WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, 23.05.2024 r.

Znak: K-2.431.1.10.2024.6.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	Burmistrz Miasta i Gminy Człopa, ul. Strzelecka 2, 78-630 Człopa.
Osoba pełniąca funkcję kierownika jednostki kontrolowanej w okresie objętym kontrolą	Pan Jerzy Bekker - Burmistrza Miasta i Gminy Człopa
Osoby pełniące funkcję kierownika jednostki kontrolowanej w okresie prowadzenia kontroli	Pan Jerzy Bekker - Burmistrz Miasta i Gminy Człopa do 6 maja 2024 r. Pan Bartosz Nowicki – Burmistrz Miasta i Gminy Człopa od 6 maja 2024 r.
Okres objęty kontrolą	od dnia 1 stycznia 2021 r. do dnia 23 lutego 2024 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 9/24 z dnia 15 lutego 2024 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	19-23 lutego 2024 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pani Joanna Jastrzębowska – zastępca Burmistrza Miasta i Gminy Człopa, Pan Piotr Ciułek – Inspektor do spraw obsługi informatycznej[3].

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.
[3] Zwany dalej Informatykiem.

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 ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Miasta i Gminy Człopa wykorzystywano system centralny XXX oraz system informatyczny wspomagający obsługę spraw obywatelskich w zakresie ewidencji ludności XXX i rejestru wyborców XXX - oprogramowanie firmy XXX, System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej Urzędu Miasta i Gminy Człopa 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 podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu Gminy oraz zabezpieczeń związanych z dostępem do systemu. (dowód: akta kontroli str. 34-35)	
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 albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania*

[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".

	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 Miasta i Gminy Człopa 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. 26, 287, 292)

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 Miasta i Gminy Człopa, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Polityka ochrony danych osobowych*, wprowadzona *Zarządzeniem nr 73/2023 Burmistrza Miasta i Gminy Człopa z dnia 2 października 2023 roku*;
- *Polityka Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Człopie*, wprowadzona *Zarządzeniem nr 80/2018 Burmistrza Miasta i Gminy Człopa z dnia 4.12.2018 roku* (okres funkcjonowania regulacji - od 4 grudnia 2018 r. do 2 października 2023 r.);
- *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Człopie*, wprowadzona *Zarządzeniem nr 80/2018 Burmistrza Miasta i Gminy Człopa z dnia 4.12.2018 roku* (okres funkcjonowania regulacji - od 4 grudnia 2018 r. do 2 października 2023 r.).

Odwołanie w samej nazwie dokumentów (dotyczących zarządzania bezpieczeństwem informacji) obowiązujących w Urzędzie do ochrony danych osobowych (*Polityka Ochrony Danych Osobowych, Procedury zarzadzania systemami informatycznymi służącymi do przetwarzania danych osobowych* - rozdział III *Polityki Ochrony Danych Osobowych*) sugeruje zawężenie problemu bezpieczeństwa informacji do zagadnień związanych z ochroną danych osobowych, podczas gdy ochronie winny podlegać wszystkie przetwarzane przez Urząd informacje.
W wyniku analizy aktualnie obowiązującej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury wymagają uzupełnienia o elementy związane z bezpieczeństwem wszystkich informacji przetwarzanych w Urzędzie (np. w zakresie zgłaszania incydentów innych niż związanych z naruszeniem danych osobowych). Należy jednak stwierdzić, że obowiązujące w Urzędzie regulacje w większości wypełniały wymogi dyspozycji w § 20 ust. 1 rozporządzenia KRI.
Dyrektywa § 20 ust. 1 rozporządzenia KRI wskazuje na konieczność monitorowania i przeglądu systemu zarządzania bezpieczeństwem informacji. Kontrolującym nie przedstawiono dokumentacji potwierdzającej realizację dyspozycji w tym zakresie.

