WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 2 czerwca 2022 r.

Znak: K-2.431.1.12.2022.9.IO

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	Działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.
Nazwa i adres organu kontrolującego	Wojewoda Zachodniopomorski, ul. Wały Chrobrego 4, 70-502 Szczecin
Nazwa i adres organu kontrolowanego	Wójt Gminy Rąbino, Rąbino 27, 78-331 Rąbino
Osoba pełniąca funkcję Wójta Gminy Rąbino w okresie objętym kontrolą / okresie prowadzenia kontroli	Pani Aneta Krawiec
Okres objęty kontrolą	od dnia 1 stycznia 2019 r. do dnia 1 marca 2022 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: 1. Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego*, 2. Pani Iwona Olesińska – inspektor wojewódzki.
Nr upoważnienia	Nr 13/22 z dnia 15 lutego 2022 r.
Podstawy prawne do przeprowadzenia kontroli	– art. 6 ust. 4 pkt 3 w związku z art. 2 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1]; – art. 25 ust. 1 pkt 3 lit. a, w związku z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2].
Kryteria prowadzenia kontroli	legalność, rzetelność
Termin kontroli	16 lutego-1 marca 2022 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły[3]

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2021r., poz. 2070.

Obszar kontroli Nr 1	Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
1.1 Współpraca systemów teleinformatycznych z innymi systemami	
Podstawa prawna	**§ 5 ust. 3 pkt 3 rozporządzenia KRI[4]:** *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.*
Ustalenia kontroli Na podstawie przedstawionej dokumentacji oraz oświadczenia Wójta Gminy z dnia 10 lutego 2022 r. ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Rąbino wykorzystywano jeden system centralny (aplikacja Źródło) oraz systemy informatyczne wspomagające obsługę spraw obywatelskich: Rejestr Mieszkańców- system SELWIN oraz Rejestr Wyborców – system RWWIN (oprogramowanie firmy XXX). System centralny (aplikacja Źródło), dostępny przez stronę WWW podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu Gminy. Systemy do realizacji zadań zleconych z zakresu administracji rządowej, współpracują z systemem zewnętrznym oraz spełniają minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu i systemami innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. (dowód: akta kontroli str. 41, 56, 58)	
1.2 Formaty danych udostępniane przez systemy teleinformatyczne	
Podstawa prawna	**§ 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*

[3] Mając na względzie obowiązujący na obszarze Rzeczypospolitej Polskiej stan epidemii (rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r., Dz. U. z 2022r., poz. 340) przedmiotowe czynności na podstawie art. 21 ustawy o kontroli w administracji rządowej, przeprowadzone zostały poza siedzibą podmiotu kontrolowanego, o czym Wójt Gminy Rąbino został poinformowany w piśmie z dnia 10 lutego 2022 r. (dowód: akta kontroli str. 20).

[4] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. 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), zwane dalej „rozporządzeniem KRI".

	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*
Ustalenia kontroli Systemy informatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Rąbino, zgodnie z oświadczeniem Wójta Gminy z dnia 10 lutego 2022 r wymieniały dane w formacie .xml. Tym samym spełniony został warunek określony w § 18 ust. 1 rozporządzenia KRI o udostępnianiu zasobów informacyjnych w co najmniej jednym z formatów wymienionych w załączniku nr 2 do rozporządzenia. (dowód: akta kontroli str. 56)	
Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1: - nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.	
Ocena obszaru kontroli nr 1	**Pozytywna**
Obszar kontroli Nr 2	System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.
2.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu	
Podstawa prawna	**§ 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 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.* **§ 20 ust. 3 rozporządzenia KRI:** *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą.*
Ustalenia kontroli Wymagania dotyczące systemów teleinformatycznych, w których przetwarzane były rejestry publiczne w postaci teleinformatycznej określone zostały w § 20 ust. 1 rozporządzenia KRI.	

Zgodnie z tym przepisem, podmiot realizujący zadania publiczne miał obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność i integralność informacji.
W Urzędzie Gminy Rąbino, w okresie objętym kontrolą obowiązywały następujące uregulowania w zakresie bezpieczeństwa informacji:

- *Zarządzenie Nr 48/07 Wójta Gminy Rąbino z dnia 12 grudnia 2007 r. w sprawie ustalenia Polityki bezpieczeństwa dla systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Rąbino (*okres funkcjonowania regulacji: 12 grudnia 2007 r.- 11 września 2019 r.)
- *Zarządzenie Nr 68/2019 Wójta Gminy Rąbino z dnia 12 września 2019 r. w sprawie wdrożenia Systemu Zarzadzania Bezpieczeństwem Informacji w Urzędzie Gminy Rąbino* (okres funkcjonowania regulacji: 12 września 2019 r.- 13 października 2021 r.).

