WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 28 listopada 2019 r.

FK-IV.431.39.2019

**Szanowny Pan**
**Bohdan Mohyła**
**Wójt Gminy Pozezdrze**
**ul. 1 Maja 1a**
**11-610 Pozezdrze**

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 Pozezdrzu, ul. 1 Maja 1a, 11-610 Pozezdrze, NIP: 8451006919, REGON: 000538320.

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

1. **Pan Bohdan Mohyła** - Wójt wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 30.11.2014 oraz 21.10.2018 - (*kierownik jednostki kontrolowanej).*
2. **Pani Krystyna Piotrowska** - Sekretarz, powołana na stanowisko w dniu 23 kwietnia 2007 Uchwałą nr IX/43/07 Rady Gminy w Pozezdrzu w sprawie powołania Sekretarza Gminy, pełniąca funkcję do 26 lutego 2018 roku.
3. **Pani Agnieszka Wierzchowska** – Sekretarz, zatrudniona na podstawie umowy o pracę od dnia 1 czerwca 2015 roku, pełniąca funkcję Sekretarza od 1 marca 2018 roku (porozumienie stron zmieniające warunki pracy i płacy z dnia 27 lutego 2018 roku) *(nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą).*
4. **Pan Krzysztof Dłuski** - Starszy Informatyk, zatrudniony na podstawie umowy o pracę od dnia 6 lipca 2004 roku *(realizujący zadania objęte kontrolą)*.

*[akta kontroli str. 52]*

Kontrolę przeprowadził pracownik Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie, Radosław Gazda – inspektor wojewódzki; legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.993.2019 z 16 października 2019 r., wydanego przez Wojewodę

Warmińsko-Mazurskiego.

*[akta kontroli str. 51]*

Kontrolę przeprowadzono w dniach 23-25 października 2019 r., co zostało odnotowane w książce kontroli Urzędu Gminy Pozezdrze pod pozycją Nr 10/2019.

Przedmiotem kontroli była ocena działania 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 (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r. oraz Dz.U. z 2019 r. poz. 700 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2018 r. do dnia 23 października 2019 r. (dzień rozpoczęcia czynności kontrolnych).

*[akta kontroli str. 1, 32, 51]*

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 (Dz. U. z 2019 r., poz. 1464) 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 (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r. oraz Dz.U. z 2019 r. poz. 700 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), 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, 32, 51]*

W czasie trwania czynności kontrolnych informacji i wyjaśnień udzielał Starszy Informatyk Urzędu Gminy Pozezdrze - upoważniony przez Wójta Gminy.

*[akta kontroli str. 53]*

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z uchybieniami.**

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

Z informacji przekazanych przez UG Pozezdrze przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **3** systemy teleinformatyczne (Źródło - 2 moduły, PUMA – 2 moduły, CEIDG).

**Systemy teleinformatyczne wykorzystywane w Urzędzie Gminy Pozezdrze:**

1) **ŹRÓDŁO** – (**Rejestr PESEL**, **Rejestr dowodów osobistych, USC**) 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).

2) **PUMA - Moduł Ewidencja Ludności** posiada homologację MSW, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę 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 prowadzenie i aktualizację rejestru wyborców, sporządzanie spisów wyborców uprawnionych do udziału w wyborach i referendum, pozwala na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców mieście na podstawie bazy danych ewidencyjnych.

3) **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 gospodarczej. Służy również do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.

Zgodnie z Uchwałą Nr XXIII/124/12 Rady Gminy w Pozezdrzu z dnia 26 listopada 2012 r. w sprawie zmiany uchwały o utworzeniu związku międzygminnego i przyjęcia jego statutu, Mazurski Związek Międzygminny – Gospodarka Odpadami, zobowiązany jest do prowadzenia rejestru 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 2018 r., poz. 1454 ze zm.).

*[akta kontroli str. 63-65]*

## 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 Pozezdrze posiada aktywną Elektroniczną Skrzynkę Podawczą **/Pozezdrze_ug/SkrytkaESP** znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie pism w formie dokumentów elektronicznych. Adres elektronicznej skrzynki podawczej: https://epuap.gov.pl/wps/portal/strefa-urzednika/katalog-spraw/profil-urzedu/pozezdrze_ug

Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu, w lewym panelu ekranu w zakładce Menu przedmiotowe – Elektroniczna skrzynka podawcza – Cyfrowy Urząd. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: doc, rtf, docx, odt, xls, xlsx, ods, txt, gif, tif, bmp, jpg, pdf.

