WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

FK-IV.431.17.2020

Olsztyn, 10 listopada 2020 r.

Szanowny Pan
Zbigniew Kudrzycki
Wójt Gminy Rozogi
ul. Wojciecha Kętrzyńskiego 22
12-114 Rozogi

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 w Rozogach[1], ul. Wojciecha Kętrzyńskiego 22, 12-114 Rozogi, NIP: 745-17-45-941, REGON: 550668120.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan Zbigniew Kudrzycki – Wójt Gminy, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 2l października 2018 roku.

Odpowiedzialnymi za realizację zadania objętego kontrolą byli:
1. Pan [redacted] – świadczący usługi informatyczne na podstawie umowy zawartej w dniu 31 grudnia 2019 r. (firma zewnętrzna).
2. Pan [redacted] – pełniący funkcję Inspektora Ochrony Danych Osobowych na podstawie umowy [redacted] z dnia 30 grudnia 2019 r. (firma zewnętrzna).

[akta kontroli str. 92-93]

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.0030.300.2020 z 24 września 2020 r., wydanego przez

[1] Zwanego 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.0030.301.2020 z 24 września 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 32-35]

Kontrolę przeprowadzono w dniach 8-28 października 2020 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją Nr 5/2020.

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 2018 r. do dnia 8 października 2020 r. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1-3, 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. 1-3, 44-54, 57-63]

Wójt Gminy Rozogi upoważnił Sekretarza Gminy do udzielania informacji i wyjaśnień w okresie trwania czynności kontrolnych:

[akta kontroli str. 94-95]

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.**
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, rejestr wyborców),
3. System PB_USC (system wspierający - obsługa USC),
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 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) **PB_USC** - moduł wspomagający w zakresie kompleksowej obsługi stanu cywilnego. Migracja aktów stanu cywilnego do Bazy Usług Stanu Cywilnego (BUSC). Producent Technika IT Sp. z o.o.

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 udzielonych i cofniętych zezwoleń 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, dla których organizatorem jest Gmina.

[akta kontroli str. 546]

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 **/h2bj5r59az/skrytka,** znajdującą

się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na głównej stronie internetowej BIP Urzędu.
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 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 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 podmiotu publicznego". Usługa ta umożliwia złożenie do wybranego organu administracji publicznej pisma (podania) w sprawie.
Jednocześnie należy zaznaczyć, że 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. 547-551]

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 portalu eUsługi kontrolowanego Urzędu, opublikowano w wersji „do pobrania" formularze wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie. Jednostka wykorzystuje również wzory „centralne" w zakresie prowadzonych spraw podatkowych.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 12, 551-552]

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://rozogi.pl/, a strona internetowa BIP Urzędu – pod adresem https://rozogi.bipgmina.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu oraz ESP (elektroniczna skrzynka podawcza), w lewej dolnej części panelu strony. Na stronie głównej BIP Urzędu również zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.

Na stronie internetowej Urzędu, 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**, 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.
- **Emp@tia** portal informacyjno-usługowy. Portal zawiera informacje ważne przy ubieganiu się o świadczenia z pomocy społecznej, świadczenia rodzinne, a także z funduszu alimentacyjnego, informacje o formach opieki nad dzieckiem do lat trzech. Przekazuje również, jakie świadczenia przysługują osobom przemieszczającym się w obrębie Unii Europejskiej i na czym polega koordynacja systemów zabezpieczenia społecznego.
- **CEiDG** – portal umożliwiający założenie działalności gospodarczej.

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. Wykaz usług świadczonych drogą elektroniczną zdefiniowany został zarządzeniem nr 58/19 Wójta Gminy Rozogi z dnia 17 lipca 2019 r.

[akta kontroli str. 553-554]

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.: *„Współpraca między systemami Puma i PB_USC możliwa jest dzięki stworzeniu dostępu dla komputera z dostępem do aplikacji Źródło do wydzielonych zasobów w sieci lokalnej Urzędu. Dostęp odbywa się dzięki* [redacted]

Wymiana danych z systemem PUMA odbywa się dzięki programowi importPESEL, który jest częścią systemu PUMA zainstalowany i uruchamiany (co godzina) jest on na komputerze z dostępem do systemu Źródło. [redacted]

Wymiana danych między PB_USC polega na wygenerowaniu pliku XML zgodnego ze specyfikacją systemu Źródło, zapisaniu go w udziale sieciowym stworzonym na potrzeby USC (login i hasło do tego udziału jest w posiadaniu kierownika USC). Następnie połączeniu się z tym udziałem z komputera gdzie uruchamiane jest Źródło, pobraniu tego pliku i zaimportowaniu go do systemu Źródło".

