WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 11 października 2021 r.

FK-IV.431.13.2021

Szanowny Pan
Bartłomiej Kłoczko
Wójt Gminy Kruklanki
ul. 22 Lipca 10
11-612 Kruklanki

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 Kruklanki[1], ul. 22 Lipca 10, 11-612 Kruklanki, NIP: 845 19 82 653, Regon: 790671248.

W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych stanowiska pełnili:

- Pan **Bartłomiej Kłoczko** - Wójt Gminy Kruklanki, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21 października 2018 r. (kierownik kontrolowanej jednostki).
- Pani **Barbara Ginkowska** - Sekretarz Gminy Kruklanki, zatrudniona na podstawie umowy o pracę od dnia 1 stycznia 2008 r. (nadzorujący bezpośrednio pracownika realizującego zadania objęte kontrolą).

W dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą w Urzędzie był Pan [redacted].

[akta kontroli str. 66]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko-Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – inspektor wojewódzki; przewodniczący zespołu kontrolnego,

[1] Zwanym dalej: Urzędem

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.0030.396.2021 z 9 sierpnia 2021 r., wydanego przez 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.0030.397.2021 z 9 sierpnia 2021 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 33-34]

Kontrolę przeprowadzono w dniach 17 sierpnia – 10 września 2021 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 2/2021.

[akta kontroli str. 67]

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 2021 r., poz. 670 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2019 r. do dnia 31 grudnia 2020 r.

[akta kontroli str. 1-2, 36-47]

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 tekst jednolity (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., Dz.U. z 2020 r., poz. 346 ze zm. - akt prawny obowiązujący do 12.04.2021 r. oraz Dz.U. z 2021 r., poz. 670

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

[akta kontroli str. 1-2, 36-47]

Wójt Gminy Kruklanki upoważnił Sekretarza Gminy Kruklanki oraz Inspektora ds. pozyskiwania środków budżetowych i informatyki do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli str. 68]

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z uchybieniami.**
Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez 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 **3** systemy teleinformatyczne:

1. Źródło (Rejestr PESEL, Rejestr Stanu Cywilnego, Rejestr Dowodów Osobistych),
2. PUMA (rejestr mieszkańców, rejestr wyborców),
3. 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:

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

meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego - gromadzenia i dostępu do danych historycznych mieszkańców.

Moduł Wyborcy - kompleksowa obsługa wyborów. Moduł Wyborcy umożliwia prowadzenie i aktualizację rejestru wyborców, sporządzanie spisów wyborców uprawnionych do udziału w wyborach i referendum, pozwala na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców mieście na podstawie bazy danych ewidencyjnych.

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

[akta kontroli str. 28-30]

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 **/kruklanki1/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. 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.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących

przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną. Jednocześnie należy zaznaczyć, iż Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych. W przypadku wybranych spraw załatwianych w Urzędzie, istnieje jednak możliwość złożenia wniosku w formie elektronicznej (np. ePUAP),
W związku z powyższym w BIP Urzędu zamieszczone zostały procedury postępowania określające sposób przyjmowania i załatwiania poszczególnych spraw w Urzędzie, w tym załatwianych przy pomocy wniosku elektronicznego zgodnie z § 5 ust. 2 pkt 1 i 4 KRI.
Obywatel ma prawo wiedzieć o wszystkich okolicznościach, które mogą wpłynąć na ustalenie jego praw i obowiązków w prowadzonym postępowaniu.

W ramach prowadzonych czynności kontrolnych ustalono, iż zarówno na stronie głównej Urzędu, jak i na stronie BIP znajduje się odnośnik do zakładki E-Usługi. Kontrolujący w ramach prowadzonych czynności kontrolnych stwierdzili, że podana zakładka nie działała, tj. nie było możliwości wejścia w podany odnośnik, w celu sprawdzenia jego przydatności.