Urząd Gminy Pozezdrze w związku z posiadaniem aktywnej Elektronicznej Skrzynki Podawczej udostępniał oraz świadczył usługę elektroniczną, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego". Usługa pismo ogólne przeznaczone jest do tworzenia pism w postaci elektronicznej wnoszonych za pomocą elektronicznej skrzynki podawczej lub doręczanych przez podmioty publiczne za potwierdzeniem doręczenia, w przypadkach gdy łącznie spełnione są następujące warunki:

- organ administracji publicznej nie określił wzoru dokumentu elektronicznego umożliwiającego załatwienie danej sprawy,
- przepisy prawa nie wskazują jednoznacznie, że jedynym skutecznym sposobem przekazania informacji jest jej doręczenie w postaci papierowej.

W zakresie publikacji procedur załatwiania spraw (drogą elektroniczną) realizowanych przez Urząd należy stwierdzić, iż UG Pozezdrze nie świadczył usług związanych

z załatwianiem spraw od początku do końca w formie elektronicznej. Na stronie BIP Urzędu Menu przedmiotowe istnieje zakładka „Wykaz spraw" w której opisano obowiązujące procedury stosowane przez Urząd przy załatwianiu poszczególnych spraw będących w kompetencjach poszczególnych stanowisk.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 80-82]*

**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 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. Potwierdzenie powyższego znajduje również odzwierciedlenie w wyjaśnieniach uzyskanych z Urzędu, cyt.: *„Gmina Pozezdrze nie przekazywała do centralnego repozytorium żadnych wzorów dokumentów. Urząd korzysta za pośrednictwem platformy EPUAP z podstawowego formularza „Pismo ogólne do urzędu" oraz formularzy umieszczonych w centralnym repozytorium, m. in.:*

a. *Dowody osobiste – obywatel.gov.pl*
b. *Ochrona przed bezdomnymi zwierzętami – epuap.gov.pl*
c. *Przyjmowanie petycji – epuap.gov.pl*
d. *Przyjmowanie skarg i wniosków – epuap.gov.pl*
e. *Udostępnienie danych w trybie jednostkowym z rej. D.O. – epuap.gov.pl*

*f. Udostępnienie danych z ewidencji ludności – epuap.gov.pl*
*g. Zezwolenie na świadczenie usług z zakresie opróżniania zbiorników bezodpływowych - epuap.gov.pl*
*h. Uzyskanie dofinansowania do kosztów usuwania azbestu – epuap*
*i. Wniosek o udostępnienie informacji publicznej – epuap.gov.pl*
*j. Wniosek o wpisanie w rejestr wyborców – obywatel.gov.pl*
*k. Wniosek o wydanie decyzji o warunkach zabudowy – epuap.gov.pl*
*l. Wniosek o wydanie odpisu danych z rejestru D.O. – epuap.gov.pl*
*m. Wniosek o wydanie zaświadczenia o przeznaczeniu nieruchomości – epuap.gov.pl*
*n. Wydanie zaświadczeń – epupa.gov.pl*
*o. Zaświadczenia – epupa.gov.pl."*

Jednocześnie należy zaznaczyć, iż na stronie BIP kontrolowanego Urzędu w zakładce „Wykaz spraw", opublikowano w wersji „do pobrania" formularzy niektórych wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 77, 81-85]*

### 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://pozezdrze.pl/, a strona internetowa BIP Urzędu – pod adresem http://bip.pozezdrze.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu w górnej części panelu strony. Na stronie głównej BIP Urzędu, zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.
Ponadto na stronie internetowej UG i BIP UG, znajdują się linki do najważniejszych serwisów internetowych ułatwiających odbiorcy internetowemu załatwienie podstawowych spraw urzędowych, tj.:

– **OBYWATEL.GOV.PL**, który powstał jako część programu pl.ID, realizowanego w ramach Programu Operacyjnego Innowacyjna Gospodarka (7. Oś priorytetowa – Społeczeństwo informacyjne – budowa elektronicznej administracji) i współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego. Znajduje się tu kilkaset najpopularniejszych usług świadczonych przez administrację publiczną.
– **CEiDG** - Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG) – jest to rejestr przedsiębiorców, którzy są osobami fizycznymi, działającymi na terenie Polski. Rejestr prowadzony jest w formie systemu teleinformatycznego przez ministra właściwego do spraw gospodarki. Rejestracja w CEIDG jest bezpłatna. Wpisowi do ewidencji podlegają przedsiębiorcy będący osobami fizycznymi. Przedsiębiorca może

podjąć działalność gospodarczą w dniu złożenia wniosku o wpis do CEIDG albo po uzyskaniu wpisu do rejestru przedsiębiorców w Krajowym Rejestrze Sądowym (KRS). Wpis dokonywany jest nie później, niż następnego dnia roboczego po dniu wpływu do CEIDG poprawnego wniosku. Zaświadczeniem o wpisie do CEIDG jest wydruk ze strony internetowej CEIDG.

