WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 3 sierpnia 2023 r.

Znak: K-2.431.1.20.2023.7.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 Krzęcin ul. Tylna 7, 73-231 Krzęcin.
Osoba pełniąca funkcję Wójta Gminy Krzęcin w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Bogdan Wojciech Brzustowicz
Okres objęty kontrolą	od dnia 1 stycznia 2020 r. do dnia 28 kwietnia 2023 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego*, Pani Iwona Olesińska – starszy inspektor wojewódzki.
Nr upoważnienia	Nr 27/23 z dnia 19 kwietnia 2023 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	24-28 kwietnia 2023 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoby udzielające wyjaśnień w trakcie kontroli	Pan Ryszard Przywarty- Sekretarz Gminy Pan Dominik Szymczykowski- Informatyk urzędu

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.

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[3]:** *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 ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Krzęcin wykorzystywano jeden system centralny (aplikacja Źródło) oraz system informatyczny XXX wspomagający obsługę spraw obywatelskich w zakresie ewidencji mieszkańców oraz rejestru zamieszkania cudzoziemców (XXX). System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej Urzędu Gminy Krzęcin został zaprezentowany w czasie kontroli, spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami zarówno Urzędu, jak i innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. System centralny (aplikacja Źródło), dostępny przez stronę WWW podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu Gminy oraz zabezpieczeń związanych z dostępem do systemu. (dowód: akta kontroli str. 30-31, 40)	
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 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*

[3] 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".

	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 System informatyczny wykorzystywany do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy Krzęcin wymieniał dane w formacie .xml. Tym samym spełniony został warunek określony w § 18 ust. 1 rozporządzenia KRI o udostępnianiu zasobów informacyjnych w co najmniej w jednym z formatów wymienionych w załączniku nr 2 do rozporządzenia. Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych Jednostki odbywa się w formacie Unicode UTF-8. (dowód: akta kontroli str. 31)	
Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1: - nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.	
Ocena obszaru kontroli	**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 są rejestry publiczne w postaci teleinformatycznej określone zostały w § 20 ust. 1 rozporządzenia KRI. Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.

W Urzędzie Gminy Krzęcin, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

1. *Zarządzenie wewnętrzne Nr 88/2011 Wójta Gminy Krzęcin z dnia 18 marca 2011r. w sprawie ustalenia Procedury zapewnienia bezpieczeństwa danych i systemów informatycznych w Urzędzie Gminy Krzęcin,*

2. *Zarządzenie wewnętrzne Nr 88a/2012 Wójta Gminy Krzęcin z dnia 15 października 2012r. zmieniające zarządzenie w sprawie ustalenia Procedury zapewnienia bezpieczeństwa danych i systemów informatycznych w Urzędzie Gminy Krzęcin,*

3. *Zarządzenie Nr 28/2018 Wójta Gminy Krzęcin z dnia 4 czerwca 2018r. w sprawie wprowadzenia zmian w Zarządzeniu Nr 88/2011 Wójta Gminy Krzęcin z dnia 18 marca 2011r. w sprawie ustalenia Procedury zapewnienia bezpieczeństwa danych i systemów informatycznych w Urzędzie Gminy Krzęcin,*

4. *Zarządzenie Nr 30/2020 Wójta Gminy Krzęcin z dnia 26 maja 2020r. w sprawie wprowadzenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń w budynkach Urzędu Gminy Krzęcin,*

5. *Zarządzenie wewnętrzne Nr 3/2023 Wójta Gminy Krzęcin z dnia 8 lutego 2023r. w sprawie wprowadzenia rejestru czynności przetwarzania danych osobowych,*

6. *Zarządzenie wewnętrzne Nr 17/2020 Wójta Gminy Krzęcin z dnia 2 listopada 2020r. w sprawie wprowadzenia Regulaminu pracy zdalnej dla pracowników Urzędu Gminy Krzęcin*.

