WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 16 kwietnia 2024 r.

.

Znak: K-2.431.1.58.2023.7.IO

WYSTĄPIENIE POKONTROLNE

Przedmiot kontroli	Działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.
Nazwa i adres organu kontrolującego	Wojewoda Zachodniopomorski, ul. Wały Chrobrego 4, 70-502 Szczecin.
Nazwa i adres organu kontrolowanego	Wójt Gminy Warnice, Warnice 66, 74-201 Warnice.
Osoba pełniąca funkcję Wójta Gminy Warnice w okresie objętym kontrolą / okresie prowadzenia kontroli	Pani Alina Werstak
Okres objęty kontrolą	od dnia 1 stycznia 2020 r. do dnia 10 listopada 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 105/23 z dnia 31 października 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	6-10 listopada 2023 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Ireneusz Rożuk – stanowisko ds. sportu, administratora systemu teleinformatycznego, pomocy materialnej; Pan Jarosław Woźniak – 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 Warnice wykorzystywano system centralny XXX oraz system informatyczny XXX, wspomagający realizację zadań Urzędu w zakresie ewidencji ludności. System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej Urzędu Gminy Warnice 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*

[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".

	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 Warnice 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. 79)	
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 Warnice, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:	

- *Zarządzenie Nr 33/2018 Wójta Gminy Warnice z dnia 25 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*;
- *Zarządzenie Nr 64/2020 Wójta Gminy Warnice z dnia 10 listopada 2020 r. w sprawie polecenia, zasad i wyłączenia z wykonywania pracy zdalnej w Urzędzie Gminy Warnice;*
- *Procedura upoważnienia do dostępu do danych osobowych w jednostce, 21 stycznia 2020r.;*
- *Regulamin użytkowania zasobów komputerowych i sieci komunikacyjnych oraz ochrony danych;*
- *Procedura postępowania z danymi osobowymi przetwarzanymi na terenie instytucji ze szczególnym uwzględnieniem działań dokonywanych w obszarze korespondencji e- mail oraz zewnętrznych nośników danych*.

W wyniku analizy aktualnie obowiązującej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że funkcjonujące w Jednostce procedury spełniają wymogi określone w § 20 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji.

Niemniej jednak odwołanie w samej nazwie dokumentów, zarówno w polityce jak i instrukcji do ochrony danych osobowych (*Polityka Ochrony Danych Osobowych w Gminie Warnice, Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych*) sugeruje zawężenie obszaru bezpieczeństwa informacji do zagadnień związanych z ochroną danych osobowych, podczas gdy ochronie winny podlegać wszystkie przetwarzane przez Urząd informacje.

Kontrolujący wskazują na konieczność usunięcia nieścisłości w obowiązujących dokumentach:

- *zarządzenie Nr 33/2018 Wójta Gminy Warnice z dnia 25 maja 2018 r.* wprowadza *Politykę Bezpieczeństwa*, podczas gdy dokument zatytułowano *Polityka Ochrony Danych Osobowych w Gminie Warnice;*
- w *Polityce Ochrony Danych Osobowych w Gminie Warnice,* zarówno w spisie treści dokumentu, jak i oznaczeniu tytułu § 6 pojawia się pojęcie Inspektora Ochrony Danych Osobowych, podczas gdy obowiązujące regulacje prawne mówią o Inspektorze Ochrony Danych[4]. W treści dokumentu użyto właściwego nazewnictwa.

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.

(dowód: akta kontroli str. 64, 100-124, 172-176, 229-286)

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 ryzyka przetwarzania danych osobowych,* dokument stanowiący załącznik do audytu okresowego 2020/2021.

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

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

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 Gminy Warnice nie zrealizowano w pełni dyspozycji, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI.
(dowód: akta kontroli str. 65, 88-99)

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 *Spis inwentarzowy komputerów w Urzędzie Gminy w Warnicach, stan na 15.03.2023r.* Dokument zawierał informacje dotycząca rodzaju użytkowanego w Jednostce sprzętu (nazwa i jego charakterystyka), zainstalowanego oprogramowania oraz współpracujących urządzeń peryferyjnych. Okazany formularz potwierdza, prowadzenie w Urzędzie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.
(dowód: akta kontroli str. 205-228)