(dowód: akta kontroli str. 66, 70-211)

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

Kontrolującym przedstawiono *Analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych.*
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 przywołana analiza ryzyka przeprowadzona została w niepełnym zakresie, tj. analiza nie odnosiła się do wszystkich aktywów Jednostki a dotyczyła (na co wskazuje już sam tytuł dokumentu) zagadnień związanych z przetwarzaniem danych osobowych.
Mając na względzie powyższe, należy stwierdzić, że w Urzędzie nie zrealizowano w pełni dyspozycji, o której mowa w§ 20 ust. 2 pkt 3 rozporządzenia KRI.

(dowód: akta kontroli str. 67, 244-271)

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.

Kontrolującym przedstawiono karty raportów inwentaryzacji dla sprzętu komputerowego użytkowanego w Urzędzie. Dokumenty zawierały informacje między innymi o rodzaju użytkowanego w Jednostce sprzętu (nazwie i jego charakterystyce), nazwie oraz wersji systemu operacyjnego, nazwie procesora, zainstalowanego oprogramowania, pojemności pamięci oraz współpracujących urządzeń peryferyjnych. Okazane formularze potwierdzają, prowadzenie w Urzędzie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str. 276-279)

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. 19). Zgodnie z zapisami procedury uprawnienia do pracy w systemach informatycznych nadawane (modyfikowane oraz zmieniane) są przez informatyka na podstawie ustnej dyspozycji Administratora Danych Osobowych. Informatyk odnotowuje fakt nadania uprawnień w *Ewidencji osób upoważnionych do przetwarzania danych osobowych.* Kontrolujący wskazują by wewnętrzne procedury uzupełnić o pisemny wniosek, który poświadczać będzie realizowanie wymogu dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych. Przedmiotowy

dokument podpisany przez upoważnione osoby spowoduje, że proces nadawania i odbierania uprawnień będzie w pełni potwierdzony.

Kontrolującym przedstawiono:

- *upoważnienie do przetwarzania danych osobowych w systemie informatycznym lub zbiorze w wersji papierowej* wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności;
- oświadczenie o zapoznaniu z obowiązującymi przepisami dotyczącymi ochrony danych osobowych, w którym zawarto między innymi oświadczenie pracownika o zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania w trakcie zatrudnienia, jak również po ustaniu stosunku pracy;
- dokument - *Wykaz osób zapoznanych z Polityką ochrony danych osobowych.*

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. 131-132, 295-304)

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 pracownicy Jednostki uczestniczyli w szkoleniu[5], w trakcie którego poruszane były zagadnienia związane z cyberbezpieczeństwem, szyfrowaniem dokumentów, bezpiecznym użytkowaniem poczty elektronicznej i sieci internet. Ponadto szkolonym przedstawiono zapisy obowiązującej w Urzędzie polityki bezpieczeństwa. Kontrolującym okazano listę obecności dokumentującą udział pracowników w wyżej opisanym szkoleniu. Z wyjaśnień Informatyka oraz przedstawionej dokumentacji wynika, że zakres tematyczny szkolenia obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

Ponadto wyznaczeni pracownicy Urzędu 4 października 2023 r. wzięli udział w szkoleniu[6] z zakresu podstawowych zasad cyberbezpieczeństwa oraz zasad bezpieczeństwa stacji roboczych SRP[7].

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji. Kontrolujący sugerują, aby szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji miały charakter cykliczny, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych.

(dowód: akta kontroli str. 284-286)

[5] Szkolenie odbyło się 24 listopada 2023 r.

[6] Szkolenie przeprowadzone przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji oraz Pion Usług Cyfrowych Centralnego Ośrodka Informatyki (COI).

[7] System Rejestrów Państwowych.

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:

- *Polityce Ochrony Danych Osobowych* (w rozdziale III art. 29 *Zasady pracy z urządzeniami mobilnymi*),
- *Procedurze ochrony danych osobowych przy pracy zdalnej,* stanowiącej załącznik nr 17 do *Polityki Ochrony Danych Osobowych.*

W wyżej wymienionych dokumentach uregulowano między innymi kwestie wynoszenia poza obszar organizacji nośników z danymi osobowymi (w tym dokumentów wytworzonych w formie papierowej), wprowadzając wymóg uzyskania zgody Administratora Danych Osobowych. Wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych, a także wymóg zabezpieczenia hasłem użytkowanych laptopów.