[redacted]

Centralna Platforma E-Usług Mieszkańca to portal integrujący wszystkie dane z innych systemów, informacje o świadczonych e-usługach przez ePUAP, spersonalizowane dane podatkowe. Jest to główny system funkcjonalny z punktu widzenia mieszkańca działający na styku Klient - Urząd. Dzięki niemu mieszkańcy mają dostęp do wszystkich produktów wytworzonych w ramach projektu.
W szczególności portal zawiera:

1) Opisy wszystkich usług świadczonych przez urząd na platformie ePUAP, z których mieszkaniec może skorzystać w sposób elektroniczny;
2) Możliwość śledzenia postępu swoich spraw;
3) Podgląd swoich, spersonalizowanych danych o należnościach i zobowiązaniach z tytułu podatków i opłat lokalnych;
4) Możliwość dokonania płatności z tytułu podatków i opłat lokalnych;
5) Możliwość umówienia się na wizytę w Urzędzie.

Wymagania funkcjonalne:

1) Prowadzenie spraw w zakresie podatku od nieruchomości od osób fizycznych.
2) Prowadzenie spraw w zakresie podatku od nieruchomości od osób prawnych.
3) Prowadzenie spraw w zakresie podatku rolnego od osób fizycznych.
4) Prowadzenie spraw w zakresie podatku rolnego od osób prawnych.

5) Prowadzenie spraw w zakresie podatku leśnego od osób fizycznych.
6) Prowadzenie spraw w zakresie podatku leśnego od osób prawnych.
7) Prowadzenie spraw w zakresie podatku od środków transportowych.

Aplikacja jest zintegrowana z systemami bankowymi oraz systemem płatności Krajowej Izby Rozliczeniowej, w celu umożliwienia uregulowania należności online. E-Usługi w dniu 11.02.2021 r., zostały przyłączone do węzła krajowego systemu teleinformatycznego zgodnie z decyzją Ministra Cyfryzacji.

Ponadto na stronie BIP opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie. 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. 99-100, 226-232]

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.

Wójt Gminy w powyższej sprawie wyjaśnił, że cyt.: *„Gmina Kruklanki nie przekazywała do centralnego repozytorium żadnych wzorów dokumentów. Urząd korzysta za pośrednictwem platformy ePUAP Z PODSTAWOWEGO FORMULARZA „Pismo ogólne do urzędu" oraz formularzy umieszczonych w centralnym repozytorium, m.in.:*

1) *Dowody osobiste - obywatel gov.pl*
2) *Przyjmowanie petycji - epuap.gov.pl*
3) *Przyjmowanie skarg i wniosków-epuap.gov.pl*
4) *Udostępnienie danych z ewidencji ludności - epuap.gov.pl*
5) *Zezwolenie na świadczenie usług z zakresie opróżniania zbiorników bezodpływowych - epuap.gov.pl*
6) *Uzyskanie dofinansowania do kosztów usuwania azbestu - epuap*
7) *Udostępnienie danych w trybie jednostkowym z rej. D.O - epuap.gov.pl*
8) *Wniosek o udostępnienie informacji publicznej - epuap.gov.pl*
9) *Wniosek o wpisanie w rejestr wyborców - obywatel.gov.pl*
10) *Wniosek o wydanie decyzji o warunkach zabudowy - epuap.gov.pl*
11) *Wniosek o wydanie odpisu danych z rejestru D.O - epuap.gov.pl*
12) *Wniosek o wydanie zaświadczenia o przeznaczeniu nieruchomości - epuap.gov.pl*
13) *Wydanie zaświadczeń - epuap.gov.pl*
14) *Ochrona przed bezdomnymi zwierzętami - epuap.gov.pl."*

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

[akta kontroli str. 15-27, 111-112, 227-232]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.3. Model usługowy

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

Strona internetowa Urzędu działa pod adresem https://www.kruklanki.pl/pl/, a strona internetowa BIP Urzędu – pod adresem https://bipkruklanki.warmia.mazury.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu, w prawej górnej części panelu strony. Na stronie głównej BIP Urzędu w zakładce ePUAP zamieszczono ścieżkę do skrzynki podawczej ESP na platformie ePUAP.
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. 227-232]

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 zarządzenia nr 81/2015 Wójta Gminy Kruklanki z dnia 8.12.2015 r. w sprawie wykonywania czynności kancelaryjnych w Urzędzie Gminy w Kruklankach, 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. System tradycyjny czynności kancelaryjnych jest systemem polegającym na dokumentowaniu przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci papierowej z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentacji w tej postaci.
W okazanej dokumentacji Urzędu (obowiązującej w okresie objętym kontrolą) brak było procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów (np. skrzynka podawcza na platformie ePUAP), 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.

