WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olszty, 5 marca 2021 r.

FK-IV.431.2.2021

Szanowny Pan
Krzysztof Locman
Wójt Gminy Kowale Oleckie
ul. Kościuszki 44
19-420 Kowale Oleckie

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Gminy Kowale Oleckie[1], ul. Kościuszki 44, 19-420 Kowale Oleckie, NIP: 847-161-21-61, Regon: 790671254.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan Krzysztof Locman – Wójt Gminy, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 listopada 2018 roku (nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą).

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie byli:

- Pan [redacted] zatrudniony na podstawie umowy o pracę od dnia 02.06.2015 r.,
- Pan [redacted] zatrudniony na podstawie umowy o pracę od dnia 16.01.2004 r.

[akta kontroli str. 76]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko-Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – inspektor wojewódzki; przewodniczący zespołu kontrolnego, 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.0030.17.2021 z 14 stycznia 2021 r., wydanego przez

[1] Zwanym dalej: Urzędem

Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.18.2021 z 14 stycznia 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 15-16]

Kontrolę przeprowadzono w dniach 27 stycznia 2021 r. – 17 lutego 2021 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 1/2021.
Kontrola prowadzona była w trybie zdalnym, tj. bez osobistej obecności kontrolerów, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. Rozpoczęcie kontroli nastąpiło podczas wideokonferencji, w trakcie której okazano legitymacje służbowe kontrolerów, poinformowano o zasadach kontroli w trybie zdalnym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania. Upoważnienia kontrolerów do kontroli zostały przekazane do kontrolowanej jednostki za pośrednictwem platformy e-PUAP.

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 2020 r., poz. 346 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 44-54]

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. 2020 poz. 224), 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., Dz.U. z 2019 r. poz. 700 ze zm. - akt prawny obowiązujący do 04.03.2020 r. oraz Dz.U. z 2020 r., poz. 346 ze zm.)[2], 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 ze zm.)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań

[2] Zwanej dalej: ustawą
[3] Zwanego dalej: rozporządzeniem KRI

publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1-2, 44-54]

Wójt Gminy Kowale Oleckie upoważnił Inspektora OC i ZK (Inspektor Ochrony Danych) oraz Informatyka Urzędu (ASI) do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 437-438]

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

Z informacji przekazanych przez Urząd przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są **4** systemy teleinformatyczne:

1. Źródło (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr Dowodów Osobistych),
2. PUMA (ewidencja ludności, paliwa),
3. SYGNITY S.A. (dodatki energetyczne),
4. CEIDG (działalność gospodarcza).

Systemy teleinformatyczne wykorzystywane w Urzędzie:

1) **ŹRÓDŁO** – (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr dowodów osobistych) bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych. 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 (rejestr mieszkańców)** posiada homologację Ministerstwa Spraw Wewnętrznych, 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 paliwa (dopłaty rolnicze do paliw) - obsługą zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej.
3) **SYGNITY S.A.** - moduł DE - Przyznanie odbiorcy wrażliwemu energii elektrycznej

przysługującego mu zryczałtowanego dodatku energetycznego.

4) **CEIDG** jest to elektroniczny rejestr przedsiębiorców działających na terenie kraju. Portal ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności gospodarczej. Służy również do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.

Rejestry publiczne i ewidencje prowadzone w Urzędzie:

- 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, Dz. U. z 2020 r., poz. 1439).
- Ewidencja podmiotów posiadających zezwolenie na opróżnianiem zbiorników bezodpływowych i transport nieczystości ciekłych na terenie Gminy (podstawa prawna - art. 7 ust. 6b ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Dz. U. z 2020 r., poz. 1439).
- Rejestr instytucji kultury których organizatorem jest Gmina Kowale Oleckie, prowadzony na podstawie ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (tekst jedn. Dz. U. z 2018 r. poz. 1993) i Rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 26 stycznia 2012 r. w sprawie sposobu prowadzenia i udostępniania rejestru instytucji kultury (Dz. U. z 2012 r. poz. 189).
- Wykaz danych o dokumentach zawierających informacje o środowisku i jego ochronie (podstawa prawna art. 23 ustawy z dnia 3 października 2008r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko Dz.U. z2017 poz. 1405).

