WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 21 lutego 2020 r.

FK-IV.431.1.2020

Szanowny Pan
Grzegorz Napiwodzki
Wójt Gminy Janowo
ul. Przasnyska 14
13-113 Janowo

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 Janowie, ul. Przasnyska 14, 13-113 Janowo, NIP: 7451123139, REGON: 000535570.

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

1. Pan **Grzegorz Napiwodzki** – Wójt Gminy Janowo, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 4 listopada 2018 roku. [redacted] *(kierownik jednostki kontrolowanej).*
2. Pan [redacted] – Wójt Gminy Janowo w latach 1995-2018.
3. Pani [redacted] – Sekretarz Gminy Janowo, [redacted].
4. Pani [redacted] – Kierownik Referatu Organizacyjnego i Spraw Obywatelskich Urzędu Gminy Janowo, [redacted]. Stanowisko Kierownika sprawuje od [redacted], wcześniej sprawowała je Pani [redacted], [redacted] *(nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą).*
5. Pan [redacted] – Inspektor ds. informatyki i bezpieczeństwa informacji, [redacted] *(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.0030.28.2020 z 15 stycznia 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 51]

Kontrolę przeprowadzono w dniach 22-24 stycznia 2020 r., co zostało odnotowane w książce kontroli Urzędu Gminy Janowo pod pozycją Nr 1/2020.

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 22 stycznia 2020 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 ze zm.) 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 udzielali:
- Sekretarz Gminy Janowo, upoważnienie Wójta Gminy Nr SEK.0052.2.2020,
- Inspektor ds. informatyki i bezpieczeństwa informacji Urzędu Gminy Janowo, upoważnienie Wójta Gminy Nr SEK.0052.1.2020.

[akta kontroli str. 53-62]

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 Janowo 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 - 3 moduły, PUMA – 2 moduły, CEIDG).

Systemy teleinformatyczne wykorzystywane w Urzędzie Gminy Janowo:

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 Rejestr 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.

Rejestry publiczne i ewidencje prowadzone w Urzędzie Gminy w Janowie:
– 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 2019 r., poz. 2010 ze zm.).

- Ewidencja udzielonych i cofniętych zezwoleń na prowadzenie działalności w zakresie opróżniania zbiorników bezodpływowych i transportu nieczystości ciekłych.
- Rejestr instytucji kultury dla których organizatorem jest Gmina Janowo (podstawa prawna art. 14 ust. 1 ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej).
- Rejestr wniosków o udostępnienie informacji publicznej (podstawa prawna Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2019 r. poz. 1429).

[akta kontroli str. 29-30, 63-67]

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 Janowo posiada aktywną Elektroniczną Skrzynkę Podawczą /ugjanowo/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/myportal/wyniki-wyszukiwania?q=Urząd+Gminy+Janowo.

Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto:

- na głównej stronie internetowej BIP Urzędu - Elektroniczna skrzynka podawcza,
- na stronie internetowej www. Urzędu, w centralnym panelu ekranu w zakładce Urząd Gminy – Dane Urzędu Gminy.

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 Janowo w związku z posiadaniem aktywnej Elektronicznej Skrzynki Podawczej udostępniał oraz świadczył m.in. usługę elektroniczną, z wykorzystaniem ePUAP, tj. „Pismo ogólne do podmiotu publicznego" oraz „Udostępnianie informacji publicznej na wniosek". 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.

Usługa „udostępnianie informacji publicznej na wniosek" umożliwia złożenie do wybranej Instytucji Publicznej wniosku o udostępnienie informacji publicznej. Zgodnie z obowiązującymi przepisami, każdy ma prawo do informacji publicznej, udostępnianej na wniosek przez instytucje publiczne. Instytucja publiczna ma obowiązek udostępnić informację publiczną w formie określonej we wniosku, ale ma też prawo do wydania decyzji administracyjnej o odmowie udostępnienia informacji publicznej. Udostępnieniu na wniosek podlega informacja publiczna, która nie została udostępniona w Biuletynie Informacji Publicznej.