W wyniku analizy aktualnie obowiązującej dokumentacji związanej z bezpieczeństwem informacji stwierdzono następujące nieprawidłowości:

- w *Polityce ochrony danych osobowych w Urzędzie Gminy Krzęcin*, stanowiącej załącznik do *Zarządzenia Nr 28/2018 Wójta Gminy Krzęcin z dnia 4 czerwca 2018r. w sprawie wprowadzenia zmian w Zarządzeniu Nr 88/2011 Wójta Gminy Krzęcin z dnia 18 marca 2011 r.:*
  - *1)* wdrożone w Jednostce regulacje nie obejmują wszystkich informacji jakie są przetwarzane w Urzędzie, a odnoszą się głównie do danych osobowych w odniesieniu do 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)[4];
  - *2)* poza określeniem odpowiedzialności za wdrożenie, nadzór i monitorowanie przestrzegania Polityki oraz regulacji zawartych w załączniku nr 7 do Polityki - *Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji* nie przypisano zadań i obowiązków, a zarazem nie wskazano osób odpowiedzialnych za realizację poszczególnych zadań i działań – używany w Polityce zwrot „*urząd”* (np.: urząd zapewnia, urząd przeprowadza, urząd wdraża, urząd dokonuje przeglądu)

[4] dalej rozporządzenie RODO

nie precyzuje osób odpowiedzialnych za realizację zadań.

- w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Krzęcin,* stanowiącej załącznik nr 3 do *Zarządzenia wewnętrznego Nr 88a/2012 Wójta Gminy Krzęcin z dnia 15 października 2012r. zmieniającego zarządzenie w sprawie ustalenia Procedury zapewnienia bezpieczeństwa danych i systemów informatycznych w Urzędzie Gminy Krzęcin :*

1) załączniki do których odwołano się w Instrukcji nie występują w przywołanej w treści tej Instrukcji postaci np.: w rozdziale II Instrukcji: *Procedury nadawania, modyfikowania oraz anulowania uprawnień do przetwarzania danych w zbiorach materialnych i informatycznych, w* punkcie 2 widnieje zapis, że *zapoznanie się z (...) informacjami pracownik potwierdza (...) na oświadczeniu, którego wzór stanowi Załącznik nr 3 do Polityki bezpieczeństwa*. W obowiązującej Polityce bezpieczeństwa załącznik nr 3 jest dokumentem: *Wzór ewidencji umów powierzenia przetwarzania danych osobowych.* W tym samym rozdziale, *w* punkcie 19 odwołano się do *Rejestru*[5]*, którego wzór stanowi Załącznik nr 4 do Polityki bezpieczeństwa,* natomiast załącznik nr 4 do Polityki bezpieczeństwa to *Wzór wniosku o wpis aktualizacyjny do RCPD;*

2) od 25 maja 2018 r., w związku z wejściem w życie przepisów rozporządzenia RODO instytucja ABI[6] została zastąpiona przez inspektora ochrony danych (IOD). W obowiązującej w Urzędzie Instrukcji wielokrotnie pojawia się pojęcie ABI, któremu przypisano zadania i obowiązki. I tak ABI występuje w treści Instrukcji w: rozdziale II pkt 14, rozdziale III pkt 11., rozdziale IV pkt 6, rozdziale VI pkt A.1, rozdziale VII pkt 3, rozdziale VIII pkt 4.1, rozdziale IX pkt 1.2. Ponadto w załączniku nr 3 do Instrukcji określono *Zakres odpowiedzialności ABI w Urzędzie Gminy Krzęcin;*

3) w Instrukcji występują następujące zapisy:

- rozdział II pkt 4 *Administrator Systemu Informatycznego Urzędu nadaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego wniosku o nadanie uprawnień dostępu do systemu informatycznego* ***Urzędu Gminy Bierzwnik*** *(...),*
- rozdział VII pkt 1 *Osobą odpowiedzialną za wykonywanie przeglądów sprzętu i konserwację systemów w* ***Urzędzie gminy Bierzwnik*** *jest Administrator Systemu,*
- rozdział II pkt 14 *Odebranie lub modyfikacja uprawnień pracownikowi wykonywane jest przez Administratora Systemu na ustny lub mailowy wniosek ABI lub bezpośredniego przełożonego danego pracownika z podaniem tego faktu ABI w celu odnotowania tego faktu w Rejestrze Osób Upoważnionych do przetwarzania danych osobowych w* ***Urzędzie Gminy Bierzwnik*** *(...).*

Zapisy powyższego dokumentu powinny zostać poddane analizie i winny być wprowadzone stosowne zmiany.

