Wojewoda
Zachodniopomorski

Znak: K-2.431.1.36.2024.10.IO
Szczecin, dnia 15 listopada 2024 r.

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 Kozielice, Kozielice 73, 74-204 Kozielice.
Osoba pełniąca funkcję Wójta Gminy Kozielice w okresie objętym kontrolą	Pan Piotr Rybkowski
Okres objęty kontrolą	od dnia 1 stycznia 2021 r. do dnia 31 lipca 2024 r.
Kontrolerzy	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, kierownik zespołu kontrolnego, Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 65/24 z dnia 19 lipca kwietnia 2024 r., nr 65/2/24 z dnia 22 lipca 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
Rodzaj kontroli i tryb kontroli	kontrola planowa, tryb zwykły
Termin kontroli	22 - 31 lipca 2024 r.

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

Osoba udzielająca wyjaśnień w trakcie kontroli	XXX Sekretarz Gminy, XXX Inspektor Bezpieczeństwa Teleinformatycznego, XXX Administrator Systemu Teleinformatycznego, na mocy *Umowy o oświadczenie usług informatycznych* zajmujący się obsługą informatyczną Urzędu[3].

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 Gminy Kozielice wykorzystywano system centralny (aplikacja Źródło) oraz system informatyczny XXX, wspomagający realizację zadań Urzędu w zakresie ewidencji ludności.
System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej, spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami 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 oraz zabezpieczeń związanych z dostępem do systemu.
(dowód: akta kontroli str. 29-30)

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**

[3] Zwany dalej Informatykiem.
[4] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), zwane dalej „rozporządzeniem KRI".

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 Kozielice 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.

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: § 19 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; **§ 19 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;* **§ 19 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 § 19 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 Kozielice, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie Nr 77.2012 Wójta Gminy Kozielice z dnia 12 grudnia 2012 r. w sprawie przyjęcia Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie*

*Gminy Kozielice (*okres funkcjonowania regulacji: 12 grudnia 2012 r. - 8 marca 2021 r.).

- *Zarządzenie Nr 16.2021 Wójta Gminy Kozielice z dnia 8 marca 2021 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Kozielicach (*okres funkcjonowania regulacji od 8 marca 2021 r.).

Dyrektywa § 19 ust. 2 pkt 1 rozporządzenia KRI wskazuje na konieczność *zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia*. Powyższy wymóg nie został spełniony. Ustalono, że w ciągu okresu obowiązywania dokumentacja nie była aktualizowana, co skutkowało między innymi brakiem wdrożenia w odpowiednim terminie regulacji, pod kątem dostosowania zapisów do obowiązujących od dnia 25 maja 2018 r. przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[5]. Ponadto należy zauważyć, że w treści aktualnego dokumentu - *Polityka Bezpieczeństwa Informacji w Urzędzie Gminy w Kozielicach*, pojawia się pojęcie inspektora ochrony danych osobowych (IODO), podczas gdy obowiązujące regulacje prawne mówią o Inspektorze Ochrony Danych[6].

Analiza aktualnie obowiązujących w Urzędzie procedur wskazuje na konieczność uzupełnienia wewnętrznych rozwiązań o kwestie przywołane w treści powyższego dokumentu kontrolnego.

(dowód: akta kontroli str. 69-121)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji.

Podstawa prawna: § 19 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

Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarządzania 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.

Metodykę przeprowadzania analizy ryzyka ujęto w *Polityce Bezpieczeństwa Informacji w Urzędzie Gminy w Kozielicach,* w rozdziale 15 *Przeprowadzanie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji.* W pkt 1 powołano się na wymóg sporządzania analizy ryzyka, *zgodnie z art. 5 ust. 2 oraz Motywem 76 Preambuły „RODO".* Wymóg przeprowadzania analizy ryzyka wynika również z dyspozycji § 19 ust. 2 pkt 3 rozporządzenia KRI.