W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, iż na stronie BIP w zakładce Urząd Gminy – Załatwianie spraw, opublikowane są metryki spraw – karty usług, będących w zakresie poszczególnych referatów w Urzędzie. Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 68-70]

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.
Z wyjaśnienia uzyskanego w powyższej sprawie z Urzędu Gminy wynika, że cyt.:
„(...) W związku z realizowanym projektem „E-usługi dla Gminy Janowo" uruchomiono 13 e-usług (interaktywne formularze ePUAP):
- *Deklaracja na podatek rolny*
- *Ustalenie warunków zabudowy*
- *Zaświadczenie o przeznaczeniu działki w miejscowym planie zagospodarowania przestrzennego*
- *Zaświadczenia o niezaleganiu z podatkami, opłatami, mandatami lub stwierdzające stan zaległości*
- *Wydanie zaświadczenia o wielkości gospodarstwa rolnego*
- *Deklaracja, korekta deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi*
- *Deklaracja na podatek leśny*
- *Informacja w sprawie podatku leśnego*
- *Informacja w sprawie podatku rolnego*
- *Deklaracja na podatek od nieruchomości*
- *Informacja w sprawie podatku od nieruchomości*
- *Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej*
- *Deklaracja na podatek od środków transportowych*

Ponadto podmiot świadczy usługę elektroniczną z wykorzystaniem ePUAP tj. „Pismo ogólne do urzędu" oraz „Udostępnianie informacji publicznej na wniosek".

Jednocześnie należy zaznaczyć, iż na stronie BIP kontrolowanego Urzędu opublikowano w wersji „do pobrania" formularze niektórych wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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 https://www.janowo.pl/, a strona internetowa BIP Urzędu – pod adresem https://bip.janowo.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 https://www.janowo.pl/, 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.
- **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, umożliwiająca doręczanie pism w formie dokumentów elektronicznych.

Urząd Gminy w Janowie zgodnie z umową zawartą z firmą ZETO Projekt Sp. z o.o. wdraża projekt centralnej platformy e-usług dla mieszkańca. Każdy zarejestrowany na platformie mieszkaniec gminy będzie mógł skorzystać z portalu e-usługi, umożliwiającego:

- prezentację stanów indywidualnych kont kontrahentów,
- otrzymywanie powiadomień o zbliżających się terminach płatności należności,
- otrzymywanie powiadomień o ważnych wydarzeniach dla mieszkańców gminy,

- korzystanie z formularzy elektronicznych przygotowanych dla mieszkańców i kontrahentów.

Planowane uruchomienie systemu przewidywane jest na marzec 2020 roku.

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych, ze względu na fakt, iż instytucja ta nie świadczyła 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. 71-72]

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, cyt.: *„Kontrolowane systemy współpracują z innymi publicznymi systemami teleinformatycznymi. Wymiana informacji odbywa się pomiędzy systemem PUMA i ŹRÓDŁO. Możliwa jest on dzięki wyposażeniu przez MSWiA w odpowiedni sprzęt do transmisji danych po łączu dedykowanym. Transmisja odbywa się przez router Cisco 1800 oraz modem Watsona z szyfrowaniem danych. Wymiana informacji między systemem PUMA a ŹRÓDŁEM odbywa się przez odizolowaną sieć wewnętrzną zgodnie z zaleceniami MSWiA. Logowanie użytkowników do systemu odbywa się za pomocą kart kryptograficznych z dedykowanymi certyfikatami."*

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str251]

1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności 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 21/2019 Wójta Gminy Janowo z dnia 31 stycznia 2019 r. w sprawie określenia sposobu wykonywania czynności kancelaryjnych, wyznaczenia koordynatora czynności kancelaryjnych i Administratora Systemu Elektronicznego Obiegu Dokumentów oraz wprowadzenia Systemu Elektronicznego Obiegu Dokumentów przy wykorzystaniu systemy EDICTA w Urzędzie Gminy Janowo, podstawowym sposobem dokumentowania przebiegu załatwiania spraw w Urzędzie jest system tradycyjny. Elektroniczny system obiegu dokumentów jest systemem wspomagającym. EDICTA to elektroniczny system obsługi dokumentów określający sposób doręczania i wysyłania korespondencji w postaci elektronicznej. Umożliwia zarządzanie dokumentami, korespondencją, sprawami (projektami), poleceniami, terminami oraz czasem pracy pracowników, tworząc centralną, uporządkowaną bazę dokumentów i informacji. Umożliwia również sprawny dostęp do korespondencji, umów, procedur wewnętrznych itp., kontroluje drogę obiegu korespondencji oraz stan realizacji projektów, usprawnia obsługę klientów.