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 *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* (w § 7) oraz *Procedurze upoważnienia do dostępu do danych osobowych w jednostce.*
Kontrolującym przedstawiono:

- *upoważnienie 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;
- *oświadczenie o zachowaniu poufności*, w którym zawarto miedzy innymi oświadczenie pracownika o zachowaniu w tajemnicy przetwarzanych danych, wskazując okres obowiązywania zobowiązania w trakcie zatrudnienia, jak również po ustaniu stosunku pracy;
- *zobowiązanie do zachowania tajemnicy służbowej;*
- potwierdzenie zapoznania pracowników Urzędu z treścią „*Procedury upoważnienia do dostępu do danych osobowych w jednostce" otrzymaną mailem w dniu 28.01.2020 r.*

Zgodnie z wyjaśnieniami Wójta z 10 listopada 2023 r. uprawnienia do pracy w systemach informatycznych nadawane są przez Informatyka na ustne polecenie kierownika jednostki organizacyjnej. Dla tych czynności nie jest tworzona dodatkowa dokumentacja. Kontrolujący wskazują by wewnętrzne procedury uzupełnić o dokument, który poświadczać będzie realizowanie wymogu dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych; pisemny wniosek osób upoważnionych spowoduje, że proces nadawania i odbierania uprawnień będzie w pełni potwierdzony.
W okresie objętym kontrolą wystąpiły trzy przypadki zmiany uprawnień do pracy w systemie informatycznym XXX. W dwóch przypadkach nastąpiło to w związku z rozwiązaniem stosunku pracy, a w jednym spowodowane było zmianą zakresu obowiązków pracownika. Dane z systemu informatycznego wskazują, że w przypadku pracownika o inicjałach EP, z którym rozwiązano stosunek pracy z końcem sierpnia 2023 r. cofnięcie uprawnień nastąpiło 3 listopada 2023 r., co nie wypełnia dyspozycji bezzwłocznego odbioru uprawnień, po zaistnieniu okoliczności uzasadniających podjęcie stosownych działań. Z wyjaśnień złożonych przez Informatyka wynika, że uprawnienia pracownikowi o inicjałach EP zostały cofnięte bezpośrednio po ustaniu świadczenia pracy, natomiast data 3 listopada 2023r., która pojawia się w systemie komputerowym wynika z faktu otwarcia przez Informatyka karty pracownika EP w celu porównania zakresu uprawnień nadanych nowemu pracownikowi z uprawnieniami poprzedniego pracownika. Informatyk zwrócił się z prośbą o wsparcie techniczne producenta oprogramowania XXX, w celu odnalezienia w logach systemu potwierdzenia faktu odbioru uprawnień z zachowaniem terminu wynikającego z przyjętych uregulowań. Z załączonej do wyjaśnień złożonych przez Informatyka korespondencji, prowadzonej z przedstawicielem producenta oprogramowania wynika, że:
- w programie zapisuje się data ostatniej aktualizacji danych użytkownika
- funkcjonalność pozwalająca na śledzenie zmian dotyczących uprawnień użytkownika zostanie zaimplementowana do programu w okresie styczeń - luty 2024 r.
Kontrolujący przyjmują wyjaśnienia złożone w tym zakresie.
(dowód: akta kontroli str. 65, 81-84, 100-116, 177-201)

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

Zgodnie z wyjaśnieniami Wójta z 10 listopada 2023 r. w okresie objętym kontrolą w Urzędzie Gminy Warnice wyznaczeni pracownicy Jednostki uczestniczyli w szkoleniu online, w trakcie którego poruszane były zagadnienia związane z cyberatakami po wybuchu wojny w Ukrainie, działaniami związanymi z obowiązującym na terenie kraju stopniem alarmowym CRP (CHARLIE-CRP) oraz kwestie zabezpieczenia parkingów i dostępu do budynku Jednostki. W Urzędzie nie sporządzono listy dokumentującej udział pracowników w wyżej opisanym szkoleniu.

Pracownicy wykonujący zadania zlecone z administracji rządowej nie uczestniczyli bezpośrednio w tym szkoleniu, natomiast zostali (zgodnie z wyjaśnieniami Wójta) poinstruowani przez pracowników uczestniczących w szkoleniu *w niezbędnym zakresie adekwatnym do wykonywanych obowiązków*.