Analiza ryzyka winna obejmować zidentyfikowane aktywa Jednostki i potencjalne rodzaje ryzyk. Ryzyko winno zostać poddane ocenie, w kierunku określenia prawdopodobieństwa

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

[6] Art. 37 ust. 1 rozporządzenia RODO: Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych (...).

wystąpienia oraz potencjalnego wpływu na działanie Jednostki w przypadku jego materializacji.
Kontrolującym przedstawiono następujące materiały dotyczące okresu objętego weryfikacją:

- Notatka służbowa z realizacji zadań związanych z analizą ryzyka w systemie teleinformatycznym w Urzędzie Gminy w Kozielicach, Kozielice 18.12.2021 r.
- Notatka służbowa z realizacji zadań związanych z analizą ryzyka w systemie teleinformatycznym w Urzędzie Gminy w Kozielicach, Kozielice 21.12.2022 r.
- Notatka służbowa z realizacji zadań związanych z analizą ryzyka w systemie teleinformatycznym w Urzędzie Gminy w Kozielicach, Kozielice 29.12.2023 r.

Okazane dokumenty nie wypełniają dyspozycji § 19 ust. 2 pkt 3 rozporządzenia KRI.
(dowód: akta kontroli str. 173-175)

2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego.
Podstawa prawna: § 19 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 § 19 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 kontrolne komputerów* – karty inwentaryzacji dla sprzętu komputerowego użytkowanego w Urzędzie. Dokumenty zawierały między innymi informacje o rodzaju użytkowanego w Jednostce sprzętu (nazwie i jego charakterystyce), nazwie oraz wersji systemu operacyjnego, nazwie procesora, zainstalowanego oprogramowania, pojemności pamięci oraz współpracujących urządzeniach peryferyjnych. Okazane formularze potwierdzają prowadzenie w Urzędzie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.
(dowód: akta kontroli str. 215-216))

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych.
Podstawa prawna: § 19 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;* **§ 19 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 § 19 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 następujących dokumentach:

- *Polityce Bezpieczeństwa Informacji w Urzędzie Gminy w Kozielicach*, w rozdziale 5 (Obowiązki osób przetwarzających dane osobowe),
- *Instrukcji zarządzania systemem informatycznym Urzędu Gminy w Kozielicach,* w rozdziale VI (Wyrejestrowanie użytkownika).

Zgodnie z zapisami procedur *do przetwarzania danych osobowych mogą być dopuszczone tylko osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych, wydane przez ADO, wraz z pisemnym oświadczeniem o zobowiązaniu się do zachowania poufności*
i w tajemnicy danych osobowych.
Kontrolującym przedstawiono:

- *Upoważnienie do przetwarzania danych osobowych* wystawione pracownikowi realizującemu zadania zlecone z zakresu administracji rządowej. Upoważnienie określa jego obszar, wynikający z zadań realizowanych na zajmowanym stanowisku oraz okres jego ważności. Dokument zawiera również oświadczenie o zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania zarówno w trakcie zatrudnienia, jak również po ustaniu stosunku pracy;
- *Rejestr upoważnień do przetwarzania danych osobowych w Urzędzie Gminy w Kozielicach.*

Zgodnie z wyjaśnieniami Wójta z dnia 30 lipca 2024 r. uprawnienia do pracy w systemach informatycznych używanych do realizacji zadań zleconych z zakresu administracji rządowej nadawane są na polecenie ustne kierownika Jednostki. 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.
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. 74, 169, 219)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.
Podstawa prawna: § 19 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

Zgodnie z wyjaśnieniami Wójta z dnia 30 lipca 2024 r., powołującego się na oświadczenie Inspektora Bezpieczeństwa Teleinformatycznego, w okresie objętym kontrolą w Urzędzie Gminy Kozielice przeprowadzono następujące szkolenia pracowników:

- *Realizacja zadań, zakres przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych CRP w Urzędzie Gminy w Kozielicach,* szkolenie zrealizowano w dniu 29 września 2021 r.*;*
- *Realizacja zadań wynikających z obowiązków państwa - gospodarza w ramach systemu HNS,* szkolenie zrealizowano w dniu 19 lipca 2022 r.*;*
- *Ochrona informacji niejawnych,* szkolenie zrealizowano w dniu 13 września 2023 r.