- **BIZNES.GOV.PL** - to serwis przeznaczony dla osób zamierzających rozpocząć i prowadzących działalność gospodarczą. Celem portalu jest pomoc w realizacji spraw związanych z zakładaniem i prowadzeniem działalności oraz uproszczenie formalności niezbędnych do założenia i prowadzenia firmy. W serwisie dostępne są opisy urzędowych usług oraz gotowe formularze. Za pomocą serwisu, osoby prowadzące firmę mogą składać wnioski do instytucji państwowych drogą elektroniczną, a także załatwiać swoje biznesowe sprawy przez Internet. Serwis łączy w sobie wiele usług i funkcji nie tylko dla przedsiębiorców, ale także dla administracji państwowej. Przedsiębiorcy znajdą tutaj szczegółowe informacje o obowiązujących przepisach prawa, wymaganych procedurach i formalnościach związanych z zakładaniem i prowadzeniem działalności gospodarczej w Polsce oraz w całej Unii Europejskiej.
- **ePUPAP -** elektroniczna skrzynka podawcza znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie pism w formie dokumentów elektronicznych.

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt, iż instytucja ta nie świadczyły usług elektronicznych na zewnątrz za pomocą systemów teleinformatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej, w związku z powyższym przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

*[akta kontroli str. 86-88]*

### 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 systemy teleinformatyczne zainstalowane i użytkowane w Urzędzie Gminy współpracują z systemami zewnętrznymi w następujących zakresach, cyt.: „*System PUMA posiada wymianę informacji ze ŹRÓDŁEM. Wymiana jest możliwa dzięki wyposażeniu w odpowiedni sprzęt przez MSWiA do transmisji danych po łączu dedykowanym DSL. Transmisja odbywa się przez router Cisco 1800 i modem Wasco SHDSL z szyfrowaniem danych. Wymiana informacji między PUMĄ a Źródłem odbywa się przez odizolowaną sieć wewnętrzną przygotowaną wg zaleceń MSWiA. Logowanie użytkowników do systemu odbywa przy pomocy kart kryptograficznych z dedykowanymi certyfikatami.”*
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 77]*

### 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.*

Zgodnie z zarządzeniem Nr 12/16 Wójta Gminy Pozezdrze z dnia 3 lutego 2016 r. w sprawie wykonywania czynności kancelaryjnych i podpisywania dokumentów w Urzędzie Gminy w Pozezdrzu, podstawowym systemem wykonywania czynności kancelaryjnych dla dokumentowania przebiegu sprawy i rozstrzygania sprawy w Urzędzie Gminy w Pozezdrzu wskazano system tradycyjny, który umożliwia wykonywanie czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci nieelektronicznej, z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentacji w tej postaci. Sposób postępowania z korespondencją wpływającą do Urzędu w formie elektronicznej za pośrednictwem mailowej skrzynki pocztowej oraz e-PUAP zawarto w §6 ust. 1 pkt 5 zarządzenia.
Jednocześnie, w okazanej dokumentacji Urzędu brak jest procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wypływających z Urzędu drogą elektroniczną (skrzynka na platformie ePUAP – dokumenty opatrzone podpisem elektronicznym), co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie, m.in. zabezpieczenia

informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Powyższe stanowi uchybienie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

*[akta kontroli str. 89-94]*

**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 przekazanych przez Sekretarza Gminy Pozezdrze wynika, że cyt*.: „System PUMA jest zasilany bezpośrednio z systemu ŹRÓDŁO za pomocą aplikacji narzędziowej dostarczonej przez producenta PUMY ZETO Software. Pobieranie danych Format przekazywanych danych to XML w kodowaniu Unicode UTF-8. Systemy informatyczne są przygotowane do przyjmowania elektronicznych dokumentów w formatach określonych w załączniku do KRI tj: xml, pdf, txt, rtf, odt, doc."*
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 77]*

## 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 285/13 Wójta Gminy Pozezdrze z dnia 25 marca 2013 r. wdrożono dokumentację przetwarzania i ochrony danych osobowych w Urzędzie Gminy Pozezdrze,

Zarządzenie wprowadzono zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2002 r., 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). Powyższa dokumentacja, a w szczególności Instrukcja Zarządzania Systemem Informatycznym w Urzędzie, stanowiły dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (…). Służyła ona zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

*[akta kontroli str. 95-135]*

- Zarządzeniem Nr 154/17 Wójta Gminy Pozezdrze z dnia 29 grudnia 2017 r. zmieniono

zarządzenie wdrażające dokumentację przetwarzania i ochrony danych osobowych w Urzędzie Gminy Pozezdrze,

- Zarządzeniem Nr 3/19 Wójta Gminy Pozezdrze z dnia 10 stycznia 2019 r. wprowadzono „Politykę Bezpieczeństwa Informacji" w Urzędzie Gminy Pozezdrze,
- W wyniku weryfikacji przyjętej wcześniej Polityki, zarządzeniem Nr 117/19 Wójta Gminy Pozezdrze z dnia 12 września 2019 r., wprowadzono do stosowania Politykę Ochrony Danych Urzędu Gminy w Pozezdrzu.