[akta kontroli str. 417-424]

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 posiada aktywną Elektroniczną Skrzynkę Podawczą **/gminakowaleoleckie/skrytka,** znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Pełny adres oraz ścieżkę bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu – Menu podmiotowe – dane teleadresowe. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: ODF, ODS, DOC, RTF, XLS, CSV, TXT, PNG, GIF, TIF, BMP, JPG, PDF, ZIP, RAR, 7zip.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, iż na stronie BIP w zakładce *Menu przedmiotowe – wykaz spraw*, opublikowane są procedury niezbędne do realizacji przy załatwianiu danej sprawy. Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych. Ponadto na stronie BIP opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie.

W wyniku prowadzonej kontroli stwierdzono, iż w ramach funkcjonującej strony internetowej Urzędu, w zakładce eUsługi działa Elektroniczne Biuro Obsługi Interesanta (eBOI). Portal eUsługi służy do komunikacji interesanta z urzędem. Dzięki udostępnieniu przez BOI katalogu spraw w postaci elektronicznej, interesanci mogą załatwić część spraw za pośrednictwem Internetu. Interesant może załatwiać sprawy, bez konieczności wizyty osobistej w urzędzie, może też z tego miejsca pobrać i wydrukować dokumenty niezbędne do załatwienia spraw, w których obecność osobista jest wymagana. Na portalu interesant może zapoznać się między innymi z katalogiem wybranych spraw świadczonych przez Urząd.
Moduł ePłatności umożliwia przegląd danych dotyczących zobowiązań kontrahentów przechowywanych w systemie dziedzinowym oraz umożliwia ich rozliczenie za pomocą płatności online. Kontrahent może sprawdzić listę swoich zobowiązań wobec Urzędu: nieopłaconych, w trakcie realizacji oraz opłaconych wraz z danymi szczegółowymi. System umożliwia zrealizowanie płatności za pomocą internetowych przelewów bankowych lub kart kredytowych oraz przegląd historii wykonywanych za pośrednictwem systemu eUsług poleceń przelewów. Dodatkowo System udostępnia funkcje generowania przelewów bankowych i pocztowych oraz powiadamia o zbliżających się terminach płatności zobowiązania.

Urząd udostępniał oraz świadczył również usługi elektroniczne, z wykorzystaniem ePUAP, tj. „Pismo ogólne do urzędu". Usługa te umożliwiają złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 425-435]

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 w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE.
Jednocześnie należy zaznaczyć, iż na stronie BIP Urzędu oraz na portalu eUsługi, opublikowano w wersji „do pobrania" formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.
W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 24-33, 432-435, 466-467]

1.3. Model usługowy

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

Strona internetowa Urzędu działa pod adresem http://www.kowaleoleckie.eu/, a strona internetowa BIP Urzędu – pod adresem https://bip.kowaleoleckie.eu/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu w zakładce dane teleadresowe zamieszczono ścieżkę do skrzynki podawczej ESP na platformie ePUAP.
Urząd w ramach działania portalu eUsługi - Elektroniczne Biuro Obsługi Interesanta

służącego do komunikacji interesanta z urzędem, oferuje katalogu spraw w postaci elektronicznej, dzięki któremu interesanci mogą załatwić część spraw za pośrednictwem Internetu.

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych realizowanych przez systemy teleinformatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej ze względu na fakt, iż jednostka nie świadczyła usług elektronicznych na zewnątrz za pomocą tych systemów. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

- § 5 ust. 3 pkt 3 rozporządzenia KRI *interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;*
- § 16 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*

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

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „[redacted]”

[akta kontroli str. 466-467]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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.*

Z uzyskanego w ramach prowadzonych czynności kontrolnych wyjaśnienia wynika, że cyt.: *„W Urzędzie nie przyjęto odrębnego zarządzenia regulującego ogólny obieg dokumentów. Obieg dokumentów w Urzędzie opiera się na „Zarządzenie Nr 39/11 w sprawie wskazania sposobu wykonywania czynności kancelaryjnych w celu dokumentowania przebiegu załatwiania spraw w Urzędzie Gminy Kowale Oleckie" oraz przedstawionym wcześniej zarządzeniu Nr 0050.35.16 z 2016 r.*