Jednocześnie należy zaznaczyć, że w przedstawionym kontrolerom zarządzeniu nr 43/2021 Wójta Gminy Kruklanki z dnia 30.06.2021r. w sprawie wykonywania czynności kancelaryjnych w Urzędzie Gminy w Kruklankach, (przyjętym poza okresem objętym kontrolą) zawarto już zapisy w dotyczące przygotowania i wysyłki korespondencji elektronicznej na platformie ePUAP.

[akta kontroli str. 15-27, 113-120]

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. 227-232]

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 w ramach dokumentacji wchodzącej w skład SZBI przyjęto:

- Zarządzenie Nr 36/2018 Wójta Gminy Kruklanki z dnia 29 czerwca 2018r. w sprawie Polityki Ochrony Danych w Urzędzie Gminy w Kruklankach.

- Zarządzenie Nr 41/2020 Wójta Gminy Kruklanki z dnia 23 lipca 2020 zmieniające zarządzenie w sprawie Polityki Ochrony Danych w Urzędzie Gminy w Kruklankach.

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.

[akta kontroli str. 121-139]

Ponadto w ramach tworzenia systemy zarzadzania bezpieczeństwem informacji w Urzędzie przyjęto:

- Zarządzenie Nr 17/2020 Wójta Gminy Kruklanki z dnia 17 marca 2020 r. w sprawie wprowadzenia i zatwierdzenia dokumentacji bezpieczeństwa Systemu Monitoringu Wizyjnego, w skład którego weszła Polityka ochrony danych osobowych przetwarzanych w systemie monitoringu wizyjnego, Instrukcja zarządzania systemem monitoringu wizyjnego oraz Plan systemu monitoringu wizyjnego.

- *Procedura pracy z wykorzystaniem systemów zdalnego dostępu do danych.* Procedura ma na celu zapewnienie zgodności działań administratora danych osobowych w zakresie wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych, dla zapewnienia adekwatnego stopnia bezpieczeństwa odpowiadającego określonemu ryzyku naruszenia praw lub wolności osób fizycznych

o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celu przetwarzania, w związku z rozwiązaniem technologicznym zakładającym możliwość wykorzystania w procesie dostępu do zasobów danych rozwiązań technicznych i informatycznych umożliwiających zdalny dostęp upoważnionego personelu.

- Zarządzenie nr 70/2020 Wójta Gminy Kruklanki z dnia 19.11.2020r. w sprawie Regulaminu pracy zdalnej w celu przeciwdziałania COVID-19 w Urzędzie Gminy w Kruklankach

[akta kontroli str. 101-110, 140-188]

Wójt Gminy Kruklanki zarządzeniami nr 35/2018 z dnia 22 czerwca 2018 r. (obowiązywało do dnia 4 kwietnia 2019 r.) oraz nr 23/2019 z dnia 4 kwietnia 2019 r. powołał w jednostce Inspektora Ochrony Danych (IOD).

[akta kontroli str. 189-191]

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.

Z informacji przekazanych przez Urząd w powyższej sprawie wynika, że cyt.: [redacted]

W czasie prowadzonych czynności kontrolnych ustalono, iż działaniami podjętymi w celu prowadzenia monitorowania, przeglądania oraz doskonalenia SZBI w jednostce (oprócz realizowanego audytu) były przeprowadzane cyklicznie kontrole uprawnień i kont użytkowników, które zgodnie z założeniami polityki pkt – 18.1 przeprowadzano co najmniej raz na pół roku. W dniach 27 - 28 kwietnia 2020 r. przeprowadzona została również

weryfikacja przechowywania przez upoważnionych pracowników dokumentów zawierających dane wrażliwe.