[akta kontroli str. 606-620]

Jednocześnie należy wspomnieć, iż Źródło jest to system zarządzany przez Ministerstwo Cyfryzacji o charakterze ogólnopolskim, umożliwia on współpracę z systemem teleinformatycznym PUMA wykorzystywanym w Urzędzie. Stacje robocze na których zainstalowany jest system Źródło pracują w odizolowanej sieci. Dostęp do systemu uprawnieni użytkownicy uzyskują uwierzytelniając się poprzez logowanie do systemu Windows oraz przy pomocy kart kryptograficznych z zainstalowanymi certyfikatami dedykowanymi dla użytkownika aplikacji.

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.*

Zgodnie z zarządzeniem Nr 77/19 Wójta Gminy Rozogi z dnia 2 września 2019 r. w sprawie wprowadzenia Systemu Elektronicznego Obiegu Dokumentów EDICTA w Urzędzie Gminy w Rozogach 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 wspomagany jest przez funkcjonujący w Urzędzie elektroniczny system obiegu dokumentów EDICTA.

EDICTA to elektroniczny system obsługi dokumentów określający sposób obiegu korespondencji również w postaci elektronicznej. Umożliwia zarzadzanie 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.

Określenie zasad obiegu dokumentacji w formie elektronicznej 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.

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 356-368]

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. 13]

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.

Zarządzeniem Nr 109/10 Wójta Gminy Rozogi z dnia 31 grudnia 2010 r. wdrożono w Urzędzie zasady dotyczące sposobu prowadzenia i zakresu dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ich ochronę w Urzędzie Gminy Rozogi (zmienione zarządzeniem Nr 77/13 Wójta Gminy Rozogi z dnia 11 października 2013 r.).
Zarządzenie wprowadzono zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2002 r., Nr 101, poz. 926 Nr 153, poz.1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285.) 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).
Powyższe stanowiło 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. 555-580]

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 dokonano weryfikacji dokumentacji systemu zarządzania bezpieczeństwem informacji i opracowano:

- Zarządzenie Nr 77/18 Wójta Gminy Rozogi z dnia 7 września 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych – obowiązujące do 25 września 2020r.
- Zarządzenie Nr 78/20 Wójta Gminy Rozogi z dnia 25 września 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych.

Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO" oraz 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.

[akta kontroli str. 100-272]

Wójt Gminy Rozogi zarządzeniem Nr 91/17 z dnia 13 listopada 2017 r. wyznaczył Administratora Systemu Informatycznego w Urzędzie (firma zewnętrzna), natomiast zarządzeniem Nr 46/18 z dnia 25 maja 2018 r. powołano w jednostce Inspektora Ochrony Danych (IOD).

[akta kontroli str. 96-99]

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 dokonywał bieżących przeglądów SZBI. Z przeprowadzanych czynności każdorazowo sporządzany był raport, który obejmował również rekomendacje wydane w celu doskonalenia SZBI w jednostce.

[akta kontroli str. 330-355]

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.
Firma zewnętrzna – Centrum Bezpieczeństwa Informatycznego przeprowadziła stosowne okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji w jednostce.

[akta kontroli str. 273-325]

Jednocześnie należy wskazać, iż zgodnie z art. 30 ust. 1 RODO, jak również zarządzeniami Wójta Gminy Rozogi: Nr 45/18 z dnia 25 maja 2018 i Nr 17/20 z dnia 5 lutego 2020 r.,

w jednostce jest opracowany i prowadzony rejestr czynności przetwarzania danych osobowych.

[akta kontroli str. 369-388]

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.*

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. 395-445]

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 77/18 Wójta Gminy Rozogi z dnia 7 września 2018 r.

w sprawie wprowadzenia Polityki Ochrony Danych – obowiązujące do 25 września 2020r.
- Zarządzeniem Nr 78/20 Wójta Gminy Rozogi z dnia 25 września 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych.