Polityka Ochrony Danych sporządzono na podstawie obowiązujących przepisów prawa, tj. 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) – zwanego dalej „RODO". Dokumentacja w zakresie ochrony danych dotyczyła 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 danych osobowych.

*[akta kontroli str. 136-315]*

- Zarządzeniem Nr 68/15 Wójta Gminy Pozezdrze z dnia 8 maja 2015 r. powołano Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Pozezdrze.
- W Urzędzie Gminy w Pozezdrzu wyznaczono Inspektora Ochrony Danych i podpisano umowę z firmą zewnętrzną na świadczenie takich usług.

*[akta kontroli str. 316-326]*

Jednocześnie należy zaznaczyć, że pracownik odpowiedzialny za realizację zadania objętego kontrolą, przeprowadził w 2018 roku 5 sprawdzeń, a w 2019 r. 11 sprawdzeń podatności systemu informatycznego w zakresie bezpieczeństwa danych osobowych.

*[akta kontroli str. 327-376]*

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 117/19 Wójta Gminy Pozezdrze z dnia 12 września 2019 r., wprowadzono do stosowania Politykę Ochrony Danych Urzędu Gminy w Pozezdrzu, skuteczne zarządzanie ryzykiem w obszarze bezpieczeństwa ochrony danych wymaga od przyjętej metody liczenia ryzyka spełnienia następujących warunków:

- zapewnienia powtarzalności i porównywalności wyników,
- uwzględnienia stopnia wrażliwości informacji,
- uwzględnienia prawdopodobieństwa wystąpienia zdarzenia (zagrożenia) i konsekwencji jego realizacji (skutków),
- uwzględnienia efektywności funkcjonujących zabezpieczeń, wpływających na prawdopodobieństwo zajścia zdarzeń, jak i na późniejsze ewentualne konsekwencje ich realizacji.

Zidentyfikowane i oceniane ryzyka o określonym stopniu istotności zostają zarejestrowane i udokumentowane na kartach oceny ryzyka i podlegają bieżącej ocenie i monitorowaniu. Na karcie ryzyka dokumentuje się również sposoby postępowania z ryzykiem, zadania mające na celu obniżenie ryzyka. Przyjęto, że ponowna ocena zidentyfikowanego ryzyka nie może być rzadsza niż raz na 12 miesięcy.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI, jak również przyjętej w Urzędzie Polityce Ochrony Danych (Rozdział III), w dniu 24 maja 2018 roku przeprowadzana była w Urzędzie analiza ryzyka bezpieczeństwa informacji. Mając powyższe na uwadze obowiązek wynikający z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz przyjętej w Urzędzie Polityce Ochrony Danych (Rozdział III) w przypadku 2018 roku został spełniony. W 2019 roku zgodnie z wyjaśnieniem Sekretarza Gminy Pozezdrze, ponowne oszacowanie ryzyka przeprowadzone zostanie w Urzędzie w miesiącu listopadzie.

*[akta kontroli str. 77, 244-269, 377-397]*

Jednocześnie należy wskazać, iż w jednostce prowadzony jest rejestr czynności przetwarzania danych osobowych zgodnie z RODO.

*[akta kontroli str. 398-402]*

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

### 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.*

Kontrolującemu przedstawiono aktualną inwentaryzację sprzętu komputerowego użytkowanego w Urzędzie Gminy w Pozezdrzu sporządzoną zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja obejmowała miedzy innymi rodzaj i konfigurację sprzętu, prowadzona była w programie „Ewidencja Sprzętu Komputerowego i Oprogramowania dla przedsiębiorstw i instytucji publicznych" wersja 1.9.0 z 2007 roku. Producentem oprogramowania jest RHO Software ul. Morawskiego 5 Kraków.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 403-413]*

## 2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI *zarządzanie 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.

Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz do pracy w systemie informatycznym określone zostały zarządzeniem Nr 117/19 Wójta Gminy Pozezdrze z dnia 12 września 2019 r., wprowadzającym do stosowania Politykę Ochrony Danych Urzędu Gminy w Pozezdrzu, zgodnie z zarządzeniem:

- **upoważnienia do przetwarzania danych osobowych**

Kierujący (sekretarz, pracownik kadr, kierownik referatu) na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych – w tym danych osobowych składa do IOD wniosek o wydanie upoważnienia do przetwarzania danych osobowych i dostępu do systemu informatycznego. Wniosek musi zawierać:

- imię, nazwisko i osoby, której upoważnienie zostanie nadane,
- zakres upoważnienia do przetwarzania danych osobowych,
- nazwę systemów informatycznych, do których upoważniony ma mieć dostęp;
- datę, z jaką upoważnienie ma być nadane,
- okres obowiązywania upoważnienia.