Ponadto, z wyjaśnienia złożonego wraz z pismem znak: [redacted]

[akta kontroli str. 218-221, 227-232, 307, 339-340]

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.

Kontrolującym przedstawiono dokumentację (akta kontroli) świadczącą o przeprowadzeniu szacowania i analizy ryzyka utraty integralności, dostępności lub poufności informacji w okresie objętym kontrolą.
Proces szacowania i analizy ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.

[akta kontroli str. 283-306]

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

[akta kontroli str. 272-279]

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.

[akta kontroli str. 233-235]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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 w zarządzeniu Nr 36/2018 Wójta Gminy Kruklanki z dnia 29 czerwca 2018r. w sprawie Polityki Ochrony Danych w Urzędzie Gminy w Kruklankach, zmienionym zarządzeniem Nr 41/2020 Wójta Gminy Kruklanki z dnia 23 lipca 2020 – rozdział 7.4 oraz 12.1.

[akta kontroli str. 122-138]

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). Ponadto zgodnie z przyjętą polityką ochrony danych - rozdział 18.1, co najmniej raz na pół roku dokonywana była kontrola uprawnień, o czym szczegółowo w pkt 2.1 PWP.

[akta kontroli str. 210-221, 224-225]

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 jednym szkoleniu (zorganizowanym przez IOD), dotyczącym ochrony danych osobowych.
Szkolenie przeprowadzone w 2019 dotyczyło zasad przetwarzania danych, bezpiecznej poczty elektronicznej, zmian w związku z wejściem w życie ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego 1 Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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).
W załączeniu przedstawiono listę obecności pracowników uczestniczących w szkoleniu.

Na zadane przez kontrolujących pytanie dotyczące podania przyczyny braku przeprowadzonych szkoleń pracowników Urzędu w zakresie dotyczącym ochrony danych osobowych w 2020 r., Urząd wyjaśnił, że cyt.: [redacted]

[akta kontroli str. 227-232, 236-242]

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.*

W zarządzeniu Nr 36/2018 Wójta Gminy Kruklanki z dnia 29 czerwca 2018r. w sprawie Polityki Ochrony Danych w Urzędzie Gminy w Kruklankach oraz zarządzeniu Nr 41/2020 Wójta Gminy Kruklanki z dnia 23 lipca 2020 zmieniającym zarządzenie w sprawie Polityki Ochrony Danych w Urzędzie Gminy w Kruklankach, określono zarys zasad postępowania przy użytkowaniu komputerów przenośnych.

Ponadto w Urzędzie opracowana został i przyjęta do stosowania *Procedura pracy z wykorzystaniem systemów zdalnego dostępu do danych*. Procedura ma na celu zapewnienie zgodności działań administratora danych osobowych w zakresie wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych, dla zapewnienia adekwatnego stopnia bezpieczeństwa odpowiadającego określonemu ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, i celu przetwarzania, w związku z rozwiązaniem technologicznym zakładającym możliwość wykorzystania w procesie dostępu do zasobów danych rozwiązań technicznych i informatycznych umożliwiających zdalny dostęp upoważnionego personelu.
W celu zapewnienia ciągłości działania Urzędu na wypadek konieczności realizacji pracy zdalnej przez pracowników, przyjęto do realizacji zarządzenie nr 70/2020 Wójta Gminy Kruklanki z dnia 19.11.2020r. w sprawie Regulaminu pracy zdalnej w celu przeciwdziałania COVID-19 w Urzędzie Gminy w Kruklankach. W 2020 roku czworo pracowników Urzędu świadczyło pracę zdalnie.

[akta kontroli str. 101-110, 121-139, 181-188, 248-251]

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.