Zgodnie z wyjaśnieniami Burmistrza z 19 lutego 2024 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. 66, 137-138, 206-210)

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 Urzędu realizowana jest przez pracownika zatrudnionego w Urzędzie Miasta i Gminy Człopa, na stanowisku Inspektora do spraw obsługi informatycznej. W zakresie obowiązków pracownika znajduje się m.in.: administrowanie siecią komputerową; instalacja oprogramowania; prowadzenie ewidencji urządzeń i programów komputerowych; zarządzanie bezpieczeństwem danych i systemów; nadzór nad aktualizacją zabezpieczeń informatycznych; archiwizacja danych.

W celu realizacji zadań z zakresu administracji rządowej z firmą XXX zawarto umowę, której przedmiotem jest sprawowanie opieki autorskiej nad systemami XXX, obejmującą m. in. informowanie i udostępnianie do pobrania nowych wersji oprogramowania, nieodpłatne usuwanie wad w działaniu oprogramowania oraz udzielanie wsparcia w zakresie jego eksploatacji.

Stwierdzono, że w powyższej umowie nie został określony maksymalny czas skutecznej naprawy oprogramowania, powyższym nie wypełniono dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI, zawierającego zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Z firmą XXX. zawarto umowę powierzenia przetwarzania danych osobowych.[8]

(dowód: akta kontroli str. 272-275, 280-283)

[8] Umowa powierzenia przetwarzania danych osobowych z dnia 19.12.2018 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 obowiązującej w Urzędzie *Procedurze zarządzania naruszeniami ochrony danych osobowych*, stanowiącej załącznik nr 13 do *Polityki Ochrony Danych Osobowych*, określono zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych, w oparciu o wymogi rozporządzenia RODO[9]. Natomiast § 20 ust. 2 pkt 13 rozporządzenia KRI wskazuje, że *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (…),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo wszystkich informacji przetwarzanych w Jednostce i nie ograniczać się wyłącznie do ochrony danych osobowych.

Kontrolującym przedstawiono *Rejestr naruszeń ochrony danych osobowych*, który nie zawierał wpisów. Zgodnie z oświadczeniem Burmistrza z 19 lutego 2024 r. w okresie objętym kontrolą nie wystąpiły incydenty naruszenia danych osobowych.

(dowód: akta kontroli str. 66, 69, 180-189)

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. Kontrolującym przedstawiono dokument: *Urząd Miasta i Gminy Człopa. Raport z audytu*. Data przeprowadzenia 02.10.2023 r. Audyt wewnętrzny zrealizowany w Jednostce w 2023 roku obejmował swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego w odniesieniu do tego okresu spełniono wymóg *zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji*.

W 2021 i 2022 roku audyty wewnętrzne, zgodnie z wyjaśnieniami Burmistrza z 19 lutego 2024 r. nie zostały przeprowadzone. Nieprzeprowadzanie audytu wewnętrznego może wpływać na ocenę 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 Miasta i Gminy Człopa w latach 2021- 2022 nie zrealizowano dyspozycji, o której mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 67, 212-243)

[9] 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).

