WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 19 października 2023 r.

Znak: K-2.431.1.14.2023.6.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 Wierzchowo, ul. Długa 29, 78-530 Wierzchowo
Osoba pełniąca funkcję Wójta Gminy Wierzchowo w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Jan Szewczyk
Okres objęty kontrolą	od dnia 1 stycznia 2020 r. do dnia 14 lipca 2023 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego*, Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 50/23 z dnia 7 lipca 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	10-14 lipca 2023 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Maciej Furykiewicz- Informatyk

[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 Wierzchowo wykorzystywano jeden system centralny (aplikacja Źródło) oraz systemy informatyczne wspomagające obsługę spraw obywatelskich: Rejestr Ewidencji Ludności - XXX oraz Rejestr Wyborców – XXX. Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej Urzędu Gminy Wierzchowo zostały zaprezentowane w czasie kontroli, spełniały 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), podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu Gminy oraz zabezpieczeń związanych z dostępem do systemu. (dowód: akta kontroli str. 30, 39)	
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 rozporządzenia.* **§ 18 ust. 2 rozporządzenia KRI:** *Jeżeli z przepisów szczegółowych*

[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".

	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 Wierzchowo wymieniał dane w formatach określonych 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. 30, 343)	
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 Wierzchowo, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji: • *Zarządzenie Nr 254/2018 Wójta Gminy Wierzchowo z dnia 25 maja 2018 r. w sprawie*	

wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy Wierzchowo (okres funkcjonowania regulacji - od 25 maja 2018 r. do 8 maja 2022 r.),

- *Zarządzenie Nr 155/2020 Wójta Gminy Wierzchowo z dnia 23 października 2020 r. w sprawie wprowadzenia w Urzędzie Gminy Wierzchowo możliwości wykonywania pracy w formie pracy zdalnej,*
- *Zarządzenie Nr 231/2021 Wójta Gminy Wierzchowo z dnia 26 października 2021 r. w sprawie wprowadzenia w Urzędzie Gminy Wierzchowo procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem,*
- *Zarządzenie Nr 284/2022 Wójta Gminy Wierzchowo z dnia 9 maja 2022 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych,*
- *Zarządzenie Nr 379/2023 Wójta Gminy Wierzchowo z dnia 31 maja 2023 r. zmieniające zarządzenie w sprawie wprowadzenia Polityki Ochrony Danych Osobowych.*

W wyniku analizy aktualnej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury zawierają między innymi oświadczenie o intencjach kierownictwa potwierdzające cele i zasady bezpieczeństwa; definicje ogólnych i szczegółowych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji oraz zakres stosowania wprowadzonych regulacji. 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 aktualizowana szczególnie w kontekście uregulowań dotyczących wykonywania obowiązków w formie pracy zdalnej.

Niemniej jednak odwołanie w samej nazwie dokumentów, zarówno w polityce jak i instrukcji do ochrony danych osobowych (*Polityka Ochrony Danych Osobowych w Urzędzie Gminy Wierzchowo, Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych* – występująca jako element wyżej opisanej polityki) sugeruje zawężenie problemu bezpieczeństwa informacji do zagadnień związanych z ochroną danych osobowych, podczas gdy ochronie winny podlegać wszystkie przetwarzane przez Urząd informacje.

(dowód: akta kontroli str. 69-172, 180-227)

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 odnoszące się do *analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii* (art. 36 Polityki ochrony danych osobowych).

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. Urząd Gminy Wierzchowo, marzec 2023,*
- *Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych. Urząd Gminy Wierzchowo, wrzesień 2022.*

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 wyżej przywołane analizy ryzyka przeprowadzone zostały w niepełnym zakresie, tj. analizy nie odnosiły się do wszystkich aktywów Jednostki a dotyczyły zagadnień ochrony danych osobowych. Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Wierzchowo nie zrealizowano w pełni dyspozycji, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI.

(dowód: akta kontroli str. 117, 228-286)

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 do inwentaryzacji XXX. System umożliwia prowadzenie inwentaryzacji generując raporty zawierające informacje dotyczące m. in. sprzętu i oprogramowania oraz rodzaju systemu operacyjnego. W trakcie kontroli okazano stosowną dokumentację, potwierdzającą prowadzenie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str. 344)

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 *Polityce Ochrony Danych Osobowych*, w rozdziale III (art. 20). Zgodnie z procedurami przyjętymi w Jednostce uprawnienia w zakresie dostępu do systemu informatycznego nadaje osoba odpowiedzialna za obsługę informatyczną urzędu, na podstawie pisemnego wniosku osób uprawnionych, po zatwierdzeniu przez administratora danych osobowych.
Kontrolującym przedstawiono:

- *upoważnienia do przetwarzania danych osobowych* wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności. W dokumencie zawarto oświadczenie pracownika o zachowaniu w tajemnicy przetwarzanych danych. Nie wskazano natomiast czasu trwania tego zobowiązania. Kontrolujący sugerują, by w odniesieniu do wyżej wymienionych pracowników zaktualizować powyższy dokument, szczególnie że w załączniku nr 7 do obowiązującej *Polityki Ochrony Danych Osobowych* zawarto odpowiednie zapisy pod kątem wskazania okresu obowiązywania zobowiązania, rozszerzając go na okres po ustaniu stosunku pracy.
- Potwierdzenie zapoznania pracowników Urzędu z treścią *Polityki Ochrony Danych Osobowych* z 2022 roku.