Z zarządzenia Nr 39/11 Wójta Gminy Kowale Oleckie z dnia 19 kwietnia 2011 r., wynika, że podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie jest system tradycyjny, tj. system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci nieelektronicznej zgodnie z zasadami określonymi w Rozporządzeniu Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. System tradycyjny czynności kancelaryjnych jest systemem polegającym na dokumentowaniu przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci nieelektronicznej (papierowej) z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentacji w tej postaci.
Podawane natomiast w wyjaśnieniu zarządzenie Nr 0050.35.2016 Wójta Gminy Kowale Oleckie z dnia 17 czerwca 2016 r. wprowadza instrukcję kontroli wewnętrznej oraz instrukcję obiegu dokumentów finansowo-księgowych w Urzędzie.

Jednocześnie, w okazanej dokumentacji Urzędu brak jest procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (skrzynka podawcza na platformie ePUAP oraz Elektroniczne Biuro Obsługi Interesanta), 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. W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie uchybieniami. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 244-255, 466-468]

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 uzyskanych z Urzędu wynika, że, cyt.: „[redacted]".

[akta kontroli str. 466-467]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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.*

Realizacja ww. zadań wymaga od podmiotu publicznego 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. Dokument ten 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.

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", w Urzędzie przyjęto:

- Zarządzeniem Nr Or. 0050.37.2018 z 25 maja 2018 r. Wójta Gminy Kowale Oleckie w sprawie wprowadzenia dokumentacji systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy w Kowalach Oleckich, wprowadzono Politykę bezpieczeństwa danych osobowych i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz przyjęto sposób postępowania w sytuacjach naruszenia ochrony danych osobowych (dokumentacja obowiązywała do 9 kwietnia 2019 r.).
- Zarządzeniem Nr Or. 0050.21.2019 z 9 kwietnia 2019 r. Wójta Gminy Kowale Oleckie w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych, wprowadzono Politykę ochrony danych i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

[akta kontroli str. 87-186]

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO", ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), w brzmieniu obowiązującym w tym okresie. 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.

Wójt Gminy Kowale Oleckie wyznaczył Administratora Systemu Informatycznego w Urzędzie (ASI) oraz powołał w jednostce Inspektora Ochrony Danych (IOD).

[akta kontroli str. 77-86]

W myśl § 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.
W celu realizacji nałożonego przez KRI obowiązku, IOD powołany w jednostce dokonał w przeglądu SZBI funkcjonującego w Urzędzie. Z przeprowadzanych czynności sporządzono raport, który obejmował również rekomendacje wydane w celu doskonalenia SZBI w jednostce.

[akta kontroli str. 242-243]

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 wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko.
W myśl przyjętej w Urzędzie Polityki ochrony danych rozdział 7.1 pkt 3 analiza ryzyka przeprowadzana jest nie rzadziej niż raz na rok.

Zgodnie z przekazaną dokumentacją wymagane oszacowanie i analiza ryzyka utraty integralności, dostępności lub poufności informacji w jednostce, przeprowadzona została 4 kwietnia 2019 roku. Jednocześnie należy zaznaczyć, iż kontrolującym nie przedstawiono dokumentacji świadczącej o przeprowadzeniu okresowej analiz ryzyka utraty integralności, dostępności lub poufności informacji w 2020 roku.

Z przekazanego w powyższej sprawie wyjaśnienia wynika, że: *„Analizę ryzyka przeprowadzono w 2019 roku. Oceniono, że analiza ryzyka przeprowadzona w 2019 roku w związku z wprowadzaniem e-Usług jest wystarczająca gdyż nie nastąpiły zmiany w sposobie działania Urzędu. Następna analiza ryzyka planowana jest w IV kw. 2021 r."*
Brak przeprowadzonej analizy ryzyka w 2020 roku stanowi nieprawidłowość.