[akta kontroli str. 108-111, 176-177, 186-187]

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. 389-394, 581-587]

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 szkoleniach (zorganizowanych przez IOD), dotyczących ochrony danych osobowych, tj.:

- **w 2018** roku przeprowadzono szkolenie zbiorowe w zakresie: „Ochrona danych osobowych oraz przygotowanie do wdrożenia RODO". Szkolenie obejmowało:
  - główne cele reformy ochrony danych osobowych w UE prowadzącej do umocnienia prawa do prywatności,
  - nowe obowiązki ADO np. rejestrowanie czynności przetwarzania, zgłaszanie naruszenia ochrony danych osobowych.
  - najważniejsze zmiany jakie niesie za sobą RODO, nowe zagadnienia np. o pojęciu profilowania, prawie do bycia zapomnianym, system „one stop shop", o międzynarodowym przetwarzaniu danych,
  - IOD - status, zadania,, sytuacje kiedy jego wyznaczenie jest obowiązkowe,
  - przetwarzanie danych przez „podmiot przetwarzający",
  - zadania i rola organu nadzorczego - PUODO,
  - konsekwencje prawne naruszenia zasad przetwarzania danych oraz nowe zasady kontroli.

- **w 2019** roku przeprowadzono szkolenie zbiorowe w temacie: „Praktyczne aspekty

stosowania wdrożonej w jednostce Polityki Ochrony Danych Osobowych". Szkolenie obejmowało:

- zakres stosowania przepisów RODO,
- dane osobowe według RODO,
- zasady przetwarzania danych osobowych w praktyce,
- prawne podstawy przetwarzania danych osobowych,
- sposoby zabezpieczania danych osobowych w praktyce,
- naruszenie bezpieczeństwa informacji - zakres, procedura zgłaszania naruszeń,
- naruszenia danych osobowych w kontekście działań podejmowanych przez UODO,
- odpowiedzialność związana z naruszeniami danych osobowych,
- środki ochrony prawnej wynikające z przepisów RODO,
- konsekwencje nieprzestrzegania przepisów dotyczących ochrony danych osobowych,
- zagrożenia związane z kradzieżą lub wyłudzeniem danych osobowych w praktyce.

– w **2020** roku do dnia kontroli nie przeprowadzono szkoleń.

[akta kontroli str. 446-451]

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 78/20 Wójta Gminy Rozogi z dnia 25 września 2020 r. *w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w celu zachowania bezpieczeństwa przy przetwarzaniu mobilnym i pracy na odległość*, w załączniku Nr 14 określone zostały szczegółowo zasady pracy zdalnej z wykorzystaniem służbowego i prywatnego sprzętu do zadań służbowych.

Jednocześnie z uzyskanych podczas kontroli informacji wynika, że cyt.: „[redacted] *Stanowiska USC nie mogą pracować zdalnie gdyż ruch sieciowy z zewnątrz dla stanowiska z aplikacją Źródło jest całkowicie blokowany na routerze. Przygotowanie i do pracy zdalnej komputerów odnotowywane jest w dziennikach pracy informatyka.".*

[akta kontroli str. 606-620]

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.

W Urzędzie użytkowane są 2 systemy teleinformatyczne przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupione u zewnętrznych dostawców, tj.:

- PB_USC - autorem oprogramowania jest firma Technika IT Sp. z o.o., z którą podpisana została stosowna umowa [redacted], w zakresie asysty technicznej umożliwiająca prawidłową eksploatację i rozwój systemu. Urząd Gminy zawarł również z powyższą firmą umowę powierzenia danych gwarantującą bezpieczeństwo przetwarzanych w systemie danych, na wypadek awarii systemu oraz konieczności ingerencji firmy jako autora oprogramowania w bazy zawierające dane osobowe.
- PUMA - związku z zakupem ww. systemu podpisana została z firmą ZETO SOFTWARE Sp. z o.o. w Olsztynie umowa licencyjna [redacted], umożliwiająca prawidłową eksploatację i rozwój systemu poprzez możliwość zgłaszania błędów pytań i roszczeń dotyczących użytkowanego systemu. W treści umowy z firmą dostarczającą system informatyczny PUMA zawarto zapisy w zakresie powierzenia danych, gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawców w związku z realizacją umowy.