Ustalono, że w ciągu okresu obowiązywania dokumentacja nie była aktualizowana, co skutkowało brakiem wdrożenia wymogów obowiązującego od dnia 12 kwietnia 2012r. rozporządzenia KRI. Procedury nie zawierały elementów określonych w rozporządzeniu KRI i ograniczały się do zagadnień związanych z ochroną danych osobowych, czym nie wypełniały dyspozycji ww. rozporządzenia. Ponadto stwierdzono, że do czasu wprowadzenia Systemu Zarzadzania Bezpieczeństwem Informacji (*Nr 68/2019 Wójta Gminy Rąbino z dnia 12 września 2019 r*) obowiązująca dokumentacja nie była zaktualizowana pod kątem dostosowania zapisów do obowiązujących od dnia 25 maja 2018 r. przepisów Rozporządzenia Parlamentu Europejskiego i 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)[5].

- *Zarządzenie Nr 55/2021 Wójta Gminy Rąbino z dnia 14 października 2021 r. w sprawie wprowadzenia w życie dokumentacji opisującej i zapewniającej bezpieczeństwo informacji w Urzędzie Gminy Rąbino* (okres funkcjonowania regulacji - od 14 października 2021 r.)

Zarządzenie powyższe wprowadza procedury zapewniające bezpieczeństwo informacji w Urzędzie, na które składają się następujące dokumenty:

- System Zarządzania Bezpieczeństwem lnformacji wraz z następującymi załącznikami:
  Procedura zwrotu sprzętu informatycznego przypisanego Użytkownikom,
  Procedura instalacji oprogramowania na stacjach roboczych pracowników,
  Plan ciągłości działania u Administratora,
  Procedura odtwarzania systemu po awarii (katastrofie) oraz testowania,
- Polityka Bezpieczeństwa Informacji,
- Polityka Bezpieczeństwa Przetwarzania Danych Osobowych,
- Instrukcja Zarządzania Systemem Informatycznym,
- Instrukcja Postępowania z Incydentami Bezpieczeństwa Informacji i w Sytuacjach Naruszenia Ochrony Danych Osobowych,
- Instrukcja Zarządzania Ryzykiem i Metodyka Szacowania Ryzyka Przetwarzania Danych Osobowych,

[5] Dz. Urz. UE L2016.119, zwane dalej rozporządzeniem *RODO.*

- Procedura RODO dotycząca Ochrony Danych osobowych w Fazie Projektowania i Domyślnej Ochrony Danych (Privacy by Design/by Default) i Oceny Skutków dla Ochrony Danych Osobowych,
- Procedura Obsługi Żądań Podmiotu Danych Osobowych w Trybie Wnioskowym,
- Procedura RODO dotycząca Przetwarzania Danych Osobowych,
- Procedura Retencji Danych Osobowych,
- Instrukcja Pełnienia Funkcji Inspektora Ochrony Danych,
- Procedura Współpracy z Organem Nadzorczym,
- Procedura Wyboru Dostawcy Przetwarzającego Dane Osobowe,
- Dokumenty Powiązane.

W wyniku analizy aktualnie obowiązującej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonująca dokumentacja spełnia wymogi określone w § 20 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. Dyrektywa § 20 ust. 2 pkt 1 rozporządzenia KRI wskazuje na konieczność *zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.* Stwierdzono, że obowiązująca w Jednostce dokumentacja była poddana przeglądowi i weryfikacji pod kątem jej aktualizacji, na co wskazują zapisy w historii zmian analizowanych dokumentów.

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Rąbino wdrożono system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność działań.

W związku z powtarzającymi się przypadkami powielania w różnych dokumentach obowiązujących w Urzędzie regulacji uwzględniających tożsame zagadnienia, kontrolujący sugerują stworzenie jednolitego tekstu procedur normujących te kwestie, co pozwoli na szybsze, bardziej intuicyjne odnalezienie a przede wszystkim kompleksowe zastosowanie odpowiednich zapisów i regulacji.