Z analizy dokumentacji zawierającej konspekty i informacje o programach wyżej opisanych szkoleń nie wynika, że w trakcie szkoleń poruszane były zagadnienia, których zakres tematyczny obejmował wszystkie zagadnienia wskazane w rozporządzeniu KRI. Jednakże kontrolujący przyjmują wyjaśnienia złożone przez Wójta i przedstawione w piśmie z dnia 30 lipca 2024 r., z których wynika, że w trakcie *szkoleń wykonywanych zgodnie z przyjętym Programem szkolenia obronnego na lata 2021-23* poruszono wszystkie zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI. Z przedstawionych list obecności wynika, że pracownik wskazany jako osoba realizująca zadania zlecone z zakresu administracji rządowej uczestniczyła w jednym ćwiczeniu.
Szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji, ze względu na zmieniające się zagrożenia związane z dynamicznym rozwojem technologii informatycznych winny mieć charakter cykliczny i obejmować zagadnienia wskazane w§ 19 ust. 2 pkt 6 rozporządzenia KRI.
(dowód: akta kontroli str. 169, 172)

2.6 Praca na odległość i mobilne przetwarzanie danych.

Podstawa prawna: § 19 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

Zasady prowadzenia pracy zdalnej zostały uregulowane w *Zarządzeniu Nr 6.2022 Wójta Gminy Kozielice z dnia 24 stycznia 2022 roku w sprawie: zasad wykonywania pracy zdalnej w Urzędzie Gminy w Kozielicach oraz Ośrodka Pomocy Społecznej w Kozielicach.*
Kwestie bezpiecznego korzystania z urządzeń przenośnych poruszono w *Instrukcji zarządzania systemem informatycznym Urzędu Gminy w Kozielicach:*
-w rozdziale VIII **-** *Zasady korzystania i przechowywania elektronicznych nośników informacji oraz sporządzania wydruków,* w punkcie 6 wskazując, że *osoba użytkująca przenośny komputer, tablet itp. służący do przetwarzania danych osobowych, zobowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego sprzętu poza obszarem ochrony danych*
w celu zapobieżenia dostępowi do tych danych osobie niepowołanej;
-w rozdziale IX - *Zabezpieczenie danych w systemie informatycznym,* w punkcie 7 wskazując, że *komputery i inne urządzenia oraz elektroniczne nośniki informacji, na których*

zapisane są dane, przekazywane poza pomieszczenia biurowe urzędu muszą być zabezpieczone w sposób zapewniający poufność i integralność danych.
Uregulowania wprowadzone w Jednostce nie określają zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i w przypadku świadczenia pracy na odległość, zgodnie z § 19 ust. 2 pkt 8 rozporządzenia KRI. Kontrolujący wskazują, aby opracować i wdrożyć procedurę w zakresie bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, z uwzględnieniem niezbędnych zabezpieczeń ochrony kryptograficznej w tym szyfrowania twardych dysków, połączeń szyfrowanych, itp.
Zgodnie z wyjaśnieniami Sekretarza Gminy z dnia 23 lipca 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. 85, 219)