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 nie była poddana przeglądowi i weryfikacji pod kątem jej aktualizacji, na co wskazują zapisy szczególnie w Instrukcji - dotyczące zadań ABI oraz niezgodności w treści przywoływanych w tym dokumencie załączników. Ponadto obowiązująca dokumentacja, nie zawiera wszystkich elementów, które decydują o skuteczności i poprawności zarządzania bezpieczeństwem informacji.
Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Krzęcin nie wdrożono kompleksowego systemu zarządzania bezpieczeństwem informacji zapewniającego, w sposób

[5] Rejestr Osób Upoważnionych do przetwarzania danych osobowych.
[6] ABI- Administrator Bezpieczeństwa Informacji.

wyczerpujący poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność działań.

(dowód: akta kontroli str. 70-165, 281-289)

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

W Jednostce zostały opracowane oraz zatwierdzone regulacje wewnętrzne opisujące sposób zarządzania ryzykiem w bezpieczeństwie informacji, w postaci procedury *Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Gminy Krzęcin*.

Kontrolującym przedstawiono następujące dokumenty potwierdzające przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, dotyczące okresu objętego kontrolą:

- *Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Gminy Krzęcin, listopad 2022*;
- Kwestionariusz zarządzania ryzykiem, Data sporządzenia 25.02.2020 r.
- Kwestionariusz zarządzania ryzykiem. Data sporządzenia 25.02.2021 r.

Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarzadzania bezpieczeństwem informacji, pozwalającym na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk. 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. Stwierdzono, że powyżej przywołana analiza ryzyka przeprowadzona została w niepełnym zakresie, tj. analiza nie odnosiła się do wszystkich aktywów Jednostki a dotyczyła głównie zagadnień ochrony danych osobowych. Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Krzęcin nie zrealizowano w pełni dyspozycji, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI.

(dowód: akta kontroli str. 173-191)

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 m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.

Inwentaryzacja zasobów informatycznych w Urzędzie jest realizowana w wersji elektronicznej przy wykorzystaniu oprogramowania XXX. Kontrolującym przedstawiono raporty zawierające informacje dotyczące sprzętu i oprogramowania wobec powyższego stwierdzono, że w Jednostce jest prowadzona inwentaryzacja, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str. 232-235, 273)

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 odbierania uprawnień do pracy w systemie informatycznym uregulowano w załączniku nr 7 do *Polityki ochrony danych osobowych w Urzędzie Gminy Krzęcin - Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji* oraz w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Krzęcin.*

Zgodnie z regulacjami zawartymi w wyżej opisanym załączniku do Polityki uprawnienia w zakresie dostępu do systemu informatycznego nadaje Administrator Systemów Informatycznych, na podstawie pisemnego wniosku osób upoważnionych (bezpośredniego przełożonego pracownika, a w przypadku osoby zatrudnionej na samodzielnym stanowisku na wniosek tej osoby) po akceptacji Administratora Danych Osobowych. Natomiast w obowiązującej Instrukcji zarządzania systemami informatycznymi proces nadawania uprawnień uregulowano w rozdziale II *Procedury nadawania, modyfikacji oraz anulowania uprawnień do przetwarzania danych w zbiorach materialnych i informatycznych*, w pkt 14, w następujący sposób: *Odebranie lub modyfikacja uprawnień pracownikowi wykonywane jest przez Administratora Systemu na ustny lub mailowy wniosek ABI lub bezpośredniego przełożonego danego pracownika z podaniem tego faktu ABI w celu odnotowania tego faktu w Rejestrze Osób Upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Bierzwnik, będącego załącznikiem Nr 4 do Polityki bezpieczeństwa*. Należy zauważyć, że istnieje sprzeczność pomiędzy zapisami regulującymi sprawy nadawania i odbierania uprawnień w systemach informatycznych zawartymi w Polityce i Instrukcji a ponadto załącznik nr 4 do obowiązującej w Jednostce Polityki to dokument *Wzór wniosku o wpis aktualizacyjny do RCPD* a nie jak wskazano w Instrukcji *Rejestrze Osób Upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Bierzwnik.*

Kontrolującym przedstawiono:

- *Wnioski o nadanie/rozszerzenie/cofnięcie upoważnienia do przetwarzania danych osobowych;*
- *Wnioski o nadanie/rozszerzenie/cofnięcie uprawnienia w systemie informatycznym;*
- *Upoważnienia do przetwarzania danych osobowych* wystawione pracownikom Jednostki. Upoważnienia określają jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres ich ważności;
- *Ewidencję osób upoważnionych do przetwarzania danych osobowych Urzędzie Gminy Krzęcin;*
- *Klauzule informacyjne dla pracowników;*
- *Klauzule poufności- oświadczenia* w których zawarto między innymi oświadczenia pracowników o zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania również na okres po ustaniu stosunku pracy;
- *Potwierdzenia zapoznania* (pracowników Urzędu*) z treścią Zarządzenia nr 28/2018 Wójta Gminy Krzęcin z dnia 4 czerwca 2018 rok*;
- *Oświadczenia o znajomości i przestrzeganiu przepisów instrukcji dotyczącej zasad postepowania z kluczami oraz zabezpieczenia pomieszczeń w budynkach Urzędu Gminy w Krzęcinie.*

Z uwagi na fakt, że w okresie podlegającym badaniu, nie wystąpiły przypadki cofania uprawnień nadanych pracownikom realizującym zadania zlecone z zakresu administracji rządowej, nie dokonano sprawdzenia blokowania dostępu do systemów informatycznych.

(dowód: akta kontroli str. 125-129, 145, 166-172, 275, 277-280)

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 Gminy Krzęcin przeprowadzono następujące szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych:

- *Ochrona danych osobowych dla osób przetwarzających dane osobowe w Urzędzie Gminy w Krzęcinie* (22 maja 2020 r.);
- *Szkolenie z zasad ochrony danych (z uwzględnieniem działalności Urzędu w czasie pandemii covid-19)* (1 marca 2021 r.);
- *Szkolenie pracownicze z przestrzegania bezpieczeństwa danych. Zasady cyberbezpieczeństwa w pracy urzędu* (25 lutego 2022 r.);
- *Ochrona danych osobowych w jednostkach samorządu terytorialnego* (21 marca 2023 r.).

Udział w szkoleniach dokumentowała lista obecności zawierająca imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w szkoleniach przeprowadzonych w dniach 22 maja 2020 r. oraz 1 marca 2021 r. nie wziął udziału jeden z dwóch pracowników wskazanych jako osoby realizujące zadania zlecone z zakresu administracji rządowej.

Z przedstawionej dokumentacji oraz złożonych wyjaśnień wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6

rozporządzenia KRI.
Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Udział pracowników w tego typu szkoleniach jest istotny, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych.

(dowód: akta kontroli str. 259-268)

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

Kwestie trybu pracy przy przetwarzaniu mobilnym i pracy na odległość zostały uregulowane w *Regulaminie pracy zdalnej dla pracowników Urzędu Gminy Krzęcin*, wprowadzonym Zarządzeniem wewnętrznym Nr 17/2020 Wójta Gminy Krzęcin z dnia 2 listopada 2020 r.
Zgodnie z wyjaśnieniami Sekretarz Gminy z dnia 25 kwietnia 2023 r. do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie nie wykorzystywano urządzeń mobilnych i nie realizowano pracy na odległość.

(dowód: akta kontroli str. 70-78, 274)

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 Krzęcin na stanowisku Informatyka. W zakresie obowiązków pracownika znajduje się m.in.: administrowanie siecią informatyczną; nadzór nad rozwojem i eksploatacją oprogramowania; instalacja i aktualizacja oprogramowania; wykonywanie kopii zapasowych i ich przechowywanie; nadzór nad bezpieczeństwem i ochroną danych w systemach informatycznych.
W celu realizacji zadań z zakresu administracji rządowej XXX, zawarto umowę serwisową XXX obejmującą swym zakresem między innymi: udostępnianie aktualizacji, naprawę niesprawności systemu oraz wsparcie użytkownika[7]. W umowie wprowadzono zapisy dotyczące poziomu dostępności oferowanych usług oraz sposobu dostarczania ich na zadeklarowanym poziomie, określono maksymalny czas skutecznej naprawy oprogramowania, zdefiniowano grupy błędów i maksymalny czas ich usunięcia. Z firmą zawarto również *Umowę powierzenia przetwarzania danych osobowych*[8], co przekłada się na realizację dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI w zakresie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(dowód: akta kontroli str. 218-231)

[7] Umowa Serwisowa nr 199/2023 z dnia 30 grudnia 2022 r.