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. 101, 156-157, 327-328, 342-343)

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

- *Ochrona danych osobowych w świetle 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, praktyczne aspekty stosowania RODO* (4 maja 2022r.);
- *Szkolenie z zakresu ochrony danych osobowych* (18 stycznia 2023 r.);
- *Szkolenie urzędników w zakresie cyberbezpieczeństwa* (14 marca 2023 r.).

Udział w szkoleniach dokumentowały listy obecności zawierające imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w szkoleniach przeprowadzonych w Jednostce wzięli udział pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.
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.
Z przedstawionej dokumentacji wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 318-326)

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 unormowane w następujących dokumentach:

- *Zarządzeniu Nr 155/2020 Wójta Gminy Wierzchowo z dnia 23 października 2020 r. w sprawie wprowadzenia w Urzędzie Gminy Wierzchowo możliwości wykonywania pracy w formie pracy zdalnej,*
- *Zarządzeniu Nr 379/2023 Wójta Gminy Wierzchowo z dnia 31 maja 2023 r. zmieniającym zarządzenie w sprawie wprowadzenia w Polityki Ochrony Danych Osobowych,*
- *Polityce Ochrony Danych Osobowych* (art. 30), wprowadzonej *Zarządzeniem Nr 284/2022 Wójta Gminy Wierzchowo z dnia 9 maja 2022 r.*

Zgodnie z wyjaśnieniami Wójta Gminy Wierzchowo z 12 lipca 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. 69-74, 107-108, 166-172, 343)

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 Wierzchowo, na stanowisku Informatyka. W zakresie obowiązków pracownika znajduje się m.in.: nadzór nad przeglądami i konserwacją systemów służących do przetwarzania danych osobowych i sprzętu komputerowego; administrowanie siecią komputerową; prowadzenie ewidencji urządzeń i programów komputerowych; nadzór nad wykonywaniem kopii zapasowych i ich przechowywaniem; pełnienie funkcji Administratora Systemów Informatycznych.

W celu realizacji zadań z zakresu administracji rządowej XXX zawarto umowę, której przedmiotem jest prowadzeniu nadzoru i serwisu oprogramowania użytkowanych systemów XXX[4]. Stwierdzono, że w powyższej umowie wprowadzono zapis określający maksymalny czas skutecznej naprawy oprogramowania, czym wypełniono dyspozycję § 20 ust. 2 pkt 10 rozporządzenia KRI, zawierającą zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. W powyższej umowie uregulowano również kwestie powierzenia przetwarzania danych osobowych.

(dowód: akta kontroli str. 173-179, 329-331)

[4] Umowa nr 14854 z dnia 21.12.2022 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

W *Procedurze zarzadzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem*, stanowiącej załącznik nr 1 do *Zarządzenia Nr 231/2021 Wójta Gminy Wierzchowo z dnia 26 października 2021 r.* określono sposób postępowania w przypadku stwierdzenia zaistnienia incydentu związanego z bezpieczeństwem informacji, wskazując jednocześnie katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia danych. Ponadto procedura postępowania w sytuacji wystąpienia incydentów przypisuje odpowiednie zadania IOD[5], ADO[6] oraz ASI[7] w przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji.

W obowiązującej *Polityce Ochrony Danych Osobowych*, w załączniku nr 12 określono zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych, zgodnie z wymogami rozporządzenia RODO[8].

Kontrolującym przedstawiono *Rejestr naruszeń i incydentów ochrony danych osobowych*, w którym odnotowano jedno zdarzenie, zaklasyfikowane jako naruszenie niskiego stopnia. W przypadku tego wpisu, kontrolujący przyjęli wyjaśnienia, że we wskazanej sytuacji nie nastąpiło naruszenie ochrony danych osobowych, skutkujące koniecznością zgłoszenia tego faktu organowi nadzorczemu.

Kontrolujący wskazują by prowadzony przez Urząd *Rejestr naruszeń i incydentów ochrony danych osobowych* rozszerzyć o inne rodzaje naruszeń bezpieczeństwa informacji i prowadzić w ten sposób jeden rejestr zawierający dane o wszystkich rodzajach naruszeń bezpieczeństwa informacji (nie tylko dotyczących incydentów ochrony danych osobowych).