Zgodnie z procedurą wykonywania przeglądów i konserwacji systemów i nośników informacji służących do przetwarzania danych, ujętą w zarządzeniu Nr 36/2018 Wójta Gminy Kruklanki z dnia 29 czerwca 2018r. w sprawie Polityki Ochrony Danych w Urzędzie Gminy w Kruklankach, zmienionym zarządzeniem Nr 41/2020 Wójta Gminy Kruklanki z dnia 23 lipca 2020 - rozdział 12.4 - informatyk jest odpowiedzialny za dokonywanie przeglądu i konserwacji systemów oraz nośników służących do przetwarzania danych.
W Urzędzie użytkowany jest jeden system teleinformatyczny przeznaczone do realizacji zadań zleconych z zakresu administracji rządowej zakupiony u zewnętrznego dostawcy, tj.:
[redacted]

Z powyższą firmą zawarta została również stosowna umowa powierzenia danych gwarantująca właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli str. 192-205]

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 36/2018 Wójta Gminy Kruklanki z dnia 29 czerwca 2018r. w sprawie Polityki Ochrony Danych w Urzędzie Gminy w Kruklankach, zmienionym zarządzeniem Nr 41/2020 Wójta Gminy Kruklanki z dnia 23 lipca 2020 – rozdział 17, załącznik nr 18.

[akta kontroli str. 121-138, 222-223]

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 2 zadania audytowe w zakresie bezpieczeństwa informacji, tj.:

- w listopadzie 2019 r. dokument – Audyt – analiza stanu faktycznego bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Kruklanki,
- w grudniu 2020 r. dokument Audyt – analiza stanu faktycznego bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Kruklanki.

Przeprowadzone zadania audytowe obejmowały m.in. następujące zagadnienia:

- Inwentaryzacja sprzętu i oprogramowania,
- Analizę ryzyka,
- Uprawnienia osób zaangażowanych w proces przetwarzania danych,

- Bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania danych,
- Szkolenia,
- Ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- Urządzenia mobilne i praca na odległość,
- Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie,
- modyfikacje, usunięcie lub zniszczenie,
- Weryfikacje umów serwisowych zawieranych ze stronami trzecimi pod kątem zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
- Zasady postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
- Poziom bezpieczeństwa w systemach teleinformatycznych,
- Incydenty związane z naruszeniem bezpieczeństwa informacji,
- Okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji,

[akta kontroli str. 69-98]

Na podstawie przekazanej dokumentacji kontrolujący stwierdzili, że w okresie objętym kontrolą obowiązek wynikający 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 - został zrealizowany.

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.

Z informacji przekazanych przez Urząd w powyższej sprawie wynika, że cyt.: [redacted]

Zgodnie z przekazaną kontrolującym dokumentacją ([redacted]) obowiązek minimalizowania ryzyka utraty informacji w wyniku awarii, poprzez wykonywanie i testowanie kopii zapasowych jest realizowany.

[akta kontroli str. 227-232, 254-271]

Jednocześnie kontrolujący zwracają uwagę na brak opracowanych regulacji wewnętrznych w których określone byłyby zasady tworzenia, przechowywania oraz testowania kopii zapasowych danych ze wszystkich systemów podmiotu kontrolowanego (dzienniki wykonywania kopii jak również protokoły z testów odtworzeniowych). [redacted]

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 [redacted]

Na obsługę aktualnie zainstalowanego oprogramowania z firmą zewnętrzną dostarczającą dany system informatyczny zawarta została stosowna umowa licencyjna (opieka autorska), gwarantująca rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

[akta kontroli str. 192-205]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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.