[8] Umowa powierzenia przetwarzania danych osobowych z dnia 2 stycznia 2023 r.

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

Procedura postępowania z incydentami, zawarta w *Instrukcji zarządzania systemami informatycznymi w Urzędzie Gminy Krzęcin* w rozdziale IX *Postępowanie w przypadku incydentu związanego z naruszeniem zasad bezpieczeństwa danych osobowych* sprowadza się jedynie do nałożenia obowiązku na pracowników poinformowania o fakcie naruszenia lub próbach naruszenia zabezpieczeń systemu informatycznego, który może skutkować naruszeniem danych osobowych. Powyższy dokument zawęża katalog zdarzeń do naruszenia zabezpieczeń systemu informatycznego, a ponadto (co wynika z samej nazwy procedury) odwołuje się do naruszeń danych osobowych. Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (...),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo informacji w całej organizacji i nie ograniczać się do ochrony danych osobowych. Równie istotny jest brak aktualizacji powyższego dokumentu, szczególnie w świetle obowiązywania rozporządzenia RODO, na mocy którego instytucja ABI została zastąpiona przez inspektora ochrony danych, o czym była mowa w punkcie 2.1 projektu wystąpienia pokontrolnego (w Instrukcji wskazano ABI jako jedną z osób, które należy poinformować o zdarzeniu w przypadku *gdy zagrożenie w ocenie zgłaszającego jest poważne).*

Kwestie postępowania z incydentami w aspekcie wymogu zgłoszenia w okresie 72 godzin do Urzędu Ochrony Danych Osobowych naruszeń ochrony danych osobowych uregulowano w *Polityce ochrony danych osobowych w Urzędzie Gminy Krzęcin*, stanowiącej załącznik do *Zarządzenia Nr 28/2018 Wójta Gminy Krzęcin z dnia 4 czerwca 2018 r. w sprawie wprowadzenia zmian w Zarządzeniu Nr 88/2011 Wójta Gminy Krzęcin z dnia 18 marca 2011 r.*

Kontrolującym przedstawiono *Wewnętrzny rejestr naruszeń ochrony danych osobowych*, w którym odnotowano 5 zdarzeń. W przypadku jednego wpisu, zaewidencjonowanego w rejestrze jako *wysłanie emaila do niewłaściwego adresata* (poz. 3) kontrolujący przyjęli wyjaśnienia, że we wskazanej sytuacji nie nastąpiło naruszenie ochrony danych osobowych. Ponadto z informacji uzyskanych od Informatyka w dniu 25 kwietnia 2023 r. oraz analizy wpisów w przedstawionym rejestrze wynika, że w kontrolowanym okresie, w Jednostce nie stwierdzono przypadków naruszenia ochrony danych osobowych, skutkujących naruszeniem praw lub wolności osób fizycznych; wobec czego nie wystąpiła konieczność zgłoszenia tego faktu organowi nadzorczemu.

Nieaktualna, niekompletna i zawężona jedynie do incydentów naruszeń danych osobowych instrukcja postępowania z incydentami, nie wypełnia dyspozycji § 20 ust. 2 pkt 13 rozporządzenia KRI.

(dowód: akta kontroli str. 111, 152, 272)

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 dokumenty dotyczące okresu objętego weryfikacją:

- Raport z audytu bezpieczeństwa teleinformatycznego, Urząd Gminy Krzęcin, 14.12.2020 r.
- Raport z Audytu Bezpieczeństwa Informacji, Urząd Gminy Krzęcin, 14.12.2020 r.
- Raport z audytu bezpieczeństwa teleinformatycznego, Urząd Gminy Krzęcin, 29.12.2021 r.
- Raport Audyt Bezpieczeństwa, Urząd Gminy Krzęcin, 29.12.2021r.
- Ocena zgodności z KRI/UoKSC, data dokumentu czerwiec 2022 r.
- Raport z audytu Bezpieczeństwa Informacji 2023 r.

Audyty wewnętrzne realizowane corocznie w Jednostce obejmowały swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego w okresie objętym kontrolą spełniono wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 193-217)

2.10 Kopie zapasowe

Podstawa prawna	**§ 20 ust. 2 pkt 12 lit. b, e rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych.*

Ustalenia kontroli

Zgodnie z wymogami określonymi w § 20 ust. 2 pkt 12 lit. b) i e) rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.