(dowód: akta kontroli str. 57, 62-132, 183-597)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji

Podstawa prawna	**§ 20 ust. 2 pkt 3 rozporządzenia KRI:** *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.*

Ustalenia kontroli

Zasady zarządzania ryzykiem, metody przeprowadzania analiz ryzyka utraty integralności, dostępności lub poufności informacji uwzględniono w dokumencie *Instrukcja zarządzania ryzykiem. Metodyka Szacowania Ryzyka Przetwarzania Danych Osobowych.* Ponadto w procedurze sformułowano wytyczne do oceny prawdopodobieństwa wystąpienia i następstw ryzyka; określono metodykę szacowania i sposób postępowania z ryzykiem, w celu jego monitorowania i zapobiegania lub minimalizacji jego materializacji. W *Polityce bezpieczeństwa informacji w Urzędzie Gminy Rąbino,* w rozdziale 9 *Zarządzanie ryzykiem bezpieczeństwem informacji* określono częstotliwość przeprowadzania analiz ryzyka i wskazano osoby odpowiedzialne za ich opracowanie.

W okresie objętym kontrolą, w Urzędzie Gminy Rąbino przeprowadzono jedną analizę ryzyka. Wyniki analizy przedstawiono kontrolującym w postaci dokumentu - *Analiza ryzyka w Urzędzie Gminy Rąbino w 2021r.,* z którego wynika, że dla zdefiniowanych w Jednostce zasobów zidentyfikowano niski poziom ryzyka.

W latach 2019 i 2020, zgodnie z wyjaśnieniami Wójta Gminy Rąbino z dnia 21 lutego 2022r. w Urzędzie nie przeprowadzono analizy ryzyka utraty integralności, dostępności lub poufności informacji.
Procedura szacowania ryzyka powinna być przeprowadzana okresowo, jednak zawsze w przypadku pojawienia się nowych zagrożeń, co wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie. Zaleca się, aby zarządzanie ryzykiem w bezpieczeństwie informacji było integralną częścią wszystkich działań związanych z tym obszarem oraz zostało zastosowane zarówno do wdrożenia, jak i w ciągłej eksploatacji SZBI.

(dowód: akta kontroli str. 57, 133-140, 367-385)

2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego

Podstawa prawna	**§ 20 ust. 2 pkt 2 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

Ustalenia kontroli

Zgodne z § 20 ust. 2 pkt 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ponadto, zgodnie z pkt 8.1.1 normy PN-ISO/IEC 27002:2014, wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis.
Inwentaryzacja zasobów informatycznych w Urzędzie jest realizowana przy wykorzystaniu programu Word. Dane dotyczące sprzętu i oprogramowania ujmowane są w postaci *Kart użytkownika urządzeń informatycznych i osobistego wyposażenia*. Kontrolującym przedstawiono *Kartę użytkownika urządzeń informatycznych (..)* osoby, która realizuje zadania zlecone z zakresu administracji rządowej. Karta zawiera między innymi informacje dotyczącą rodzaju sprzętu, rodzaju systemu operacyjnego, zainstalowanego oprogramowania oraz współpracujących urządzeń peryferyjnych.
Jednym z obowiązkowych elementów procesu zapewnienia bezpieczeństwa informatycznego jest gromadzenie bieżących informacji w zakresie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmujących ich rodzaj i konfigurację. Brak informacji o posiadanych zasobach informatycznych służących do przetwarzania danych, w przypadku wystąpienia awarii lub innego zdarzenia losowego może znacząco utrudnić szybkie odtworzenie infrastruktury, w celu zapewnienia ciągłości działania.

(dowód: akta kontroli str. 57, 165-167)

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych

Podstawa prawna	**§ 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.

Ustalenia kontroli

Przepisy § 20 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI stanowią m.in, że kierownictwo podmiotu publicznego w celu zapewnienia bezpieczeństwa informacji powinno podjąć działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, adekwatne do realizowanych zadań, a także podjąć bezzwłoczne działania w przypadku zmiany zadań tych osób.

Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby, w ustalonym zakresie. Kwestie nadawania i odwoływania uprawnień do przetwarzania danych osobowych oraz nadawania, modyfikacji oraz odbierania uprawnień użytkownikom do pracy w systemach informatycznych uregulowane są w następujących dokumentach:

- *System zarzadzania bezpieczeństwem informacji w Urzędzie Gminy Rąbino,* w rozdziale 3 *Zasady zarządzania dostępem do informacji,*
- *Polityka Bezpieczeństwa Przetwarzania Danych Osobowych,* w rozdziale 7 *Osoby upoważnione do przetwarzania danych osobowych* oraz rozdziale 10 *Upoważnienia do przetwarzania danych osobowych przez pracowników,*
- *Instrukcja Zarządzania Systemem Informatycznym* w rozdziale 3 *Nadawanie i rejestrowanie uprawnień,*
- *Polityka Bezpieczeństwa Informacji* w rozdziale 7 *Zarządzanie dostępem.*

W wyniku analizy obowiązującej dokumentacji stwierdzono, że:

- realizowanie wymogu dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych, w postaci pisemnego wniosku osób upoważnionych, powoduje, że proces nadawania i odbierania uprawnień jest w pełni potwierdzony;
- w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem wprowadzono zabezpieczenia polegające m.in. na konieczności logowania się do systemów informatycznych z wykorzystaniem unikalnego identyfikatora oraz hasła o odpowiedniej złożoności.

Kontrolującym przedstawiono upoważnienia do przetwarzania danych osobowych wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Ponadto przedłożono oświadczenie o zapoznaniu się z *Polityką bezpieczeństwa dla systemów informatycznych* oraz deklarację zobowiązującą do zachowania w tajemnicy pozyskanych danych, w czasie zatrudnienia jak i po ustaniu stosunku pracy.

W trakcie kontroli nie dokonano sprawdzenia blokowania/modyfikacji dostępu do systemów informatycznych, ponieważ w okresie podlegającym badaniu, nie wystąpiły przypadki cofania lub modyfikowania uprawnień nadanych pracownikom realizującym zadania zlecone z zakresu administracji rządowej, w systemach objętych kontrolą.

Z uwagi na fakt, że kontrola prowadzona była w trybie zdalnym nie dokonano oględzin stanowisk komputerowych.

(dowód: akta kontroli str. 57, 141-144, 193-196, 198-200, 266-269, 317-318, 571-572)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Podstawa prawna	**§ 20 ust. 2 pkt 6 rozporządzenia KRI:** *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.

Ustalenia kontroli

W okresie objętym kontrolą w Urzędzie przeprowadzono jedno szkolenie pracowników. Szkolenie odbyło się 30 listopada 2021 r. Udział w szkoleniu dokumentowała lista obecności zawierająca imię i nazwisko uczestnika oraz jego własnoręczny podpis, stanowisko służbowe i datę szkolenia. Stwierdzono, że w szkoleniu uczestniczyli pracownicy zaangażowani w proces przetwarzania informacji w systemach teleinformatycznych oraz rejestrach publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej (będących przedmiotem kontroli).

Z udostępnionej *Karty szkolenia wstępnego/okresowego z zakresu ochrony danych osobowych*, dokumentującej treści poruszone w trakcie kursu wynika, że jego zakres tematyczny nie obejmował wszystkich zagadnień wskazanych w § 20 ust. 2 pkt 6 rozporządzenia KRI.

Szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych winny mieć charakter cykliczny i obejmować zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI. Szkolenie przeprowadzone w Urzędzie nie wypełnia dyspozycji wyżej przywołanego rozporządzenia.

(dowód: akta kontroli str. 57, 168-170)

2.6 Praca na odległość i mobilne przetwarzanie danych

Podstawa prawna	**§ 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.*

Ustalenia kontroli

Tryb pracy na komputerach przenośnych i sprzęcie mobilnym został unormowany w następujących dokumentach:

- *Regulamin użytkowania komputerów przenośnych i mobilnych nośników danych przez pracowników w Urzędzie Gminy Rąbino*,
- *System zarzadzania bezpieczeństwem informacji w Urzędzie Gminy Rąbino*, w rozdziale 7 *Zasady bezpieczeństwa przy korzystaniu ze sprzętu przenośnego, bezpiecznej pracy w przypadku dostępu zdalnego, postępowania w przypadku naruszeń i realizacja szkoleń z bezpiecznego użytkowania SI.*

W powyższych regulacjach określono zasady oraz tryb pracy na komputerach i innych urządzeniach przenośnych, z uwzględnieniem niezbędnych zabezpieczeń, w tym szyfrowania twardych dysków. Kwestie ochrony kryptograficznej ujęto w *Systemie zarzadzania bezpieczeństwem informacji w Urzędzie Gminy Rąbino*, w rozdziale 14.