[redacted]

[akta kontroli str. 227-232]

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, cyt.: [redacted]

[akta kontroli str. 227-232]

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 cyt.:

[redacted]

[akta kontroli str. 227-232]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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. W toku kontroli dokonano jednak weryfikacji zgodności ze standardem WCAG 2.0 strony internetowej Urzędu oraz BIP Urzędu.
Dostępność strony internetowej oznacza, że może z niej skutecznie korzystać każdy na dowolnej aplikacji klienckiej, na dowolnym urządzeniu, z dowolnego rodzaju połączenia, w każdych warunkach, bez względu na sprawność swoich zmysłów. Podmioty publiczne zobowiązane są do zapewnienia dostępności cyfrowej swoich stron. Zapewnienie dostępności cyfrowej stron internetowych oznacza spełnienie wielu kryteriów sukcesu zdefiniowanych w Web Content Accessibility Guidelines (WCAG 2.1). Wytyczne wymagają spełnienia czterech głównych zasadami, którymi są:

1. postrzegalność,
2. funkcjonalność,
3. zrozumiałość,
4. kompatybilność.

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.

Zgodnie z publikowaną w BIP Deklaracją dostępności Biuletynu Informacji Publicznej Urzędu Gminy w Kruklankach oraz Portalu Internetowego Gminy Kruklanki strona internetowa jest częściowo zgodna z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 Portalu Internetowego Urzędu wykazała 32 błędy, natomiast walidacja strony BIP nie wykazała istotnych błędów. WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga projektantom i administratorom tworzyć bardziej dostępne strony internetowe. Wprawdzie nie odpowiada do końca na pytanie, czy zawartość serwisu jest dostępna, bo to może uczynić tylko człowiek-użytkownik, ale poglądowo wskazuje miejsca, które mogą powodować problemy z dostępnością.

[redacted]

Mając powyższe na uwadze, należy stwierdzić, że Portal Internetowy Urzędu zawiera pewne elementy umożliwiające korzystanie z treści na nim zawartych przez osoby niepełnosprawne, w tym niedowidzące, tj. zmiana kontrastu strony, funkcja powiększania i pomniejszania tekstu na podstronach. W związku z tym brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, w tym niepełne dostosowanie portalu do standardów WCAG 2.0, należy ocenić jako uchybienie. Osobą odpowiedzialną za powstanie uchybienia jest Kierownik kontrolowanej jednostki.

[akta kontroli str. 243-245, 246-247, 280-282]

Powyższe zagadnienie oceniono pozytywnie z uchybieniami.

Do projektu wystąpienia pokontrolnego z dnia 21 września 2021 r., pismem znak: OR.1710.1.2021, z dnia 24 września 2021 r. zostały złożone przez Sekretarza Gminy Kruklanki z upoważnienia Wójta Gminy zastrzeżenia, w których jednostka kontrolowana nie zgadzała się z zapisem zawartym w p.w.p. stanowiącym, że: *w okresie objętym kontrolą jedynymi działaniami podjętymi w celu prowadzenia monitorowania, przeglądania oraz doskonalenia SZBI w jednostce (oprócz realizowanego audytu) były przeprowadzane cyklicznie kontrole uprawnień i kont użytkowników, które zgodnie z założeniami polityki pkt – 18.1 przeprowadzano co najmniej raz na pół roku oraz przeprowadzona w dniach 27 - 28 kwietnia 2020 r. weryfikacja przechowywania przez upoważnionych pracowników dokumentów zawierających dane wrażliwe.*
Powyższe zastrzeżenia zostały uwzględnione w całości (co znalazło odzwierciedlenie w wystąpieniu pokontrolny), a stanowisko Kierownika komórki ds. kontroli w tym zakresie, przekazane zostało jednostce pismem z dnia 29 września 2021 r., znak j.w.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Uzupełnienie dokumentacji SZBI o opracowane regulacje, w zakresie tworzenia i testowania kopii zapasowych zgodnie z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI.

2. Podjęcie działań w celu osiągnięcia pełnej zgodności Portalu Internetowego Urzędu z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, w tym dostosowanie portalu do standardów WCAG 2.0.

W związku ze stwierdzonym podczas realizacji czynności kontrolnych uchybieniem, tj. brakiem w okresie objętym kontrolą, w dokumentacji dotyczącej wykonywania czynności kancelaryjnych w Urzędzie procedur, w których określone byłyby zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną, odstępuje się od wydania zaleceń pokontrolnych w tym zakresie, ze względu na opracowanie powyższych procedur w 2021 roku.

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