Ponadto wniosek wskazuje jaki poziom dostępu powinien mieć upoważniony do systemów i

zasobów teleinformatycznych. Wniosek powinien być przygotowany w porozumieniu z ASI, który nadaje identyfikatory użytkownika w systemach i odpowiednie uprawnienia, wskazane przez kierującego. Osoba, która ma zostać dopuszczona do przetwarzania danych musi zostać zapoznana z wymogami przepisów z zakresu ochrony danych osobowych i Polityką Ochrony Danych. Po zrealizowaniu wniosku (wydanie upoważnień, nadanie uprawnień itp.), co jest potwierdzane podpisami ze strony IOD oraz ASI wniosek pełni funkcję karty zasobów, uprawnień. Razem z upoważnieniem do przetwarzania danych osobowych podpisywane jest przez upoważnianego pracownika oświadczenie o zachowaniu tajemnicy, poufności, znajomości polityk i innych warunkach związanych z bezpieczeństwem informacji. Na podstawie zrealizowanego wniosku ASI przekazuje upoważnionemu dostęp do wskazanych zasobów.

- **upoważnienia do pracy w systemach informatycznych**

1) Dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu).
2) Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne.
3) Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na polecenie przełożonych (lub innych osób upoważnionych).
4) Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada informatyk.
5) Powyższą procedurę wykonuje się w przypadku: wniosku o wydanie sprzętu, zgłoszenia zbioru DO, powierzenia DO, upoważnienia do przetwarzania DO, nadania uprawnień, instalacji oprogramowani
6) Obowiązuje zasada minimalizacji uprawnień.
7) Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
8) Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.
9) W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. "root" lub "administrator") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
10) Stosowany jest system uwierzytelniania: login i hasło.

*[akta kontroli str. 254-257, 313]*

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych. Pracownikom posługującym się systemem teleinformatycznym wydane zostały stosowne upoważnienia do pracy w określonym systemie. W Urzędzie prowadzona była również

ewidencja wydanych upoważnień w zakresie dostępu do pracy w systemach informatycznych.

*[akta kontroli str. 414-482]*

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji**

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że z*arządzanie 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 okresie objętym kontrolą pracownicy Urzędu Gminy w Pozezdrzu uczestniczący w procesie przetwarzania danych brali udział w 2 szkoleniach, w zakresie zdobycia wiedzy i umiejętności dotyczących ochrony danych osobowych:

- w dniu 25 maja 2018 r. Starszy Informatyk Urzędu Gminy w Pozezdrzu przeprowadził szkolenie dotyczące „Ochrony danych osobowych”,
- w dniu 21 lutego 2019 r. Starszy Informatyk Urzędu Gminy w Pozezdrzu przeprowadził szkolenie dotyczące „Polityki Bezpieczeństwa Informacji”.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 483-503]*

**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.*

W zarządzeniu Nr 117/19 Wójta Gminy Pozezdrze z dnia 12 września 2019 r., wprowadzającym do stosowania Politykę Ochrony Danych Urzędu Gminy w Pozezdrzu, określony został regulamin użytkowania komputerów przenośnych, zgodnie z którym:

1) W przypadku przechowywania na komputerze przenośnym danych w szczególności danych osobowych lub stanowiących tajemnicę Urzędu, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym (włączona funkcja BitLocker), zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
2) Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Urzędu.

3) W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za bezpieczeństwo teleinformatyczne i ochronę danych, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
4) Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu.
5) W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, itp.
6) W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach
7) Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
8) Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Z uzyskanych z Urzędu Gminy informacji wynika, że sprzęt przenośny wykorzystywany jest tylko i wyłącznie w siedzibie Urzędu (tryb stacjonarny).

*[akta kontroli str. 25, 312]*

Przedmiotowe cząstkowe zagadnienie ze względu na wykorzystywanie sprzętu w zakresie systemów teleinformatycznych tylko w siedzibie jednostki (stacjonarny tryb pracy) nie podlegało ocenie.

## 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 Pozezdrzu użytkowany jest 1 system teleinformatyczny do realizacji zadań publicznych (składający się z dwóch modułów) zakupiony u zewnętrznego dostawcy, tj.: PUMA. W związku z zakupem ww. systemu podpisana zostały z firmą ZETO

SOFTWARE Sp. z o.o. w Olsztynie umowy: licencyjna (opieka autorska JU/1086/17, 18/1356/ZU) oraz umowa powierzenia przetwarzania danych osobowych (18/0287/ZU).

W treści umowy powierzenia przetwarzania danych osobowych zawartej z firmą dostarczającą system informatyczny PUMA, umieszczono zapisy w zakresie powierzenia danych, gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawców w związku z realizacją umowy.