W zarządzeniu określono sposób postępowania z korespondencją wpływającą i wypływającą z Urzędu w formie elektronicznej, co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 73-84]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI *kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez 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 Urząd Gminy wynika, że cyt.: *„System PUMA jest zasilany bezpośrednio z systemu ŹRÓDŁO za pomocą aplikacji narzędziowej dostarczonej przez producenta oprogramowania PUMA - ZETO Software Sp. z o.o. Przekazywanie danych odbywa się w formacie XML z kodowaniem 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. 251]

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI *podmiot 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, w celu 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 150/2016 Wójta Gminy Janowo z dnia 1 lutego 2016 r. r. wdrożono dokumentację ochrony danych osobowych w Urzędzie Gminy Janowo, w skład której weszła Polityka Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcja Zarządzania Systemem Informatycznym. Zarządzenie wprowadzono zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2014 r., Nr 101, 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).
  Powyższa dokumentacja, (Polityka Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcja Zarządzania Systemem Informatycznym), stanowiła 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. 99-148]

- 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO", Zarządzeniem Nr 390/2018 Wójta Gminy Janowo z dnia 31 sierpnia 2018 r. w sprawie wprowadzenia Księgi polityk ochrony danych w Urzędzie Gminy Janowo. Dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „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. 149-199]

- Zarządzeniem Nr 65/2015 Wójta Gminy Janowo z dnia 29 czerwca 2015 r. powołano Administratora Systemu Informatycznego.
- Urząd Gminy w Janowie podpisał w dniu 17 lipca 2018 r. umowę z firmą zewnętrzną na świadczenie usług Inspektora Ochrony Danych zgodnie z art. 39 RODO, w Urzędzie i jednostkach podległych.

[akta kontroli str. 255-260]

Pracownik odpowiedzialny za realizację zadania objętego kontrolą, przeprowadził w 2018 roku 2 sprawdzenia/przeglądy infrastruktury IT Urzędu, tj.: serwerów, stacji roboczych i urządzeń sieciowych. W wyniku czynności sprawdzających nie wykryto istotnych nieprawidłowości.
Z dokumentacji przedstawionej kontrolującemu nie wynikało, aby w 2019 roku podobne sprawdzenia/przeglądy były również dokonywane. Brak powyższych sprawdzeń stanowi uchybienie skutkujące naruszeniem § 20 ust. 1 rozporządzenia KRI, który stanowi, że *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.* Osobami odpowiedzialnymi za powstanie uchybienia są pracownik odpowiedzialny za realizację zadania oraz osoba bezpośrednio go nadzorująca.

Inspektor Ochrony Danych w okresie objętym kontrolą przeprowadził w jednostce 3 wyrywkowe (niepełny audyt SZBI) sprawdzenia audytowe o czym szczegółowo w punkcie 2.9.

[akta kontroli str. 261-277]

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

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 wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI,), w 2018 roku

przeprowadzana była w Urzędzie analiza ryzyka bezpieczeństwa informacji. W ramach przeprowadzonej analizy dokonano oszacowania ryzyka dla bezpieczeństwa danych oraz opracowano katalog zagrożeń/incydentów naruszenia przepisów o ochronie danych. W 2019 roku Inspektor Ochrony Danych powołany w Urzędzie również przeprowadził wymaganą analizę ryzyka. Mając powyższe na uwadze obowiązek wynikający z § 20 ust. 2 pkt 3 rozporządzenia KRI został spełniony.

[akta kontroli str. 174-176, 221-230, 278-280]

Jednocześnie należy wskazać, iż zgodnie z art. 30 ust. 1 RODO, w jednostce jest opracowany i prowadzony rejestr czynności przetwarzania danych.

[akta kontroli str. 240-243]

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 Janowo sporządzoną zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja zgodnie z cyt. powyżej przepisami obejmowała miedzy innymi rodzaj i konfigurację sprzętu.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 85-90]

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 390/2018 Wójta Gminy Janowo z dnia 31 sierpnia 2018 r. w sprawie wprowadzenia Księgi polityk ochrony danych w Urzędzie Gminy Janowo. Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz zasady nadawania uprawnień do pracy w systemie informatycznym opisane są w punkcie 14 powoływanej powyżej Polityki.