Niedokonanie okresowej analizy ryzyka stanowi naruszenie § 20 ust. 2 pkt 3 rozporządzenia KRI, jak również rozdziału 7.1 pkt 3 przyjętej w Urzędzie Polityki ochrony danych. Osoba odpowiedzialną za powstanie nieprawidłowości jest IOD powołany w jednostce.

[akta kontroli str. 187-241, 466-467]

Jednocześnie należy wskazać, iż w jednostce jest opracowany i prowadzony rejestr czynności przetwarzania danych osobowych.

[akta kontroli str. 256-267]

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

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.*

Kontrolującym przedstawiono aktualną inwentaryzację sprzętu komputerowego użytkowanego w Urzędzie sporządzoną zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI. Przedmiotowa inwentaryzacja zgodnie z cyt. powyżej przepisami obejmowała między innymi rodzaj i konfigurację sprzętu.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 268-299]

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 (bezpieczeństwa informacji) 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 określonym zbiorze danych (systemie informatycznym) określone zostały zarządzeniem Nr Or. 0050.21.2019 z 9 kwietnia 2019 r. Wójta Gminy Kowale Oleckie w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych.

[akta kontroli str. 89-152]

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym).

[akta kontroli str. 300-308]

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 kontrolującym wynika, że pracownicy Urzędu zaangażowani w proces przetwarzania informacji, uczestniczyli w okresie objętym kontrolą w dwóch szkoleniach (zorganizowanych przez IOD), dotyczącym ochrony danych osobowych.
Szkolenia przeprowadzone w 2019 i 202 roku dotyczyły ochrony danych osobowych przetwarzanych w Urzędzie w świetle obowiązującego prawa. W załączeniu przedstawiono listy obecności pracowników uczestniczących w szkoleniu.

[akta kontroli str. 309-316]

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.*

Zarządzeniem Nr Or. 0050.21.2019 z 9 kwietnia 2019 r. Wójta Gminy Kowale Oleckie w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych, wprowadzono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. W rozdziale XIII przedmiotowej instrukcji ujęto zasady pracy na komputerach przenośnych oraz zasady wynoszenia przenośnego sprzętu informatycznego poza siedzibę Urzędu. Jednocześnie z informacji uzyskanych podczas prowadzonych czynności kontrolnych wynika, że w jednostce nie wystąpiły przypadki przetwarzania danych osobowych na odległość.

[akta kontroli str. 153-186, 466-467]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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.

Procedura wykonywania przeglądów i konserwacji systemów i nośników informacji ujęta została w zarządzeniu Nr Or. 0050.21.2019 z 9 kwietnia 2019 r. Wójta Gminy Kowale Oleckie w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. – rozdział XI.

W Urzędzie użytkowane są dwa systemy teleinformatyczny przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupione u zewnętrznego dostawcy, tj.: PUMA oraz SYGNITY S.A. moduł DE.

[redacted]

[redacted] zawarta została również stosowna umowa gwarantująca właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli str. 439-460]

Kontrolującym nie przedstawiono umowy powierzenia przetwarzania danych osobowych podpisanej z firmą SYGNITY S.A. Z wyjaśnienia Urzędu w powyższej sprawie wynika, że cyt.: *„Umowa powierzenia przetwarzania danych nie została podpisana ze względu na nie przekazywanie danych do firmy SYGNITY S.A. W przypadku zaistnienia potrzeby przesłania danych do firmy umowa taka zostanie podpisana przed przesłaniem danych."*

[akta kontroli str. 466-467]

Zgodnie z rozdziałem 5.4. Polityki - *Powierzanie przetwarzania danych osobowych*, ADO w sytuacjach, w których powierza przetwarzanie danych osobowych innemu podmiotowi zawiera z nim stosowną umowę powierzenia. Powierzenie następuje, gdy podmiot trzeci będzie przetwarzał dane osobowe w imieniu ADO (np. umowy serwisowe sprzętu zawierającego dane osobowe, dostęp podmiotów zewnętrznych do baz danych ADO w ramach tzw. helpdesk, zlecanie realizacji zadań wymagających przetwarzania danych osobowych podmiotom zewnętrznym). Kontrolujący przychylają się do wyjaśnień Urzędu w kwestii braku umowy powierzenia przetwarzania danych podpisanej z firmą SYGNITY S.A. Jednocześnie należy zauważyć, że brak aktualnej umowy powierzenia przetwarzania danych w sytuacji wystąpienia awarii danego systemu, znacznie wydłuży okres jego przywrócenia do prawidłowego działania, gdyż w pierwszej kolejności należy podpisać stosowną umowę, a dopiero po jej podpisaniu możliwe jest przekazanie ewentualnych uszkodzonych baz danych do weryfikacji w ramach umów serwisowych.