*[akta kontroli str. 504-521]*

Zgodnie z zarządzeniem Nr 117/19 Wójta Gminy Pozezdrze z dnia 12 września 2019 r., wprowadzającym do stosowania Politykę Ochrony Danych Urzędu Gminy w Pozezdrzu informatyk odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email oraz odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia. W przypadku napraw dokonywanych na zewnątrz z komputerów należy uprzednio wymontować dyski i wszelkie nośniki. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site). Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

*[akta kontroli str. 313-314]*

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## 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.*

Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych została uregulowana zarządzeniem Nr 117/19 Wójta Gminy Pozezdrze z dnia 12 września 2019 r.,

wprowadzającym do stosowania Politykę Ochrony Danych Urzędu Gminy w Pozezdrzu (Rozdział IV, Rozdział V-pkt 6).
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 270-272, 275]*

**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.*

W okresie objętym kontrolą tj. od 1 stycznia 2018 rok do dnia rozpoczęcia czynności kontrolnych (23 października 2019 r.) przeprowadzono w kontrolowanej jednostce dwa zadania audytowe obejmujące audyt wewnętrzny bezpieczeństwa informacji oraz audyt wewnętrzny infrastruktury IT. Czynności sprawdzające prowadzone były na przełomie styczeń/marzec 2018 r. oraz maj 2018 r.

*[akta kontroli str. 534-579]*

Mając powyższe na uwadze należy stwierdzić, że dopełniono w 2018 roku obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI oraz Polityki Ochrony Danych, który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Jednocześnie należy zaznaczyć, iż zgodnie z załącznikiem nr 17 (Procedura audytu), do zarządzenie Nr 154/17 Wójta Gminy Pozezdrze z dnia 29 grudnia 2017 r. zmieniającego zarządzenie wdrażające dokumentację przetwarzania i ochrony danych osobowych w Urzędzie Gminy Pozezdrze, celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

*[akta kontroli str. 161]*

W 2018 roku obydwa zadania audytowe przeprowadził pracownik Urzędu Gminy - Starszy Informatyk, który opracował dokumentację stanowiącą (w okresie prowadzenia zadań audytowych) system zarządzania bezpieczeństwem informacji w jednostce tj.:

- Zarządzenie Nr 285/13 Wójta Gminy Pozezdrze z dnia 25 marca 2013 r. wdrażające dokumentację przetwarzania i ochrony danych osobowych w Urzędzie Gminy Pozezdrze (Politykę Bezpieczeństwa Przetwarzania Danych Osobowych),
- Zarządzenie Nr 154/17 Wójta Gminy Pozezdrze z dnia 29 grudnia 2017 r. zmieniające zarządzenie wdrażające dokumentację przetwarzania i ochrony danych osobowych w Urzędzie Gminy Pozezdrze (obowiązujące do 10 stycznia 2019),

jak również w czasie prowadzonych czynności audytowych pełnił funkcję Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Pozezdrzu. W powyższej sytuacji osoba przeprowadzająca zadania audytowe – audytowała własną pracę, co jest sprzeczne z zapisami przyjętej w Urzędzie Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.
Powyższe stanowi uchybienie. Osobą odpowiedzialną za powstanie uchybienia jest Kierownik kontrolowanej jednostki.
Przedmiotowe cząstkowe zagadnienie w przypadku 2018 r. ocenia się pozytywnie z uchybieniami.

W przypadku 2019 roku zaznaczyć należy, że do dnia kontroli (23.10.2019) wymagany roczny audyt bezpieczeństwa informacji nie został przeprowadzony. Wobec powyższego dopełnienie obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, w przypadku roku 2019 nie podlegało ocenie, ze względu na istniejącą możliwość przeprowadzenia przez jednostkę audytu bezpieczeństwa informacji do końca 2019 roku. Z informacji uzyskanych z Urzędu Gminy wynika, że audyt wewnętrzny bezpieczeństwa informacji w 2019 roku przeprowadzony zostanie w listopadzie br.

*[akta kontroli str. 77]*

## 2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że *zarządzanie 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.

Zasady tworzenia i przechowywania kopii zapasowych uregulowane zostały zarządzeniem Nr 117/19 Wójta Gminy Pozezdrze z dnia 12 września 2019 r., wprowadzającym do stosowania Politykę Ochrony Danych Urzędu Gminy w Pozezdrzu (Rozdział II pkt 5-6).