W Urzędzie Gminy wprowadzono również *Procedurę pracy zdalnej i stacjonarnej z danymi osobowymi w okresie pandemii* oraz *Regulamin pracy zdalnej*, gdzie zawarto zasady podejmowania i realizowania pracy w okresie epidemii.

W związku z wprowadzonymi uregulowaniami należy stwierdzić, że w Urzędzie opracowano i wdrożono procedurę w zakresie bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, w myśl dyspozycji § 20 ust. 2 pkt 8 rozporządzenia KRI.

Zgodnie z wyjaśnieniami Wójta Gminy z dnia 10 lutego 2022 r. do realizacji zadań zleconych z zakresu administracji rządowej nie wykorzystywano urządzeń mobilnych.

(dowód: akta kontroli str. 56, 209-212, 232-234, 306-307, 530-546)

2.7 Serwis sprzętu informatycznego i oprogramowania	
Podstawa prawna	**§ 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.*

Ustalenia kontroli

Obsługa informatyczna realizowana jest przez pracownika zatrudnionego w Urzędzie Gminy w Rąbinie, na stanowisku Informatyka. W zakresie obowiązków pracownika znajduje się m.in.: administrowanie systemem informatycznym Urzędu; zapewnienie ciągłości działania, aktualizację i rozbudowę systemu; nadzór nad eksploatacją i konserwacją systemu informatycznego; nadzór nad bezpieczeństwem danych; przeciwdziałanie dostępowi do systemu osób niepowołanych; bieżąca naprawa i konserwacja sprzętu komputerowego i archiwizowanie danych pochodzących z systemów informatycznych.

W celu realizacji zadań z zakresu administracji rządowej zawarto XXX, której przedmiotem jest prowadzenie nadzoru i serwisu oprogramowania użytkowanych systemów SELWIN, RWWIN, USCWIN[6]. Stwierdzono, że w powyższej umowie nie wprowadzono zapisów określających maksymalny czas skutecznej naprawy oprogramowania, powyższym nie wypełniono dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI, zawierającego zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

W załączniku do wyżej opisanej umowy określono zasady powierzenia przetwarzania danych osobowych.

(dowód: akta kontroli str. 171-182)

2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji	
Podstawa prawna	**§ 20 ust. 2 pkt 13 rozporządzenia KRI:** *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.*

Ustalenia kontroli

Zasady reagowania i postępowania w sytuacjach naruszenia bezpieczeństwa informacji uregulowano w *Instrukcji postępowania z incydentami bezpieczeństwa informacji i w sytuacjach naruszenia ochrony danych.* W powyżej przywołanej instrukcji przedstawiono także katalog form naruszeń bezpieczeństwa informacji oraz wskazano osoby odpowiedzialne za wdrożenie odpowiednich działań po stwierdzeniu incydentu.

Kwestie zasad i sposobu postępowania w przypadku wystąpienia incydentów naruszenia bezpieczeństwa informacji uregulowano także w dokumencie - *System zarzadzania bezpieczeństwem informacji w Urzędzie Gminy Rąbino,* w rozdziale 18 *Zarządzanie incydentami naruszenia bezpieczeństwa informacji; Polityce bezpieczeństwa informacji w Urzędzie Gminy Rąbino,* w rozdziale 10 *Zarządzanie incydentami* oraz *Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Rąbino,* w rozdziale 20 i 21 (gdzie określono zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych).

W trakcie kontroli kontrolującym przedstawiono *Rejestr naruszeń ochrony danych osobowych*, który zawierał jeden wpis. Wpis nie dotyczył przypadku naruszenia ochrony danych osobowych, skutkujący naruszeniem praw lub wolności osób fizycznych; wobec czego nie wystąpiła

[6] Umowa nr 14447 z dnia 11.01.2022 r.

konieczność zgłoszenia tego faktu organowi nadzorczemu.
(dowód: akta kontroli str. 145, 241-243, 272-274, 349-365, 575-577)

2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Podstawa prawna	**§ 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.*

Ustalenia kontroli

W myśl § 20 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Audyt wewnętrzny stanowi istotne źródło informacji dla kierownictwa Jednostki o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.

Kontrolującym przedstawiono następujące dowody potwierdzające wykonywanie audytów:

- *Sprawozdanie (preaudyt wewnętrzny) ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych*, datowane na dzień 6 kwietnia 2021 r.
- *Sprawozdanie (audyt wewnętrzny) ze sprawdzenia bezpieczeństwa informacji i zgodności przetwarzania danych osobowych przepisami o ochronie danych osobowych*, datowane na dzień 20 stycznia 2022 r.