2.7 Serwis sprzętu informatycznego i oprogramowania.
Podstawa prawna: § 19 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 na podstawie *Umowy o świadczenie usług informatycznych*, XXX[7]. Obsługa informatyczna wg. zapisów umowy obejmuje między innymi następujące czynności: administrowanie siecią teleinformatyczną; konfigurację, administrowanie, wdrażanie i zarządzanie systemami informatycznymi; przygotowanie i konserwację stanowisk komputerowych i oprogramowania.
W związku z zapisem umowy, stanowiącym że obowiązki wynikające z realizacji umowy będą realizowane w siedzibie Urzędu cztery razy w tygodniu, w godzinach pracy Jednostki, wskazanym było by uregulowanie kwestii czasu reakcji na zgłoszenie problemów związanych z działaniem systemów informatycznych w dniu tygodnia, którego nie obejmują zapisy ww. umowy. W przywołanej umowie w § 1 pkt 1 lit. b wskazano, że jej przedmiotem jest *wykonywanie obowiązków inspektora ochrony danych osobowych,* podczas gdy na stronie internetowej Urzędu (https://bip.kozielice.pl/artykul/klauzula-informacyjna-3) widnieje informacja*: Administrator wyznaczył Inspektora Ochrony Danych, którym jest XXX* (...). Kontrolujący wskazują, by odpowiednio skorygować sprzeczne zapisy.
W celu realizacji zadań z zakresu administracji rządowej zawarto *Umowę na licencję i serwis systemu*[8] XXX, której przedmiotem jest udzielenie licencji na korzystanie z systemu XXX oraz świadczenie usług serwisowych ww. systemu. Stwierdzono, że w powyższej umowie został określony maksymalny czas skutecznej naprawy oprogramowania, czym wypełniono dyspozycję § 19 ust. 2 pkt 10 rozporządzenia KRI.
Z podmiotem tym zawarto umowę powierzenia przetwarzania danych osobowych.[9]
(dowód: akta kontroli str. 180-197)

2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.
Podstawa prawna: § 19 ust. 2 pkt 13 rozporządzenia KRI: *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów*

[7] Umowy o świadczenie usług informatycznych z dnia 7 grudnia 2020 r.
[8] Umowa nr 64/COI/L/2024/SMP z dnia 20.12.2023r.
[9] Umowa powierzenia przetwarzania danych osobowych nr 64/COI/L/2024/SMP/UP z dnia 20.12.2023r.

naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Ustalenia kontroli

W *Polityce Bezpieczeństwa Informacji w Urzędzie Gminy w Kozielicach* określono sposób postępowania w przypadku stwierdzenia zaistnienia incydentu związanego z bezpieczeństwem informacji, wskazując zasady postępowania w przypadku naruszenia danych osobowych. Kwestie zgłaszania incydentów naruszenia bezpieczeństwa informacji poruszono w *Instrukcji zarządzania systemem informatycznym Urzędu Gminy w Kozielicach,* w rozdziale XV – Naruszenie bezpieczeństwa systemu informatycznego. W wyżej opisanej regulacji umieszczono zapis dotyczący naruszenia bezpieczeństwa sieciowego, nakładając na Administratora Systemu Teleinformatycznego[10] obowiązek (po stwierdzeniu faktu naruszenia) do wstrzymania udostępniania zasobów użytkownikom oraz ustalenia przyczyny tego naruszenia.

Kontrolującym przedstawiono *Rejestr naruszeń zasad ochrony danych osobowych w Urzędzie Gminy w Kozielicach*, który nie zawierał wpisów dotyczących incydentów (trzy dokonane wpisy dotyczą przeprowadzonej w Urzędzie analizy ryzyka w systemie teleinformatycznym).

(dowód: akta kontroli str. 87-88, 219-221)

2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Podstawa prawna: § 19 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 § 19 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 następujące dokumenty dotyczące okresu objętego weryfikacją:

- Ankieta dotycząca działania systemów teleinformatycznych używanych do realizacji zadań publicznych na stanowisku ds. gospodarki komunalnej i działalności gospodarczej, Załącznik Nr 1 do Zarządzenia Nr 111.2020 Wójta Gminy Kozielice z dnia 21 grudnia 2020 r.,
- Ankieta dotycząca działania systemów teleinformatycznych używanych do realizacji zadań publicznych na stanowisku ds. obsługi rady gminy, kadr, ewidencji ludności i dowodów osobistych, Załącznik Nr 1 do Zarządzenia Nr 111.2020 Wójta Gminy Kozielice z dnia 21 grudnia 2020 r.,
- Sprawozdanie z audytu wewnętrznego w zakresie bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Gminy w Kozielicach, Kozielice 23.02.2021 r.,
- *Ocena zgodności z KRI/UoKSC,* data opracowania: 27 sierpnia 2022 r.