(dowód: akta kontroli str. 160-164, 335)

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:

- Sprawozdanie z zadania audytowego przeprowadzonego w Urzędzie Gminy Wierzchowo z zakresu bezpieczeństwa informacji, data sporządzenia 15.01.2020 r.;

[5] Inspektor Ochrony Danych
[6] Administrator Danych Osobowych
[7] Administrator Systemów Informatycznych
[8] 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).

- Raport z audytu z zakresu bezpieczeństwa informacji, data sporządzenia 28.04.2022 r.;
- Raport z audytu z zakresu bezpieczeństwa informacji, data sporządzenia 18.04.2023 r.

Zgodnie z wyjaśnieniami Wójta Gminy Wierzchowo z 12 lipca 2023 r. audyt wewnętrzny z zakresu bezpieczeństwa informacji w 2021 roku nie został przeprowadzony. Audyty wewnętrzne realizowane w Jednostce, w latach 2020, 2022-2023 obejmowały swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego w tym okresie spełniono wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 287-317)

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 art. 23 *Polityki Ochrony Danych Osobowych*. Wskazano osobę odpowiedzialną za sporządzanie kopii zapasowych oraz określono częstotliwość ich tworzenia. Ustanowiono zasady testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania.

Kopie programu XXX, zgodnie z wyjaśnieniami Informatyka wykonywane są automatycznie codziennie na lokalnym komputerze, a raz w tygodniu przenoszone na zaszyfrowany nośnik zewnętrzny, przechowywany w zamykanej na klucz metalowej szafie w pomieszczeniu innym, niż miejsce ich wytworzenia. Dodatkowo kopiowane są na serwer XXX. Z wyjaśnień Informatyka wynika również, że realizowane jest próbne testowane w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa.

(dowód: akta kontroli str. 103, 344)

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, której przedmiotem jest prowadzeniu nadzoru i serwisu oprogramowania użytkowanych systemów XXX.

(dowód: akta kontroli str. 173-179)

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 stanowiska komputerowego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że: - na urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła, - komputer miał zainstalowane oprogramowanie antywirusowe oraz 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, - żadnemu z użytkowników nie nadano uprawnień administratora uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń, - pomieszczenie serwerowni wyposażono w klimatyzację, antywłamaniowe drzwi wejściowe. W pomieszczeniu brak czujnika dymu. W *Polityce Ochrony Danych Osobowych* uregulowano zasady serwisu i konserwacji oraz utylizacji sprzętu elektronicznego. (dowód: akta kontroli str. 109-110, 336-341, 345-346)	
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 Sieć i systemy informatyczne Urzędu zabezpieczono przy wykorzystaniu zapory sieciowej. Urządzenia informatyczne Jednostki są podłączone do lokalnych zasilaczy awaryjnych UPS. Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe. (dowód: akta kontroli str. 344-345)	
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). Systemy objęte kontrolą zawierają logi, w których są odnotowanie działania użytkowników zgodnie z zapisami § 21 ust. 2 i 3 rozporządzenia KRI. Logi systemów są przechowywane przez okres ponad 2 lat, wobec czego wypełniono dyspozycję § 21 ust. 4 wyżej opisanego rozporządzenia. Zgodnie z wyjaśnieniami Informatyka w Jednostce prowadzone są 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. 332-334, 344)

Stwierdzone nieprawidłowości w obszarze nr 2:

- 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.
- Nieprzeprowadzenie w 2021 roku audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 rozporządzenia KRI.

Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 3/2023
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	Jednym z elementów systemu zarządzania bezpieczeństwem informacji, znacząco wpływającym na jego skuteczność 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 odnosić się i obejmować wszystkie posiadane i przetwarzane informacje, z uwzględnieniem specyfiki realizowanych przez Jednostkę zadań. Nieprzeprowadzenie audytu wewnętrznego z zakresu bezpieczeństwa informacji może wpłynąć negatywnie na prawidłową ocenę skuteczności przyjętych w Jednostce rozwiązań w zakresie bezpieczeństwa informacji. Audyt wewnętrzny stanowi bowiem istotne źródło wiedzy kierownictwa o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.
Zalecenia	• przeprowadzać analizy ryzyka odnoszące się do wszystkich aktywów Jednostki, zgodnie z dyspozycją § 20 ust. 2 pkt 3 rozporządzenia KRI, • przeprowadzać nie rzadziej niż raz na rok audyt wewnętrzny w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 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	z upoważnienia Wojewody Zachodniopomorskiego Mateusz Wagemann II Wicewojewoda Zachodniopomorski