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 wykonywania kopii bezpieczeństwa oraz kwestie ich testowania uregulowano w art. 22, w rozdziale III *Polityki Ochrony Danych Osobowych*. Kopie zapasowe baz danych zgodnie z wyjaśnieniami Informatyka z dnia 20 lutego 2024 r. wykonywane są codziennie, a następnie są kopiowane na dysk sieciowy i replikowane na kolejny zapasowy dysk sieciowy. Ponadto dysk serwera raz w tygodniu kopiowany jest na dysk przenośny, który przechowywany jest poza miejscem wytworzenia kopii. W Urzędzie realizowane jest próbne testowane kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania, przy czym nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów. Kontrolujący wskazują by dokumentować te czynności, tak by realizowane działania były w pełni potwierdzone. (dowód: akta kontroli str. 133, 287)	
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 realizacji zadań z zakresu administracji rządowej z firmą XXX zawarto umowę, której przedmiotem jest sprawowanie opieki autorskiej nad systemami XXX. W procedurach wewnętrznych uregulowano zasady wdrażania nowych wersji użytkowanego oprogramowania, działania związane z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności. (dowód: akta kontroli str.136-137)	
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: - dostęp do systemu operacyjnego na urządzeniu możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła, - komputer miał zainstalowane oprogramowanie antywirusowe oraz skonfigurowany 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 uniemożliwiało odczyt wyświetlanych danych przez osoby postronne, - użytkownikom 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, co wpływa na możliwość utrzymania odpowiedniego poziomu temperatury powietrza; gaśnicę; zamontowano czujkę dymu. XXX. (dowód: akta kontroli str. 287-291, 304-305)	
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 informatyczną Urzędu zabezpieczono przy wykorzystaniu zapory sieciowej firewall,
- Urządzenia informatyczne Jednostki są podłączone do lokalnych zasilaczy awaryjnych UPS,
- Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe,
- W procedurach wewnętrznych Jednostki określono zasady:

- przesyłania danych poza obszar przetwarzania oraz zasady bezpiecznej wymiany informacji;
- poprzez zastosowanie między innymi ochrony kryptograficznej;
- naprawy urządzeń komputerowych;
- niszczenia elektronicznych nośników informacji;
- nadzoru nad kluczami do pomieszczeń Jednostki.

(dowód: akta kontroli str. 66-67, 133-134, 139-140, 142-143, 287, 304)

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 odnotowane działania użytkowników, zgodnie z zapisami § 21 ust. 2 i 3 rozporządzenia KRI. Logi systemu 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, natomiast nie jest sporządzana dokumentacja tego procesu. Kontrolujący wskazują aby dokumentować działania związane z przeglądaniem logów systemowych, tak by realizowane czynności były w pełni potwierdzone. (dowód: akta kontroli str. 287, 293-294)	
Stwierdzone nieprawidłowości w obszarze nr 2: • Dokumentacja regulująca kwestie bezpieczeństwa informacji, obowiązująca w Urzędzie nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. • Przeprowadzanie analiz ryzyka w niepełnym zakresie (analizy nie odnosiły się do wszystkich aktywów Jednostki a dotyczyły zagadnień ochrony danych osobowych), co nie odpowiada dyspozycji § 20 ust. 2 pkt 3 rozporządzenia KRI, • W umowie XXX, której przedmiotem jest sprawowanie opieki autorskiej nad systemami wykorzystywanymi 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, • Zawężenie procedur postępowania z incydentami do przypadków naruszeń ochrony danych osobowych. • Nieprzeprowadzenie w latach 2021 - 2022 audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 rozporządzenia KRI. • Pomieszczenie serwerowni nie dysponuje należytymi zabezpieczeniami, zgodnie z dyspozycją § 20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.	
Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 37
Zalecenia	• uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji, zgodnie z wymogami rozporządzenia KRI; • w umowie XXX., której przedmiotem jest sprawowanie opieki autorskiej nad systemami wykorzystywanymi 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; • uzupełnić procedury postępowania z incydentami o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji; • przeprowadzać analizy ryzyka odnoszące się do wszystkich aktywów Jednostki, zgodnie z dyspozycją § 20 ust. 2 pkt 3 rozporządzenia KRI; • przeprowadzać corocznie audyty wewnętrzne obejmujące wszystkie zagadnienia związane z bezpieczeństwem informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI; • w pomieszczeniu serwerowni zapewnić warunki gwarantujące utrzymanie odpowiedniego poziomu bezpieczeństwa informacji, zgodnie z dyspozycją § 20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.
Pouczenie	– od wystąpienia pokontrolnego nie przysługują środki odwoławcze, – o podjętych działaniach, mających na celu realizację zaleceń pokontrolnych, 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 up. WOJEWODY ZACHODNIOPOMORSKIEGO *Bartosz Brożyński* I Wicewojewoda Zachodniopomorski