[10] Zwany dalej AST

W 2023 roku audyt wewnętrzny, zgodnie z wyjaśnieniami Sekretarza Gminy z 23 lipca 2024 r. nie został przeprowadzony. 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 Gminy Kozielice w 2023 roku nie zrealizowano dyspozycji, o której mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI.
Audyt wewnętrzny przeprowadzony w Jednostce w 2021 roku został wykonany przez pracowników Urzędu wyznaczonych Zarządzeniem Nr 94.2020 Wójta Gminy Kozielice z dnia 23 listopada 2020 r. na Administratora Systemu Teleinformatycznego oraz Inspektora Bezpieczeństwa Teleinformatycznego. Administrator Systemu Teleinformatycznego, odpowiedzialny jest za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, natomiast Inspektor Bezpieczeństwa Teleinformatycznego, odpowiedzialny jest za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji. W przypadku audytu wykonanego w 2021 roku osoby odpowiadające za bieżące prowadzenie przetwarzania danych osobowych i bezpieczeństwo danych w systemach informatycznych weryfikowały swoje własne kompetencje i działania, pod kątem zgodności z wymogami rozporządzenia KRI. W tym zakresie rozwiązaniem jest wyznaczenie audytora (lub audytorów), który będzie dokonywał analizy obszaru, za który nie odpowiada bezpośrednio w trakcie bieżącej działalności Jednostki. Audytor wewnętrzny powinien powstrzymać się bowiem od oceny działalności operacyjnej, za którą jest odpowiedzialny, ze względu na ograniczenie obiektywizmu w ocenie tych działań.
(dowód: akta kontroli str. 135-166, 219, 222-224)

2.10 Kopie zapasowe.

Podstawa prawna: § 19 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 § 19 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 *Instrukcji zarządzania systemem informatycznym Urzędu Gminy w Kozielicach,* w rozdziale VII
– Zasady i częstotliwość tworzenia kopii zapasowych.
Kopie zapasowe baz danych, zgodnie z oświadczeniem Informatyka z dnia 30 lipca 2024 r. przechowywane są na dysku twardym oraz na nośnikach zewnętrznych typu pendrive. Nośniki zewnętrzne, na których zapisywane są kopie przechowuje się w innej lokalizacji niż miejsce wytworzenia w odpowiednio zabezpieczonej szafie.

W Urzędzie, zgodnie z oświadczeniem Informatyka 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. 84, 169-171)

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 XXX, zawarto *Umowę na licencję i serwis systemu* XXX, której przedmiotem jest udzielenie licencji na korzystanie z systemu oraz świadczenie usług serwisowych ww. systemu.
(dowód: akta kontroli str. 180-192)

2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji.
Podstawa prawna: § 19 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,
- użytkownikowi systemów wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej nie nadano uprawnień administratora, uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń.
(dowód: akta kontroli str. 211-214, 217-218)

2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych.
Podstawa prawna: § 19 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; **§ 19 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.
- Wszystkie stanowiska w Urzędzie są podłączone do zasilacza awaryjnego UPS.
- Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe.
- W budynku urzędu zainstalowano monitoring wizyjny.
- W procedurach wewnętrznych Jednostki określono zasady:
  - przesyłania danych poza obszar przetwarzania,
  - napraw i konserwacji systemu informatycznego przez podmioty zewnętrzne,
  - niszczenia elektronicznych nośników informacji.
- Serwerownia znajduje się w wydzielonej części Urzędu. XXX.