[akta kontroli str. 186-187]

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienie. Prowadzona była też elektroniczna ewidencja osób upoważnionych do przetwarzania danych oraz pracy w systemach. Pracownikom posługującym się systemem teleinformatycznym wydane zostały stosowne upoważnienia do pracy w określonym systemie. Jednocześnie należy zaznaczyć, iż z imiennego upoważnienia udzielonego pracownikowi nie wynika do jakiego konkretnego systemu informatycznego (np. PUMA, Źródło, CEiDG) pracownik został upoważniony. Powyższe informacje odczytać można dopiero z prowadzonego oddzielnie rejestru użytkowników i ich uprawnień w systemie. Na wydanym upoważnieniu widnieje tylko nazwa zbioru danych osobowych, do przetwarzania których pracownik został upoważniony (np. dokumentacja Urzędu Stanu Cywilnego).

[akta kontroli str. 348-359]

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 *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.*

Z dokumentacji przedstawionej kontrolującemu wynika, że pracownicy Urzędu Gminy Janowo zaangażowani w proces przetwarzania informacji uczestniczyli w 2018 roku w jednym szkoleniu dotyczącym aspektów RODO.
Ponadto pracownicy Urzędu mieli możliwość uczestnictwa w 4 szkoleniach zorganizowanych na platformie eLearningowej, tj.:

- Podstawy prawne ochrony danych osobowych – przegląd aktów prawnych. Przegląd podstawowych definicji RODO i ich znaczenie dla organizacji. Prawa i obowiązki

administratora danych. IOD. Organy nadzorcze – postępowanie kontrolne, odpowiedzialność za naruszenia – czas szkolenia 2 godziny.
- Najważniejsze obowiązki administratora danych nałożone przez RODO oraz rola IOD w organizacji – czas szkolenia 30 min..
- Ograniczenia prawa do informacji publicznej ze względu na ochronę tajemnicy przedsiębiorcy i ochronę danych osobowych. Anonimizacja danych osobowych przed opublikowaniem dokumentu w BIP – czas szkolenia 1 godzina.
- Zmiany wprowadzone przez RODO – czas szkolenia 1 godzina.

[akta kontroli str. 91-98]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.6. Praca na odległość i mobilne przetwarzanie danych

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

Z uzyskanych z Urzędu Gminy informacji wynika, że cyt.: *„W chwili obecnej nie są podejmowane działania i nie określono zasad i reguł pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość z uwagi na stacjonarny tryb pracy."*

[akta kontroli str. 253]

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 Janowo użytkowany jest 1 system teleinformatyczny do realizacji zadań publicznych zakupiony u zewnętrznego dostawcy, tj.: [redacted]

[redacted] umożliwiające prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu.

[akta kontroli str. 281-307]

W ramach prowadzonych czynności kontrolnych stwierdzono, że Urząd Gminy [redacted] stosowną umowę powierzenia danych na wypadek awarii systemu oraz konieczności ingerencji firmy jako autora oprogramowania w bazy danych zawierające dane osobowe.

[akta kontroli str. 308-314]

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 określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony danych osobowych została uregulowana Zarządzeniem Nr 390/2018 Wójta Gminy Janowo z dnia 31 sierpnia 2018 r. w sprawie wprowadzenia Księgi polityk ochrony danych w Urzędzie Gminy Janowo. (pkt 10 *Procedura alarmowa*, pkt 11 *Procedura sprawdzająca*, pkt 12 *Procedura działań korygujących i zapobiegawczych*).
Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 178-183]

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Na podstawie okazanej dokumentacji kontrolujący stwierdził, iż w okresie objętym kontrolą tj. od 1 stycznia 2018 r. do dnia rozpoczęcia czynności kontrolnych (22 stycznia 2020 r.) Inspektor Ochrony Danych przeprowadził w kontrolowanej jednostce 3 wyrywkowe (niepełny audyt SZBI) sprawdzenia audytowe dotyczące:

- Realizacji zapisu art. 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Realizacji art. 173 Prawa telekomunikacyjnego – audyt zdalny strony internetowej Urzędu oraz strony BIP – rok 2018.
- Monitoringu wizyjnego - jako tematu ujętego w planie kontroli sektorowych UODO na 2019 rok.
- Anonimizacji danych osobowych publikowanych w BIP – rok 2019.