Kontrolującemu udostępniono opracowany schemat tworzenia kopii zapasowych.
Zgodnie z wyjaśnieniem Sekretarza Gminy Pozezdrze cyt.: *„W Urzędzie podstawowym systemem backupu jest oprogramowanie „Veeam Backup& Replication" w wersji 9.5. Oprogramowanie zainstalowane jest na wirtualnym serwerze Windows Server 2016. Zadaniem oprogramowania Veeam jest robienie kopii bezpieczeństwa całych serwerów wirtualnych. Do backupu serwery wirtualne urzędu pogrupowane są na 2 grupy wg*

*przeznaczenia: grupa 1 kopia robiona w tzw. trybie bez wyciszenia serwerów a grupa 2 są to serwery wymagające tzw. wyciszenia (zawierające bazy danych).*
*Kopie bezpieczeństwa robione są w określonym harmonogramie:*

1. *kopie dzienne, robione codzienne o godzinie 20:00 (grupa 1) i 22:00 (grupa 2) – przechowujemy 14 kopii inkrementalnych, co 7 kopia jest kopia całościową – kopie przechowywane są na wydzielonym miejscu macierzy w UG Pozezdrze.*
2. *kopie tygodniowe, robione są codziennie inkrementalnie z co 7 kopią pełną. Przechowywane są 4 kolejne kopie pełne. Kopie przechowywane są w dedykowanej chmurze z lokalizowanej w Łodzi, transfer odbywa się w trakcie robienia kopii (mamy redutancję łącza – światłowodowe i LTE).*
3. *kopie miesięczne – kopie robione na koniec miesiąca na tzw. tasiemkach w Łodzi i dostarczane są do Urzędu Gminy w Giżycku (gdzie umieszczone są w sejfie).*

*Sprawdzenie kopii bezpieczeństwa odbywa się poprzez rozpakowanie wybranej kopii w specjalnym testowym środowisku programu Veeam. Pozwala to ocenić poprawność wykonanej kopii całego systemu. Dodatkowo sprawdzana jest kopia baz danych programów: KP, Kadry, Podatki, Płatnik, PUMA i Besti@. W tym przypadku wypakowuję tylko plik bazy danych i podłącza do testowego oprogramowania".*

*[akta kontroli str. 78, 522-523, 529-533]*

Jednocześnie kontrolujący (na podstawie udostępnionej dokumentacji) stwierdził, że w Urzędzie Gminy są wykonywane testy w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenie przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu.

*[akta kontroli str. 524-528]*

Regularne testowanie jakości kopii zapasowych poprzez odtworzenie systemu informatycznego z kopii zwykle na niezależnym od środowiska produkcyjnego sprzętowym środowisku testowym oraz testowanie pracy użytkowej odtworzonego systemu jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęłaby podstawowy ośrodek przetwarzania danych.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

## 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.*

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej dzieliły się na systemy centralne tj. ŹRÓDŁO i CEiDG oraz system wspierający zakupiony u dostawcy zewnętrznego - PUMA. Na obsługę aktualnie zainstalowanego oprogramowania z firmą dostarczającą system informatyczny zawarto stosowną umowę licencyjną (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. System teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.
Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 504-513]*

**2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji**

Z § 20 ust. 2 rozporządzenia KRI wynika, że *zarządzanie 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 uzyskanych w Urzędzie Gminy wynika, że w celu zabezpieczenia danych będących w posiadaniu Urzędu oraz uzyskania maksymalnego poziomu bezpieczeństwa ich przetwarzania zastosowano:
*„Sieć wewnętrzna na styku z Internetem chroniona jest przez oprogramowanie „Endian Firewall Community". Jest to wielofunkcyjny firewall którego zadaniem jest ochrona sieci LAN i DMZ. Jednym z zadań Endiana jest nadzór nad podłączanymi urządzeniami do sieci LAN poprzez dynamiczny przydział adresów IP tylko dla zdefiniowanych urządzeń po MAC adresie. Firewall ma włączone polityki aktualizacji anti-spyware list, clamav virus signatures*

*oraz IPS signatures. Dodatkowo Endian filtruje antyspamowo przychodząca poczta oraz jest możliwość blokady wybranych stron www.*
*W celu ochrony przed wirusami urząd posiada (co rocznie odnawianą) licencje Eset Endpoint Antywirus na 25 komputerów. Każdy komputer posiada sprawny UPS. Każdy z użytkowników posiada unikatowy login do systemu i programów. Uprawnieniami użytkowników do zasobów urzędu zarządzane są centralnie przez usługę katalogową Active Directory. Hasła do komputerów zmieniane są okresowo (co 42 dni) wymuszone przez usługę Active Directory. Ustawiona jest blokada konta użytkownika na 15 min po 5 nieudanych próbach logowania. Każdy użytkownik ma aktywny wygaszacz ekranu który po 15 min blokuje ekran monitora w przypadku bezczynności.*
*Logowanie do programów np. PUMA, odbywa się na podstawie przydzielonych loginów. Systemy wymuszą zmianę hasła co 60 dni. W przypadku CEIDG i Źródła logowanie odbywa się za pomocą odpowiednio karty z certyfikatem kwalifikowanym i karty z certyfikatem źródła.*
*Wydzielone zostały konta administratora systemów i programów. Hasła konta administrator zostały dodatkowo zdeponowane (w zamkniętej kopercie) w sejfie pok. nr 3 (sekretarz gminy).*
*Wydzielone zostało pomieszczenie na serwerownię. Do pomieszczenia dostęp ma tylko informatyk. Serwerownia wyposażona jest w klimatyzację, czujkę dymu oraz termometr i wilgotnościomierz.*
*Poza godzinami pracy urzędu załączany jest alarm z monitoringiem firmy ochroniarskiej. Pokoje są zamykane przez pracowników na klucz (w przypadku ich opuszczania) a klucze umieszcza są w sejfie pok. nr 4."*