Zasady tworzenia kopii zapasowych zbiorów danych oraz programów uregulowane zostały w:

- *Procedurze bezpieczeństwa fizycznego i bezpieczeństwa informacji* oraz w *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Krzęcin,* stanowiącej załącznik nr 7 do *Polityki ochrony danych osobowych w Urzędzie Gminy Krzęcin* (w rozdział VI i VII);
- *Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Krzęcin* - rozdział V *Procedury tworzenia kopii zapasowych zbiorów danych i aplikacji służących przetwarzaniu danych osobowych.* Powyższy dokument nie został zaktualizowany i w jego treści istnieje zapis regulujący udział ABI w procesie tworzenia kopii zapasowych (pkt 2 procedury).

Kopie zapasowe baz danych systemów informatycznych, zgodnie z wyjaśnieniami Informatyka wykonywane są codziennie i zapisywane na serwerze, natomiast pełne kopie zapasowe serwera

tworzone są raz w tygodniu. Ponadto raz w tygodniu wykonywana jest replika kopii. Nośniki kopii zapasowych są przechowywane w innej lokalizacji niż miejsce ich wytworzenia, co z uwagi na ryzyko utraty informacji w przypadku zaistnienia sytuacji nadzwyczajnych zapewnia ciągłość działania Jednostki. Z wyjaśnień Informatyka wynika, że minimum raz w miesiącu realizowane jest próbne testowane w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa, przy czym nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów. (dowód: akta kontroli str. 128-129, 148, 271)	
2.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych	
Podstawa prawna	**§ 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.*
Ustalenia kontroli W celu wykonywania zadań z zakresu administracji rządowej XXX, zawarto umowę serwisową XXX, obejmującą swym zakresem między innymi: udostępnianie aktualizacji, naprawę niesprawności systemu oraz wsparcie użytkownika. (dowód: akta kontroli str. 218-223)	
2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji	
Podstawa prawna	**§ 20 ust. 2 rozporządzenia KRI:** *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.*
Ustalenia kontroli W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi nadano identyfikator i hasło wejścia do systemów zainstalowanych na komputerach oraz do programów, z których korzystają. W przypadku systemu „Źródło" dostęp jest możliwy wyłącznie z użyciem karty, na której zapisany jest certyfikat umożliwiający zalogowanie się do centralnego systemu. Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych. W wyniku oględzin przeprowadzonych w toku czynności kontrolnych ustalono, że: - na każdym urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu	

nazwy użytkownika i hasła,
- komputery miały zainstalowane oprogramowanie antywirusowe,
- na wszystkich jednostkach skonfigurowano wygaszacz ekranu,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitora stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej (podlegających kontroli) uniemożliwia odczyt wyświetlanych danych przez osoby postronne,
- pomieszczenie serwerowni wyposażono w klimatyzację, antywłamaniowe drzwi wejściowe, czujnik dymu oraz gaśnicę proszkową.

Zarządzeniem Nr 30/2020 Wójta Gminy Krzęcin z dnia 26 maja 2020 r. w sprawie wprowadzenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń w budynkach Urzędu Gminy Krzęcin uregulowano zasady zabezpieczenia pomieszczeń biurowych w Urzędzie, w tym zasady przebywania osób w miejscach wskazanych jako pomieszczenia strefy bezpieczeństwa. Na szczególne uznanie zasługuje fakt, ze Informatyk poprosił kontrolujących o potwierdzenie faktu przebywania w serwerowni, (w związku z przeprowadzanymi oględzinami) poprzez wpis do prowadzonego przez Niego *Rejestru wejść i wyjść do serwerowni.*

(dowód: akta kontroli str. 269-270, 281-289)

2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych

Podstawa prawna	**§ 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.*

Ustalenia kontroli

Sieci i systemy zabezpieczono przy wykorzystaniu zapory sieciowej – firewall. Na komputerach podlegających badaniu zainstalowano oprogramowanie antywirusowe. W Urzędzie funkcjonuje system monitorowania sieci oraz działań użytkowników.

W procedurach wewnętrznych Jednostki określono zasady naprawy oraz wycofywania elektronicznych nośników informacji zawierających dane osobowe.