Kontrolującym przedstawiono ponadto dokumenty, które nie dotyczyły okresu objętego kontrolą:

- *Listę obecności na szkoleniu z zakresu RODO*, które odbyło się 25 czerwca 2019 roku,
- *Listę odbioru karty szkolenia wstępnego z zakresu ochrony danych osobowych*, zawierającą imię i nazwisko uczestnika oraz datę odbioru i zwrotu karty wraz z własnoręcznym podpisem osoby dokonującej wpisu. Wpisy pochodziły z 2019 roku.

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

Z przedstawionych wyjaśnień wynika, że zakres tematyczny szkolenia przeprowadzonego w Urzędzie, zarówno w okresie objętym kontrolą (jak i w 2019 roku, który nie był okresem objętym kontrolą) nie ujmował wszystkich zagadnień wskazanych w § 20 ust. 2 pkt 6 rozporządzenia KRI. Wobec powyższych ustaleń należy stwierdzić, że w Jednostce nie zrealizowano w pełni dyspozycji § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 64, 80, 202-203)

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:

1. *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, wprowadzonej Zarządzeniem Nr 33/2018 Wójta Gminy Warnice z dnia 25 maja 2018 r.;*
2. *Procedurze postępowania z danymi osobowymi przetwarzanymi na terenie instytucji ze szczególnym uwzględnieniem działań dokonywanych w obszarze korespondencji e- mail oraz zewnętrznych nośników danych*;
3. *Regulaminie użytkowania zasobów komputerowych i sieci komunikacyjnych oraz ochrony danych.*

W wyżej wymienionych dokumentach uregulowano między innymi kwestie wynoszenia poza obszar organizacji nośników z danymi osobowymi, wprowadzając wymóg uzyskania zgody Administratora Danych Osobowych na użytkowanie urządzeń przenośnych poza organizację. Wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych przed opuszczeniem Jednostki oraz wymóg zabezpieczenia hasłem i zaszyfrowania informacji przekazywanych przy użyciu poczty elektronicznej.
Zarządzeniem Nr 64/2020 Wójta Gminy Warnice z dnia 10 listopada 2020 r. w sprawie polecenia, zasad i wyłączenia z wykonywania pracy zdalnej w Urzędzie Gminy Warnice określono zasady świadczenia pracy w formie pracy zdalnej.
Zgodnie z wyjaśnieniami Wójta z 7 listopada 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. 64, 67-72, 118-120, 172-176, 280)

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 na podstawie umowy zlecenia czynności *polegających na prowadzeniu spraw z zakresu informatyki i komputeryzacji Urzędu Gminy Warnice* XXX[5]. Obsługa informatyczna wg. zapisów umowy obejmuje między innymi następujące czynności: opiekę nad oprogramowaniem sieciowym, zapewnienie obsługi informatycznej podczas wyborów i referendów, obsługę incydentów związanych z cyberbezpieczeństwem, konsultacje telefoniczne i bezpośrednie. W powyższej umowie uregulowano kwestię czasu reakcji na zgłoszenie konieczności realizacji zadań wynikających z zapisów umowy. Z XXX zawarto *Umowę powierzenia przetwarzania danych osobowych*[6].
W celu realizacji zadań z zakresu administracji rządowej zawarto *Umowę na licencję i serwis systemu*[7] 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 § 20 ust. 2 pkt 10 rozporządzenia KRI, zawierającego zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Z podmiotem tym zawarto umowę powierzenia przetwarzania danych osobowych.[8]

(dowód: akta kontroli str. 151-171, 290-294)

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 *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,* w § 15 - *Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu*

[5] Umowa zlecenie nr 37/2021 z dnia 27.12.2021r.
[6] Umowa powierzenia przetwarzania danych osobowych z 27.12.2021 r.
[7] Umowa nr 170/COI/L/2023/SMP
[8] Umowa powierzenia przetwarzania danych osobowych nr 170/COI/L/2023/SMP/UP.

informatycznego 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 Specjaliście do spraw ochrony danych osobowych, ADO[9] oraz ASI[10] w przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji.