*[akta kontroli str. 78-79, 580-597]*

Mając na uwadze powyższe wyjaśnienia przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Zapewniono również środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej, poprzez:
- w systemie: PUMA, logowanie odbywa się za pomocą przyznanego loginu i hasła, które wymaga okresowej wymiany,
- w systemie CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła,
- w systemie Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe.

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Gminy w Pozezdrzu. W wyniku oględzin stwierdzono, że pomieszczenia budynku w którym znajduje się serwerownia posiadają zabezpieczenie alarmowe. Drzwi wejściowe do serwerowni są to specjalistyczne drzwi wzmocnione, zabezpieczone zamkiem patentowym. Urządzenia serwerowe umieszczono w specjalistycznych szafach. W pomieszczeniu zainstalowano urządzenie klimatyzujące oraz UPS chroniący przed spadkiem napięcia podawanego na urządzenia serwerowe. Pomieszczenie wyposażono w gaśnicę przystosowaną do gaszenia urządzeń pod napięciem. W zakresie monitoringu parametrów środowiskowych pomieszczenie serwerowni wyposażono w czujki: monitorującą temperaturę i wilgotność, oraz zadymienie. Powyższe potwierdza dokumentacja z przeprowadzonych oględzin.

*[akta kontroli str. 598-604]*

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

**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 uzyskanych w Urzędzie Gminy wynika, że cyt.: *„Urząd nie ma centralnego serwera rejestracji logów. Systemy dziedzinowe posiadają mechanizmy rejestracji wszystkich logów: poprawnego i nieautoryzowanego logowania, błędy i ostrzeżenia aplikacji, oraz sprzętu. Cykl życia logów: bezterminowy, kasowany dopiero z usunięciem danego obiektu, programu czy systemu."*
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

*[akta kontroli str. 79]*

## 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, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

Zarówno strona internetowa Urzędu Gminy, jak i BIP zawierają elementy umożliwiające zmianę wielkości czcionki oraz zmianę jej kontrastu. Zmiany wielkości czcionki w przypadku strony www dokonuje się przy pomocy ikony A+ (umieszczonej w prawym górnym rogu), natomiast w przypadku strony BIP – przy pomocy ikony AAA (umieszczonej centralnie na środku strony). Zmiana kontrastu możliwa jest za pomocą odpowiednio oznaczonych ikon, umieszczonych w prawym górnym rogu – w przypadku strony www i centralnie - w przypadku strony BIP Urzędu.
Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strona internetowa Urzędu oraz strona BIP 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.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP wykazała 3 błędy, dla strony www. nie wykazała błędów. Sekretarz Gminy w powyższej sprawie wyjaśnił, że, cyt.: „*Do przeprowadzenia testu WCAG 2.0 stron użyłem walidatora on-line http://wave.webaim.org/. Dla strony www.pozezdrze.pl nie stwierdzono błędów, natomiast strona bip.pozezdrze.pl przystosowana jest do standardu WCAG 2.1 po przeprowadzeniu walidacji zawierała 3 błędy oznaczające: 1 brak alternatywnego tekstu i 2 puste linki. Ponieważ, strona bip.pozezdrze.pl została niedawno zaktualizowana (początek października 2019) do najwyższego standardu WCAG 2.1, powyższe błędy zostały zgłoszone do autorów BIP celem ich eliminacji. Z punktu widzenia użytkowania serwisu są nieistotne”.*

*[akta kontroli str. 79, 605-606]*

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

**IV. Zalecenia:**

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1) Uzupełnienie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych o zasady obiegu dokumentów wypływających z Urzędu drogą elektroniczną, co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwiłoby realizację i egzekwowanie m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.
2) Prowadzenie czynności audytowych wynikających z § 20 ust. 2 pkt 14 rozporządzenia KRI, zgodnie z zapisami przyjętej w Urzędzie Polityki Bezpieczeństwa Przetwarzania Danych Osobowych, tj. zgodnie z zasadą, że audytorzy nie audytują własnej pracy.

Proszę Pana Wójta 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*