(dowód: akta kontroli str. 290)

2.14 Rozliczalność działań w systemach teleinformatycznych.	
Podstawa prawna	**§ 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:** *w zakresie wynikającym z analizy ryzyka 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.*
Ustalenia kontroli Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych). System objęty kontrolą zawiera logi, w których są odnotowanie działania użytkowników zgodnie z § 21 rozporządzenia KRI. Logi, zgodnie z zapisami § 21 ust. 4 rozporządzenia KRI winny być przechowywane przez okres ponad 2 lat. Najstarsze zaprezentowane podczas kontroli logi systemu pochodziły z 6 września 2021 r., wobec czego nie wypełniono dyspozycji § 21 ust. 4 wyżej opisanego rozporządzenia. Zgodnie z wyjaśnieniami Informatyka w Jednostce są prowadzone działania związane z przeglądaniem logów systemu informatycznego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, w celu stwierdzenia i ewentualnej identyfikacji działań niepożądanych. (dowód: akta kontroli str. 236-258, 276)	

Stwierdzone nieprawidłowości w obszarze nr 2: 1. Obowiązująca w Urzędzie dokumentacja regulująca kwestie bezpieczeństwa informacji, nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. 2. Nieprzeglądanie i nieaktualizowanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji, do czego zobowiązują zapisy § 20 ust. 1 i 2 pkt 1 rozporządzenia KRI. 3. Przeprowadzanie analiz ryzyka w niepełnym zakresie (analizy nie odnosiły się do wszystkich aktywów Jednostki a dotyczyły zagadnień ochrony danych osobowych), co nie odpowiadało dyspozycji § 20 ust. 2 pkt 3 rozporządzenia KRI. 4. Sprzeczność pomiędzy zapisami regulującymi kwestie nadawania i odbierania uprawnień w systemach informatycznych zawartymi w obowiązujących w Jednostce procedurach. 5. Nieaktualna, niekompletna i zawężona jedynie do incydentów naruszenia danych osobowych instrukcja postępowania z incydentami dotyczącymi bezpieczeństwa informacji, co nie wypełnia dyspozycji § 20 ust. 2 pkt 13 rozporządzenia KRI. 6. Nieprzechowywanie przez okres 2 lat logów systemu informatycznego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, zgodnie z zapisami § 21 ust. 4 rozporządzenia KRI.	
Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 1/2023
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	W Urzędzie Gminy Krzęcin funkcjonują procedury regulujące kwestie bezpieczeństwa informacji, niemniej jednak wymagają one podjęcia działań korygujących i usprawniających. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. 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. Jednym z elementów zarządzania bezpieczeństwem informacji, znacząco wpływającym na skuteczność tego zarządzania jest okresowo przeprowadzana analiza ryzyka utraty integralności, dostępności lub poufności informacji w celu jego monitorowania i zapobiegania lub minimalizacji jego materializacji. Odpowiednio przygotowany proces szacowania ryzyka winien obejmować wszystkie posiadane i przetwarzane informacje, z uwzględnieniem specyfiki realizowanych przez Jednostkę zadań.
Zalecenia	• Uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji, zgodnie z wymogami rozporządzenia KRI. • Dokonywać przeglądu i aktualizować dokumentację dotyczącą bezpieczeństwa informacji, do czego zobowiązują zapisy § 20 ust. 1 i 2 pkt 1 rozporządzenia KRI

	• Przeprowadzać analizy ryzyka odnoszące się do wszystkich aktywów Jednostki, na co wskazuje dyspozycja § 20 ust. 2 pkt 3 rozporządzenia KRI. • Uzupełnić procedurę postępowania w przypadku naruszenia ochrony danych osobowych o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji, zgodne z dyspozycją § 20 ust. 2 pkt 13 rozporządzenia KRI. • Przechowywać przez okres 2 lat logi systemu informatycznego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, zgodnie z zapisami § 21 ust. 4 rozporządzenia KRI. • Ujednolicić zapisy obowiązujących w Jednostce procedur w zakresie nadawania i odbierania uprawnień do pracy w systemach informatycznych.
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	z upoważnienia Wojewody Zachodniopomorskiego Mateusz Wagemann II Wicewojewoda Zachodniopomorski