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 oraz podejmowanych działań korygujących została uregulowana zarządzeniem Nr Or. 0050.21.2019 z 9 kwietnia 2019 r. Wójta Gminy Kowale Oleckie w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych, wprowadzającym Politykę bezpieczeństwa danych osobowych i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

[akta kontroli str. 89-186]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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 stwierdzili, iż w okresie objętym kontrolą tj. od 1 stycznia 2019 r. do dnia 31 grudnia 2020 r., w jednostce przeprowadzono 1 zadanie audytowe w zakresie bezpieczeństwa informacji. W 2019 r. firma zewnętrzna przeprowadziła badanie audytowe w zakresie systemu bezpieczeństwa informacji w Urzędzie Gminy Kowale Oleckie. Raport z badania składał się z dwóch części:

- Części 1: stanowiącej podsumowanie analizy stosowanych w Urzędzie Gminy Kowale Oleckie mechanizmów zapewniających spełnienie wymagań prawnych w zakresie bezpieczeństwa informacji i ochrony danych osobowych.
- Części 2: stanowiącej określenie stanu faktycznego zabezpieczeń technicznych i systemów informatycznych w Urzędzie Gminy Kowale Oleckie.

Powyższy raport zawiera również rekomendacje w zakresie stwierdzonych podczas przeprowadzonego badania uchybień.

[akta kontroli str. 317-409]

Na podstawie przekazanej dokumentacji kontrolujący stwierdzili, że w 2020 r. nie przeprowadzono audytu wewnętrznego wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI 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. Powyższe stanowi nieprawidłowość.
Z wyjaśnienia Urzędu w powyższej sprawie wynika, że cyt.: *„Ze względu na zaistniałą sytuację pandemiczną podjęto decyzję o nieprzeprowadzaniu w 2020 roku audytu. Natomiast audyt planowany jest w IV kw. 2021 r."*

[akta kontroli str. 466-467]

Odnosząc się do powyższych wyjaśnień należy zaznaczyć, że nie można uwzględnić argumentacji jednostki kontrolowanej, co do wskazanych okoliczności odstąpienia od przeprowadzenia audytu wewnętrznego. Obowiązek przeprowadzenia audytu z zakresu bezpieczeństwa informacji wynika wprost z przepisów prawa. Fakt wystąpienia stanu pandemii nie spowodował zmiany powyższych przepisów. Jednostka kontrolowana nie przedstawiła dodatkowej argumentacji na okoliczność wskazującą na niemożliwość bądź znaczne utrudnienie przeprowadzenia przedmiotowego audytu.
Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą

odpowiedzialną za powstanie nieprawidłowości jest Kierownik jednostki.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

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 testowania kopii zapasowych uregulowane zostały zarządzeniem Nr Or. 0050.21.2019 z 9 kwietnia 2019 r. Wójta Gminy Kowale Oleckie w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, rozdział VII. [redacted]

Zgodnie z przekazaną kontrolującym dokumentacją (zrzuty ekranu potwierdzające wykonywanie automatycznej kopii bazy danych systemu PUMA oraz SYGNITY) obowiązek minimalizowania ryzyka utraty informacji w wyniku awarii, poprzez wykonywanie kopii zapasowych jest realizowany.

[akta kontroli str. 153-186, 466-467]

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenia przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu Urząd wyjaśnił, że cyt.: [redacted]

[redacted]

Odnosząc się do powyższego wyjaśnienia należy stwierdzić, że zgodnie z przyjętą do stosowania instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, rozdział VII - [redacted]

Z uzyskanego wyjaśnienia wynika, że testowanie kopii zapasowych nie jest przeprowadzane zgodnie z przyjętą do stosowania instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych co stanowi uchybienie. Osoba odpowiedzialną za powstanie uchybienia jest informatyk Urzędu.