W wyniku przeglądu powyższej dokumentacji stwierdzono, że:

- w 2021 roku obok analizy zagadnień dotyczących zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (wskazanych w tytule dokumentu) dokonano także sprawdzenia obowiązującej w Jednostce dokumentacji pod kątem jej aktualności i zgodności między innymi z zapisami rozporządzenia KRI. Audyt wewnętrzny przeprowadzony w Urzędzie w tym okresie nie obejmował jednakże pełnego zakresu zagadnień związanych z bezpieczeństwem informacji,
- w 2022 roku *sprawdzeniu podlegał system zarzadzania bezpieczeństwem informacji i danych osobowych w celu ustalenia aktualnego stanu bezpieczeństwa przetwarzania informacji i danych osobowych oraz bezpieczeństwa fizycznego*. Audyt wewnętrzny przeprowadzony w 2022 r. spełniał wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.

W roku 2019 i 2020, zgodnie z wyjaśnieniami Wójta Gminy Rąbino z dnia 21 lutego 2022r. w Jednostce nie przeprowadzono audytu wewnętrznego z zakresu bezpieczeństwa informacji. Nieprzeprowadzanie kompleksowego audytu wewnętrznego w zakresie bezpieczeństwa informacji lub przeprowadzanie go w niepełnym zakresie może wpływać na oceną skuteczności przyjętych w jednostce rozwiązań, w zakresie bezpieczeństwa informacji; audyt wewnętrzny stanowi bowiem istotne źródło informacji dla kierownictwa jednostki o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Rąbino w latach 2019-2020 nie realizowano (a w 2021 r. nie w pełni zrealizowano) dyspozycji, o której mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 57, 146-164)

Stwierdzone nieprawidłowości w obszarze Nr 2: **1.** Nieprzeglądanie obowiązującej w Urzędzie do 13 października 2021 r. dokumentacji dotyczącej bezpieczeństwa informacji, do czego zobowiązuje § 20 ust. 1 i 2 rozporządzenia KRI; co skutkowało brakiem wszystkich elementów wymaganych przepisami przywołanego wyżej rozporządzenia. **2.** Nieprzeprowadzanie cyklicznie szkoleń obejmujących zakresem zagadnień wskazanych w § 20 ust. 2 pkt 6 rozporządzenia KRI. **3.** W umowie XXX, regulującej kwestię serwisu oprogramowania programu wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej brak zapisów określających maksymalny czas skutecznej naprawy oprogramowania, czym nie wypełniono dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI. **4.** Nieprzeprowadzenie w latach 2019, 2020 audytów wewnętrznych z zakresu bezpieczeństwa informacji, do czego zobowiązuje § 20 ust. 2 pkt 14 rozporządzenia KRI.	
Ocena obszaru kontroli nr 2	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 1/2022
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	Istotną kwestią z punktu widzenia bezpieczeństwa informacji jest ciągłe podnoszenie świadomości pracowników dotyczące istnienia potencjalnych zagrożeń oraz wiedza w jaki sposób unikać, zminimalizować ale także postępować w przypadku materializacji ryzyk związanych z naruszeniem bezpieczeństwa informacji a w szczególności naruszenia ochrony danych osobowych; dlatego też szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji winny mieć charakter cykliczny. Nieprawidłowości polegające na nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji mogą wpłynąć negatywnie na prawidłową oceną skuteczności przyjętych w jednostce rozwiązań w zakresie bezpieczeństwa informacji. Brak zapisów w umowach serwisowych określających maksymalny czas skutecznej naprawy oprogramowania wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej potencjalnie zagraża ciągłości działania Urzędu.
Zalecenia	• w umowie regulującej kwestie serwisu oprogramowania programu wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej wprowadzić zapisy określające maksymalny czas skutecznej naprawy oprogramowania, zgodnie z dyspozycją § 20 ust. 2 pkt 10 rozporządzenia KRI, • przeprowadzać corocznie audyty wewnętrzne z zakresu bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, • przeprowadzać cyklicznie szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji obejmujące wszystkie zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.
Pouczenie	– od wystąpienia pokontrolnego nie przysługują środki odwoławcze; – o podjętych działaniach, mających na celu wyeliminowanie

	stwierdzonych nieprawidłowości, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie 14 dni od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	Wz. Wojewody Zachodniopomorskiego Tomasz Wójcik I Wicewojewoda Zachodniopomorski