W *Polityce Ochrony Danych Osobowych,* w § 26 - *Postępowanie w razie zaistnienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych lub naruszenia zasad przetwarzania danych osobowych* określono zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych, zgodnie z wymogami rozporządzenia RODO[11]. Ponadto w *Regulaminie użytkowania zasobów komputerowych i sieci komunikacyjnych oraz ochrony danych* ujęto *Skróconą instrukcję postępowania w przypadku naruszenia ochrony danych osobowych.*

Kontrolującym przedstawiono *Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych*, który nie zawierał wpisów. Zgodnie z oświadczeniem Wójta w okresie objętym kontrolą nie wystąpiły incydenty naruszenia bezpieczeństwa informacji.

(dowód: akta kontroli str. 64, 78, 123, 249, 284-285)

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 kontroli w zakresie funkcjonowania obszaru ochrony danych osobowych Urząd Gminy Warnice. Warnice, kwiecień 2021 rok.*
- *Ocena zgodności z KRI/UoKSC 16.03.2022.*

W wyniku analizy powyższej dokumentacji stwierdzono nieprawidłowość w postaci nieobjęcia w roku 2021 audytem pełnego zakresu zagadnień związanych z bezpieczeństwem informacji. Audyt dotyczył głównie zagadnień ochrony danych osobowych w kontekście przepisów rozporządzenia RODO. Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy Warnice w roku 2021 nie realizowano w pełni dyspozycji, o której mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI.

W 2020 roku nie został przeprowadzony w Urzędzie audyt wewnętrzny z zakresu bezpieczeństwa informacji. Zgodnie z wyjaśnieniami Wójta z 7 listopada 2023 r. audyt z powodu pandemii został przesunięty na początek 2021 roku.

Nieprzeprowadzanie audytu lub przeprowadzanie audytu wewnętrznego w niepełnym zakresie może wpływać na ocenę skuteczności przyjętych w Jednostce rozwiązań w zakresie bezpieczeństwa informacji. Raport z audytu stanowi bowiem istotne źródło informacji dla

[9] Administrator Danych Osobowych
[10] Administrator Systemów Informatycznych
[11] 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).

kierownictwa Jednostki o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących.

(dowód: akta kontroli str. 65, 125-150)

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.

Kopie programu XXX zgodnie z wyjaśnieniami Wójta z dnia 10 listopada 2023 r. wykonywane są raz w tygodniu w wersji przyrostowej i przechowywane na dedykowanym do tego celu nośniku danych. *Nośnik umieszczony jest w metalowej, zamykanej szafie w miejscu wytworzenia*. Kopie w pełnej wersji wykonywane są kilka razy w roku. Kopie zapasowe systemów działających w sieci Urzędu wykonywane są codziennie, *przechowywane są na osobnym nośniku danych w miejscu wytworzenia*.

Z wyjaśnień Wójta wynika również, że raz w miesiącu realizowane jest próbne testowane w celu sprawdzenia poprawności wykonania kopii bezpieczeństwa, przy czym nie sporządza się dokumentacji potwierdzającej przeprowadzenie testów.

W *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* określono osobę odpowiedzialną za sporządzanie kopii zapasowych, wskazano na konieczność testowania kopii oraz oznaczono miejsce przechowywania wytworzonych kopii zapasowych. W dokumencie nie określono natomiast częstotliwości tworzenia kopii (w procedurze, w stosunku do tego zadania użyto określenia, że *za tryb i częstotliwość tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego*). W odniesieniu do zagadnienia testowania kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania nie wyznaczono precyzyjnie interwału czasowego dla wykonywania tych działań (w procedurze, w stosunku do tego zadania użyto określenia *regularnie*).

Kontrolujący wskazują by w wewnętrznych procedurach doprecyzować zapisy dotyczące częstotliwości tworzenia i testowania kopii zapasowych (np. zgodne z dotychczasową praktyką) oraz dokumentować te czynności, tak by realizowane działania były w pełni potwierdzone.

Nośniki kopii zapasowych winny być przechowywane w innej lokalizacji niż miejsce ich wytworzenia, z uwagi na ryzyko utraty informacji w przypadku zaistnienia sytuacji nadzwyczajnych (w wyniku których zniszczeniu mogą ulec urządzenia i dane na nich przechowywane), co bezpośrednio może przyczynić się do braku zapewnienia ciągłości działania Jednostki i zaistnienia zakłóceń w jej funkcjonowaniu.