[akta kontroli str. 466-467]

Należy wskazać, że regularne testowanie jakości kopii zapasowych 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 systemy wspierające zakupione u dostawców zewnętrznych – PUMA oraz SYGNITY S.A. Na obsługę aktualnie zainstalowanego oprogramowania z firmami dostarczającymi dany system informatyczny zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantująca rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupione systemy teleinformatyczne, w razie awarii podlegają ekspertyzie technicznej zlecanej firmie dostarczającej.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 439-460]

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.

Zgodnie z wyjaśnieniem uzyskanym w trakcie kontroli, cyt.: „[redacted]

Jednocześnie w celu zapewnienia odpowiedniego poziomu bezpieczeństwa w budynku zgodnie z załącznikiem Nr 6.3.1 do przyjętej w Urzędzie Polityki ochrony danych, wyznaczono osoby odpowiedzialne za otwarcie i zamknięcie budynku urzędu oraz za aktywację i dezaktywację systemu alarmowego w wyznaczonych godzinach pracy. Jednocześnie zobowiązano wyznaczonych pracowników do:

- wykorzystywania udostępnionych kluczy zgodnie z przeznaczeniem,
- niewykonywania kopii udostępnionych kluczy,
- starannego zamknięcie wejścia do budynku,
- aktywacji i dezaktywacji systemu alarmowego,

- w momencie otwierania budynku sprawdzania czy nie doszło do próby włamania i ewentualne niezwłoczne poinformowanie o takim zdarzeniu, w przypadku jego wystąpienia.

[akta kontroli str. 416, 466-467]

Mając na uwadze powyższe 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:

[redacted]

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.*

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Z wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że [redacted]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 466-467]

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.

Każda strona dostępna w Internecie powinna zapewniać maksymalne wsparcie wszystkim grupom wiekowym jak i społecznym. Warunkiem dostępności strony jest dobry kontrast zapewniający swobodny odczyt przedstawionych informacji. Im wyższy jest kontrast, tym łatwiej odróżnić obiekt, zdjęcie czy tekst pierwszego planu od tła. Niski poziom kontrastu utrudnia korzystanie z witryny przede wszystkim użytkownikom o mniejszej ostrości wzroku, a także osobom niedowidzącym. Celem ułatwienia postrzegania tekstu użytkownikom niedowidzącym można również umożliwić zmianę wielkości tekstu bez utraty jego czytelności lub funkcjonalności serwisu internetowego. Zarówno strona internetowa BIP, jak i strona www. Urzędu zawierają elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niedowidzące. Na stronie www. widnieje informacja, że Urząd zapewnia wszystkim zainteresowanym przy załatwieniu spraw urzędowych bezpłatną pomoc tłumacza języka migowego. Serwis urzędu został stworzony zgodnie ze standardami W3C oraz WCAG2.0 w oparciu o mechanizmy ułatwiające osobom niepełnosprawnym dostęp do publikowanych treści. Ponadto portal został zaprojektowany zgodnie z wymaganiami kontrastu opisanym w KRI. Wszystkie elementy na stronie spełniają minimalne wymagania kontrastu koloru treści do tła.
Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strony BIP i www. spełniają 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 i strony www. Urzędu nie wykazała istotnych błędów.

[akta kontroli str. 461-462]

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Opracowanie wewnętrznych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby również zasady obiegu dokumentów wpływających i wypływających z Urzędu drogą elektroniczną.
2. Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI jak

również rozdziału 7.1 pkt 3 przyjętej w Urzędzie Polityki ochrony danych przeprowadzanie okresowej analiza ryzyka utraty integralności, dostępności lub poufności informacji, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, wprowadzenie działań minimalizujących to ryzyko.

3. Zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
4. Zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI oraz przyjętą instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych - rozdział VII, regularne testowanie jakości wytworzonych kopii zapasowych poprzez odtworzenie danych systemu informatycznego z wytworzonej kopii. Ponadto każdorazowe dokumentowanie wykonywanych testów poprawności tworzonych kopii zapasowych.

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