp do stron www z niepożądaną treścią itp.
- zarówno na serwerze jak i komputerach stacjonarnych zainstalowany jest program antywirusowy „*Eset Endpoint Security”*, wprowadzono system haseł (do uruchomienia systemu operacyjnego, do uruchomienia aplikacji narzędziowej – hasła regularnie są zmieniane), pracownicy logują się na konta z prawami użytkownika,
- zastosowano zasilacze awaryjne UPS,
- wykonywane są kopie zapasowe danych.

W GOPS stosowane są zabezpieczenia typu:

- sieć LAN na styku z siecią WAN zabezpieczona urządzeniem UTM, którego polityki bezpieczeństwa filtrują wszystkie przechodzące pakiety, w tym sprawdzana jest poczta elektroniczna,
- komputery stacjonarne dodatkowo zabezpieczone są programem antywirusowym i systemem trzech haseł (do uruchomienia komputera, do uruchomienia systemu operacyjnego, do uruchomienia aplikacji narzędziowej – hasła regularnie są zmieniane),
- wykonywane są kopie zapasowe danych.

Powyższe zostało sprawdzone przez kontrolującego na 3 stacjach roboczych (w tym 1 w GOPS) obsługujących systemy informatyczne służące do realizacji zadań publicznych.
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 555-559]

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.*

W punkcie 2.12 wykazano stosowane mechanizmy jakie jednostki kontrolowane (UG i GOPS), zastosowały w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Odbywa się to również poprzez: działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp oraz kontrolę dostępu do systemów operacyjnych. W systemach: PUMA, Sygnity, CEIDG, AW_USC logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga okresowej wymiany. W systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe.

Oprócz zabezpieczeń systemów teleinformatycznych wykazanych w punkcie 2.12, zarówno

Urząd gminy jak i GOPS w Janowcu Kościelnym stosują fizyczne zabezpieczenia na wypadek próby dostępu do danych przetwarzanych przez systemy.
Urząd Gminy zapewnia fizyczne bezpieczeństwo przetwarzanych informacji, m.in. poprzez:
- zainstalowanie zabezpieczenia alarmowego -– podpisano stosowne umowy na obsługę systemu alarmowego i jego konserwację,
- objęcie z zewnątrz budynku monitoringiem wizyjnym,
- wydzielone zostało pomieszczenie serwerowni do którego mają dostęp tylko upoważnieni pracownicy,
- zainstalowanie elektronicznego systemu alarmowego wewnątrz budynku,
- zamykanie na klucz pokoi, w których przetwarzane są informacje, każdorazowo przy opuszczeniu przez pracownika stanowiska pracy,
- kontrolę dysponowania kluczami do pomieszczeń.

GOPS zapewnia fizyczne bezpieczeństwo przetwarzanych informacji, m.in. poprzez:
- zainstalowanie zabezpieczenia alarmowego -– podpisano stosowne umowy na obsługę systemu alarmowego i jego konserwację,
- zamykanie na klucz pokoi, w których przetwarzane są informacje, każdorazowo przy opuszczeniu przez pracownika stanowiska pracy,
- kontrolę dysponowania kluczami do pomieszczeń,
- pomieszczenia, w których przetwarzane są dane zabezpieczone są drzwiami z dwoma zamkami, dodatkowo pomieszczenie gdzie znajduje się serwer wyposażone jest w kraty w oknach.

Bezpieczeństwo działania systemów teleinformatycznych realizowane jest również poprzez okresową aktualizację oprogramowania w zakresie działania poszczególnych systemów do najnowszych wersji.

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Gminy w Janowcu Kościelnym. W wyniku oględzin stwierdzono, że pomieszczenie posiada zainstalowane urządzenie klimatyzujące oraz urządzenia monitorujące parametry środowiskowe (temperatura i wilgotność). W pomieszczeniu znajduje się czujka alarmowa (reagująca na ruch wewnątrz) oraz czujka dymna generująca sygnał dźwiękowy, w przypadku zadymienia pomieszczenia. Wejście do pomieszczenia posiada obite blachą drzwi, w których zainstalowano dwa zamki. Główny budynek urzędu posiada zabezpieczenie alarmowe, co potwierdza dokumentacja z przeprowadzonych oględzin.
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 538-547, 555-559]

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 Systemy dziedzinowe użytkowane w Urzędzie Gminy posiadają mechanizmy rejestracji logów, jest to prezentacja logów wszystkich operacji w systemie, w tym informacji o logowaniu i wylogowaniu. Logi w modułach są przechowywane bezterminowo, są usuwane tylko jeżeli usuwany jest dany obiekt.
W przypadku rozliczalności działań w systemach informatycznych GOPS, podczas wykonywania kopii zapasowych kopiowane są również logi systemu o działaniach użytkownika jak również o błędach jakie wystąpiły w działaniu samego systemu.
Mając na uwadze powyższe wyjaśnienia przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 555-559]

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 Janowcu Kościelnym, 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 5 błędów, w przypadku strony BIP walidacja wykazała 4 błędy. 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.

Strona internetowa www Urzędu zawierała elementy umożliwiające zmianę wielkości czcionki, natomiast strona BIP Urzędu zawierała elementy umożliwiające zmianę kontrastu oraz wielkości czcionki. Dostosowanie zostało wykonane z możliwością zmiany kontrastu oraz kilku rozmiarów czcionki, za pomocą ikony (wersja wysokokontrastowa) oraz (A+ A-) umieszczonej w prawym górnym rogu w przypadku strony www oraz lewym górnym rogu w przypadku strony BIP. Powyższe zagadnienie oceniono pozytywnie.

[akta kontroli str. 548-552]

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

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

2. Przeprowadzanie audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, przez firmę zewnętrzną lub w oparciu o własny zasób kadrowy.

Proszę Panią Wójt o podjęcie działań mających na celu usunięcie stwierdzonych uchybień oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 14 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

Do wiadomości:
- Kierownik GOPS
  w Janowcu Kościelnym.