[akta kontroli str. 261-277]

Przedmiotowe audyty nie obejmowały swoim zakresem całości zagadnień związanych z bezpieczeństwem informacji przetwarzanych w Urzędzie. Brak corocznego całościowego audytu bezpieczeństwa informacji w jednostce (ze względu na przeprowadzone wyrywkowe sprawdzenia audytowe), należy zakwalifikować jako uchybienie, skutkujące tylko częściowym dopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną za powstanie uchybienia jest IOD kontrolowanej jednostki.

W przypadku roku 2020 r., istnieje jeszcze możliwość przeprowadzenia przez jednostkę audytu bezpieczeństwa informacji (do końca bieżącego roku). Wobec powyższego dopełnienie obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, w zakresie roku 2020, nie podlegało ocenie.

[akta kontroli str. 261-275]

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 390/2018 Wójta Gminy Janowo z dnia 31 sierpnia 2018 r. w sprawie wprowadzenia Księgi polityk ochrony danych w Urzędzie Gminy Janowo. (pkt 17 *Procedura tworzenia kopii zapasowych*). Zgodnie z wytycznymi zawartymi w przyjętej Polityce ASI zobowiązany jest do opracowania procedury oddzielnie dla każdego systemu informatycznego, w postaci instrukcji zarzadzania systemem informatycznym. Z dokumentacji przedstawionej kontrolującemu wynika, że przedmiotowe instrukcje zostały opracowane zgodnie z wytycznymi przyjętej w Urzędzie Polityki. W instrukcji zarządzania systemem informatycznym opracowanym dla sytemu PUMA znajdują się procedury tworzenia i przechowywania kopii zapasowych. W aktach kontroli zamieszczono wydruki potwierdzające tworzenie kopii zapasowych w cyklu dziennym, tygodniowym (automatyczne) oraz w cyklu miesięcznym wykonywane ręcznie na zewnętrznych nośnikach

pamięci.

W powyższej sprawie kontrolujący otrzymał wyjaśnienia, cyt.: „(...) [redacted]"

[akta kontroli str. 191, 212-219, 253, 317-321]

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenie przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu, z otrzymanego z Urzędu Gminy wyjaśnienia wynika, że cyt.: *„Okresowo wykonywane są testy w celu sprawdzenia poprawności wykonywania kopii zapasowych baz danych. Podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu sprawdza się przydatność utworzonych wcześniej kopii. Przywrócenie systemów wykonywane jest na maszynie wirtualnej po wcześniejszym wykonaniu migawki (snapshota) lub na maszynie zastępczej".*

[akta kontroli str. 253]

Jednocześnie należy zaznaczyć, iż kontrolującemu nie przedstawiono żadnej dokumentacji potwierdzającej wykonywanie testów w celu sprawdzenia poprawności tworzonych kopii zapasowych oraz sprawdzenia przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu. Brak potwierdzenia w dokumentacji przedmiotowych czynności nie pozwala kontrolującemu jednoznacznie stwierdzić, że sprawdzenia poprawności tworzonych kopii zapasowych były faktycznie wykonywane. Powyższe należy zakwalifikować jako uchybienie. Osobami odpowiedzialnymi za powstanie uchybienie są: pracownik realizujący zadanie oraz osoba bezpośrednio go nadzorująca.

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 z uchybieniami.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.*

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. 281-307]

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, cyt.: *„W celu zapewnienia ochrony przetwarzanych informacji*

sieć wewnętrzna [redacted]

W celu ochrony przed wirusami na wszystkich komputerach zainstalowany jest program „ESET Endpoint Security". Blokuję on również możliwość zapisu danych na zewnętrznych nośnikach pamięci.
Każdy użytkownik posiada indywidualny login i hasło do systemu operacyjnego. Uprawnieniami zarządza się centralnie za pomocą usługi „Active Directory". Wymusza ona m.in. okresową zmianę haseł. Pracownicy logują się na konta z uprawnieniami użytkownika bez możliwości ingerencji w oprogramowanie i ustawienia systemu. (...)
Regularnie i automatycznie wykonywane są kopie zapasowe danych. [redacted] *Kopie baz danych poddawane są okresowej poprawności odtworzenia.*
Serwerownia znajduje się w wydzielonym pomieszczeniu do którego dostęp mają tylko uprawnione osoby. Bezpieczeństwo działania systemów teleinformatycznych realizowane jest również poprzez aktualizację systemów i oprogramowania do najnowszych wersji. Budynek posiada system alarmowy wraz z umową na konserwację, monitoring i ochronę budynku. Przeprowadzono szkolenia pracowników w zakresie bezpieczeństwa informacji".