(dowód: akta kontroli str. 79-80, 280-281)

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. 151-165)

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 stanowisk komputerowych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że:
- dostęp do systemu operacyjnego na urządzeniach możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- komputery miały zainstalowane oprogramowanie antywirusowe oraz skonfigurowane wygaszacze ekranu,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitora 1 stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej (podlegających kontroli) umożliwiało odczyt wyświetlanych danych przez osoby postronne,
- jednemu użytkownikowi nadano uprawnienia administratora, co umożliwiało instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego,
- wejście do serwerowni wyposażono w antywłamaniowe drzwi wejściowe; w pomieszczeniu brak czujnika dymu, gaśnicy oraz klimatyzacji.
W *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* uregulowano zasady serwisu i konserwacji oraz utylizacji sprzętu elektronicznego.

(dowód: akta kontroli str. 73-77, 281, 287-288)

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 Firewall. Urządzenia informatyczne Jednostki są podłączone do lokalnych zasilaczy awaryjnych UPS. Na komputerach 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. (dowód: akta kontroli str. 73, 80, 172-176)	
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 odnotowane 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, 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.

Podczas weryfikacji poprawności realizacji dyspozycji cofania uprawnień do pracy w systemie informatycznym stwierdzono fakt braku zapisów w logach systemu XXX zmian dotyczących uprawnień użytkowników. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie działania wykonał w systemie teleinformatycznym, szczególnie gdy przetwarzanie danych podlega prawnej ochronie. Brak zapisów w logach systemu narusza § 21 ust. 2 rozporządzenia KRI, stanowiącego, że *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników (...) polegające na dostępie do (...) systemu z uprawnieniami administracyjnymi(...).* Z wyjaśnień przedstawiciela producenta oprogramowania wynika, że funkcjonalność pozwalająca na śledzenie zmian dotyczących uprawnień (nadawania i ich modyfikacji) zostanie zaimplementowana do programu w okresie styczeń - luty 2024 r.

(dowód: akta kontroli str. 79, 83-87)

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,
- Zakres tematyczny szkolenia dotyczącego bezpieczeństwa informacji przeprowadzonego w Urzędzie, w okresie objętym kontrolą nie obejmował wszystkich zagadnień wskazanych w § 20 ust. 2 pkt 6 rozporządzenia KRI.
- Nieobjęcie w roku 2021 audytem pełnego zakresu zagadnień związanych z bezpieczeństwem informacji, co bezpośrednio przekłada się na niepełną realizację dyspozycji, o której mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI.
- Niesporządzanie dokumentacji dotyczącej testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz przechowywanie kopii zapasowych w miejscu wytwarzania danych, co jest niezgodne z § 20 ust. 2 pkt 12 lit. b i e rozporządzenia KRI.
- Posiadanie przez pracownika realizującego zadania zlecone z zakresu administracji rządowej uprawnień administratora, co jest sprzeczne z dyspozycją § 20 ust. 2 pkt 9 rozporządzenia KRI.
- Niewłaściwe ustawienie monitora stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej umożliwiające odczyt wyświetlanych danych przez osoby postronne, co jest sprzeczne z dyspozycją § 20 ust. 2 pkt 9 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 12
Zalecenia	• przeprowadzać analizy ryzyka odnoszące się do wszystkich aktywów Jednostki, zgodnie z dyspozycją § 20 ust. 2 pkt 3 rozporządzenia KRI; • przeprowadzać cyklicznie szkolenia, których celem jest zagwarantowanie bezpieczeństwa w zakresie przetwarzania informacji, obejmujące wszystkie zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI; • przeprowadzać corocznie audyty wewnętrzne obejmujące wszystkie zagadnienia związane z bezpieczeństwem informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI; • sporządzać dokumentację dotyczącą testowania kopii zapasowych danych i systemów na potrzeby weryfikacji poprawności i stanu ich wykonywania oraz przechowywać kopie zapasowe wszystkich systemów i programów poza miejscem wytwarzania danych, zgodne z § 20 ust. 2 pkt 7 i 12 lit. b i e rozporządzenia KRI; • odebrać pracownikowi realizującemu zadania zlecone z zakresu administracji rządowej uprawnienia administratora, by zrealizować dyspozycję § 20 ust. 2 pkt 9 rozporządzenia KRI; • ustawić monitor stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej w taki sposób, by uniemożliwić odczyt wyświetlanych danych przez osoby postronne, do czego zobowiązują § 20 ust. 2 pkt 9 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