[akta kontroli str. 475-508]

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 zarządzeniami:

- Zarządzeniem Nr 77/18 Wójta Gminy Rozogi z dnia 7 września 2018 r. w sprawie

wprowadzenia Polityki Ochrony Danych – obowiązujące do 25 września 2020r. (Zał. 18)
- Zarządzeniem Nr 78/20 Wójta Gminy Rozogi z dnia 25 września 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych. (Zał. 18)

[akta kontroli str. 155-160, 260-268]

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 2018 r. do dnia rozpoczęcia czynności kontrolnych (8 października 2020 r.), w jednostce przeprowadzono 3 zadania audytowe w zakresie bezpieczeństwa informacji, tj.:
- w 2018 r. certyfikat AC/34/2018,
- w 2019 r. certyfikat AC/134/2019,
- w 2020 r. certyfikat AC/1222/2020.

[akta kontroli str. 326-329]

W związku z dopełnieniem obowiązku 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 - przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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.

W okresie objętym kontrolą zasady tworzenia kopii zapasowych uregulowane zostały:

- Zarządzeniem Nr 77/18 Wójta Gminy Rozogi z dnia 7 września 2018 r. w sprawie wprowadzenia Polityki Ochrony Danych – obowiązujące do 25 września 2020 r. (Zał. 13)
- Zarządzeniem Nr 78/20 Wójta Gminy Rozogi z dnia 25 września 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych. (Art. 23).

[akta kontroli str. 143-144, 188]

Z wyjaśnienia przekazanego z Urzędu w powyższej sprawie wynik, iż, cyt.: „[redacted]".

[akta kontroli str. 596-605, 606-620]

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 UG Rozogi wyjaśnił, że cyt.: „[redacted]".

[akta kontroli str. 509-544, 606-620]

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.

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 dostawcy zewnętrznego – PUMA, PB_USC. Na obsługę aktualnie zainstalowanego oprogramowania z firmami dostarczającymi dany system informatyczny zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej. Z zapisów dziennika czynności realizowanych przez informatyka wynika, że systemy teleinformatyczne były każdorazowo aktualizowane do najnowszej wersji.

Jednocześnie należy wspomnieć, iż obsługę informatyczną Urzędu zapewnia firma zewnętrzna, z którą Wójt podpisał stosowne umowy zarówno na zapewnienie bieżącej i nieprzerwanej obsługi w zakresie funkcjonowania sprzętu i oprogramowania, jak również powierzenia danych w ramach świadczonej usługi.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 456-474, 509-545]

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] *(...)".*

[akta kontroli str. 606-620]

Ponadto przyjęta zarządzeniem Nr 78/20 Wójta Gminy Rozogi Polityki Ochrony Danych Osobowych, zawiera tzw. "politykę kluczy" (art. 39), która definiuje sposób postępowania z kluczami w zakresie poszczególnych pomieszczeń Urzędu.
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:

- 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 PB_USC, logowanie indywidualnym loginem i hasłem,
- w systemie CEIDG logowanie odbywa się za pomocą certyfikatu kwalifikowanego i hasła.

Ponadto zgodnie z wyjaśnieniem uzyskanym w trakcie kontroli, cyt.: „(...)[redacted]"

[akta kontroli str. 606-620]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

- § 21 ust. 2 rozporządzenia KRI *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;*
- § 21 ust. 3 rozporządzenia KRI *poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka;*
- § 21 ust. 4 rozporządzenia KRI *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*

Z wyjaśnień uzyskanych z Urzędu w powyższej sprawie wynika, że cyt.: „[redacted]

[redacted]."

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 596-620]

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 zmianę wielkości czcionki oraz kontrastu w celu ułatwienia korzystania z treści na niej zawartych przez osoby niedowidzące. Zmiany wielkości czcionki dokonuje się przy pomocy ikony – A +. 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 wykazała 1 błąd - nie mający wpływu na realizację przedmiotowego zagadnienia, dla strony www. Urzędu nie wykazała błędów.

[akta kontroli str. 592-595]

Powyższe zagadnienie oceniono pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

W związku z tym, iż nie stwierdzono istotnych nieprawidłowości i uchybień w kontrolowanym zakresie odstępuje się od wydania zaleceń pokontrolnych.

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