(dowód: akta kontroli str. 170, 217-218)

2.14 Rozliczalność działań w systemach teleinformatycznych.
Podstawa prawna: § 20 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; **§ 20 ust. 3 rozporządzenia KRI:** *Poza informacjami wymienionymi w ust. 2 mogą być 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; **§ 20 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 § 20 ust. 2 i 3 rozporządzenia KRI. Logi systemu są przechowywane przez okres ponad 2 lat, wobec czego wypełniono dyspozycję § 20 ust. 4 wyżej opisanego rozporządzenia.
Zgodnie z wyjaśnieniami Wójta 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. Kontrolujący wskazują aby dokumentować działania związane z przeglądaniem logów systemowych (np. w postaci dziennika administratora), tak by realizowane czynności były w pełni potwierdzone.
(dowód: akta kontroli str. 170, 208-210)

Stwierdzone nieprawidłowości w obszarze Nr 2	• Nieprzeglądanie i nieaktualizowanie obowiązującej w Urzędzie dokumentacji dotyczącej bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 1 i 2 pkt 1 rozporządzenia KRI. • Dokumentacja regulująca kwestie bezpieczeństwa informacji nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI. • Nieprzeprowadzanie analiz ryzyka, zgodnie z dyspozycją § 19 ust. 2 pkt 3 rozporządzenia KRI. • Nieprzeprowadzenie w 2023 roku audytu wewnętrznego z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 14 rozporządzenia KRI.

	• Zrealizowanie audytu wewnętrznego z zakresu bezpieczeństwa informacji przez osoby odpowiedzialne za bieżące funkcjonowanie obszarów poddawanych analizie. • Nieuwzględnienie zabezpieczeń ochrony kryptograficznej w procedurach określających zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i w przypadku świadczenia pracy na odległość, zgodnie z wymogami § 19 ust. 2 pkt 8 i 9 rozporządzenia KRI. • Niesporządzanie dokumentacji dotyczącej testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz dokumentacji działań związanych z przeglądaniem logów systemowych, zgodnie z dyspozycją § 19 ust. 1 rozporządzenia KRI, w zakresie rozliczalności prowadzonych działań. • Pomieszczenie serwerowni nie dysponuje zabezpieczeniami, zgodnie z dyspozycją § 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.
Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 5/2024
Zalecenia	• Przeglądać i aktualizować dokumentację dotyczącą bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 1 i 2 pkt 1 rozporządzenia KRI. • Uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji zgodnie z wymogami przepisów rozporządzenia KRI. • Przeprowadzać analizę ryzyka, zgodnie z dyspozycją § 19 ust. 2 pkt 3 rozporządzenia KRI. • Przeprowadzać co roku audyt wewnętrzny z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 19 ust. 2 pkt 14 rozporządzenia KRI. • Powierzyć realizację audytów wewnętrznych osobie (podmiotowi), która nie jest odpowiedzialna za bieżące funkcjonowanie obszarów poddawanych analizie. • Wprowadzić zabezpieczenia ochrony kryptograficznej do procedur określających zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i w przypadku świadczenia pracy na odległość, zgodnie z wymogami § 19 ust. 2 pkt 8 i 9 rozporządzenia KRI. • Sporządzać dokumentację dotyczącą testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz dokumentacji działań związanych z przeglądaniem logów systemowych, zgodnie z dyspozycją § 19 ust.

	1 rozporządzenia KRI, w zakresie rozliczalności prowadzonych działań. • W pomieszczeniu serwerowni zapewnić warunki gwarantujące utrzymanie odpowiedniego poziomu bezpieczeństwa informacji, zgodnie z dyspozycją § 19 ust. 2 pkt 12 lit. b i e oraz ust. 4 rozporządzenia KRI.
Pouczenia	– zgodnie z art. 48 ustawy z dnia 15 lipca 2011 roku o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224) 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 upoważnienia Wojewody Zachodniopomorskiego Bartosz Brożyński I Wicewojewoda Zachodniopomorski