[akta kontroli str. 253-254, 322-339]

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 Źródło logowanie odbywa się poprzez imienną kartę dostępową i indywidualne hasło dostępowe,
- 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.

Powyższe sprawdzono na wybranym stanowisku roboczym.

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Gminy Janowo. W wyniku oględzin stwierdzono, że pomieszczenia budynku, w którym znajduje się serwerownia posiadają zabezpieczenie alarmowe. 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. Pomieszczenie serwerowni wyposażono w stację monitorującą temperaturę i wilgotność.

W wyniku oględzin stwierdzono ponadto uchybienia, tj.: drzwi wejściowe do serwerowni są to zwykłe drzwi wewnętrzne z pojedynczym zamkiem patentowym. Podłoga serwerowni wyłożona jest wykładziną dywanową. W pomieszczeniu znajduje się grzejnik oraz instalacja centralnego ogrzewania. W pomieszczeniu serwerowni przechowywany jest dodatkowy sprzęt niezwiązany z funkcjonowaniem serwerowni.
Przyczyną powstania uchybień jest niedostosowanie pomieszczenia do pełnienia roli serwerowni, co skutkować może awarią urządzeń serwerowych i utratą danych. Osobą odpowiedzialną za powstanie uchybień jest kierownik kontrolowanej jednostki.

Powyższe potwierdza dokumentacja z przeprowadzonych oględzin.

[akta kontroli str. 340-347]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

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.: *„Wykorzystywane systemy dziedzinowe posiadają mechanizmy rejestracji logów wszystkich operacji, w tym informacji o logowaniu i wylogowaniu użytkowników. Przechowywane są one w katalogach i bazach danych poszczególnych systemów od momentu wdrożenia."*
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 254]

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 A+ A++ (umieszczonej w prawym górnym rogu), natomiast w przypadku strony BIP – przy pomocy ikony A +A ++A (umieszczonej w lewym górnym rogu strony). Zmiana kontrastu możliwa jest za pomocą

odpowiednio oznaczonych ikon, umieszczonych w prawym górnym rogu - w przypadku strony www lewym górnym rogu - 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 2 błędy, dla strony www. Urzędu 4 błędy.

Z wyjaśnienia Urzędu wynika, ze cyt.: „Strony internetowe zostały dostosowane do standardu WCAG 2.0. Zawierają elementy umożliwiające zmianę wielkości czcionki oraz kontrastu. Planowane jest również wdrożenie w najbliższym czasie nowych szablonów dostosowanych do standardu WCAG 2.1".

[akta kontroli str. 254, 315-316]

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Przeprowadzanie sprawdzeń/przeglądów infrastruktury IT Urzędu Gminy, tj.: serwerów, stacji roboczych i urządzeń sieciowych, w celu doskonalenia systemu zarządzania bezpieczeństwem informacji i utrzymywania go na odpowiednio wysokim poziomie.

2. Zapewnienie w jednostce nie rzadziej niż raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.

3. Regularne testowanie jakości wytworzonych kopii zapasowych poprzez odtworzenie danych systemu informatycznego z wytworzonej kopii oraz każdorazowe dokumentowanie wykonywanych testów poprawności tworzonych kopii zapasowych.

4. W miarę możliwości finansowych Urzędu zabezpieczenie pomieszczenia serwerowni poprzez montaż wzmocnionych drzwi wejściowych o podwyższonej odporności ogniowej, usunięcie podłogowej wykładziny dywanowej, demontaż instalacji CO w pomieszczeniu lub zakup czujki informującej o zalaniu, usunięcie z pomieszczenia serwerowni dodatkowego sprzętu niezwiązanego z funkcjonowaniem serwerowni.

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