WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 6 lipca 2022r.

Znak: K-2.431.1.17.2022.11.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 Morynia, Plac Wolności 1, 74-503 Moryń.
Osoba pełniąca funkcję Burmistrza Morynia w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Józef Piątek
Okres objęty kontrolą	od dnia 1 stycznia 2019 r. do dnia 23 marca 2022 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: 1. Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego*, 2. Pani Iwona Olesińska – inspektor wojewódzki.
Nr upoważnienia	Nr 18/22 z dnia 4 marca 2022 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	9-23 marca 2022 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły[3]

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2021r., poz. 2070.
[3] Mając na względzie obowiązujący na obszarze Rzeczypospolitej Polskiej stan epidemii (rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r., Dz. U. z 2022r. poz. 340) przedmiotowe czynności na podstawie art. 21 ustawy o kontroli w administracji rządowej, przeprowadzone zostały poza siedzibą podmiotu kontrolowanego, o czym Burmistrz Morynia został poinformowany w piśmie z dnia 4 marca 2022 r. (dowód: akta kontroli str. 47).

Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Maciej Molenda- Informatyk.
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 oraz oświadczenia Burmistrza Morynia z dnia 3 marca 2022 r. ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Miejskim w Moryniu wykorzystywano jeden system centralny (aplikacja Źródło) oraz system informatyczny XXX, wspomagający realizację zadań Urzędu w zakresie ewidencji ludności i rejestru wyborców. System centralny (aplikacja Źródło), dostępny przez stronę WWW podlegał kontroli w zakresie formalnego posiadania uprawnień przez pracowników Urzędu Miejskiego. System do realizacji zadań zleconych z zakresu administracji rządowej, współpracuje z systemem zewnętrznym oraz spełnia minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. (dowód: akta kontroli str. 55, 61, 157-158)	
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.*

[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".

	§ 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 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 Miejskim w Moryniu, zgodnie z oświadczeniem Burmistrza Morynia z dnia 11 marca 2022 r. 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 Windows-1250. (dowód: akta kontroli str.55)	
Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1: - nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.	
Ocena obszaru kontroli nr 1	**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 miał obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.

W Urzędzie Miejskim w Moryniu, w okresie objętym kontrolą obowiązywały następujące uregulowania w zakresie bezpieczeństwa informacji:

- *Polityka Ochrony Danych Osobowych w Urzędzie Miejskim w Moryniu* wprowadzona *Zarządzeniem Nr 65/2018 Burmistrza Morynia z dnia 25 maja 2018 r.,*
- *Instrukcja Zarządzania RODO - wykaz zabezpieczeń RODO w Urzędzie Miejskim w Moryniu,* stanowiąca załącznik nr 1 do *Polityki Ochrony Danych Osobowych,*
- *Regulamin Ochrony Danych Osobowych w Urzędzie Miejskim w Moryniu,* stanowiący załącznik nr 2 do *Polityki Ochrony Danych Osobowych,*
- *Analiza ryzyka ogólnego i ocena skutków dla przetwarzania danych (DPIA) w Urzędzie Miejskim w Moryniu,* stanowiąca załącznik nr 3 do *Polityki Ochrony Danych Osobowych.*

W wyniku analizy aktualnie obowiązującej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że:

- w *Polityce ochrony danych osobowych* zdefiniowano *katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych.* Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (...),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo informacji w całej organizacji i nie ograniczać się wyłącznie do ochrony danych osobowych. Wdrożone w Jednostce regulacje dotyczące zgłaszania incydentów bezpieczeństwa informacji odnoszą się do danych osobowych,

- *celem audytów,* zgodnie z zapisami obowiązującej *Polityki Ochrony Danych Osobowych jest ocena czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO*. Zawężenie przy przeprowadzaniu audytów wewnętrznych obszaru badania do zagadnień wskazanych w powyższym dokumencie jest niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI, które stanowi, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji (...),*

- *w Instrukcji Zarządzania RODO,* w punkcie 8.2 *Ochrona przed nieautoryzowanym dostępem do sieci lokalnej* wskazano czynności oraz mechanizmy, które mają zabezpieczać systemy informatyczne przed takim dostępem, natomiast nie przypisano obowiązków i odpowiedzialności za realizację tych czynności,

- nie uregulowano kwestii dokonywania przeglądów obowiązujących w Jednostce procedur dotyczących bezpieczeństwa informacji, co bezpośrednio przekłada się na niewypełnienie dyrektywy § 20 ust. 2 pkt 1 rozporządzenia KRI *zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,*

- w procedurach wewnętrznych pojawia się pojęcie administrator/informatyk –osoba wskazana do wykonania zadań lub odpowiedzialna za realizację określonych czynności. W dokumencie *Polityka Ochrony Danych Osobowych,* w rozdziale Definicje pojęcie administrator/ informatyk nie występuje, natomiast zdefiniowano w nim funkcję *administratora(danych)* i jest to *osoba fizyczna lub prawna, organ publiczny (...), który (...) ustala cele i sposoby przetwarzania danych*

osobowych. Wobec nieścisłości zapisów niemożliwe jest wskazanie osoby lub osób odpowiedzialnych za realizację zadań. Należy doprecyzować zapisy, tak by nie zachodziły wątpliwości komu przypisano realizację i odpowiedzialność za powierzone zadania.

Ustalono, że obowiązująca *w* Urzędzie Miejskim w Moryniu dokumentacja z zakresu bezpieczeństwa informacji została zaktualizowana, pod kątem dostosowania do wymogów rozporządzenia RODO. [5]

Mając na względzie powyższe, należy uzupełnić i uściślić obowiązujące w Urzędzie procedury, w celu wdrożenia kompleksowego systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji.

(dowód: akta kontroli str. 62-145, 202)

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 i ocenę skutków przetwarzania danych osobowych w Urzędzie Miejskim w Moryniu w roku 2019.* W dokumencie określono zagrożenia dla zidentyfikowanych zasobów, źródła zagrożeń, siłę wpływu zdarzeń na czynniki decydujące o bezpieczeństwie informacji. Dla poszczególnych grup zagrożeń określono poziom ryzyka, zalecenia w celu minimalizacji jego materializacji, określono poziom ryzyka przed wprowadzeniem zabezpieczeń oraz poziom ryzyka po wprowadzeniu zabezpieczeń, wskazano także właściciela ryzyka. Elementem analizy jest oświadczenie Burmistrza Morynia o zapoznaniu z wynikami procesu szacowania ryzyka.

Z wyjaśnień Burmistrza z dnia 11 marca 2022 r. wynika, że w okresie objętym kontrolą analiza ryzyka wykonana była w Urzędzie w 2019 r. W kolejnych latach 2020 i 2021 nie przeprowadzono analiz, gdyż nie stwierdzono zmian, które wpłynęłyby na wynik szacowania ryzyka.

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.

(dowód: akta kontroli str. 55, 108-145)

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

[5] 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), dalej RODO.

i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ponadto, zgodnie z pkt 8.1.1 normy PN-ISO/IEC 27002:2014, wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis. Inwentaryzacja m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.
Inwentaryzacja zasobów informatycznych w Urzędzie jest realizowana w wersji elektronicznej przy wykorzystaniu programu komputerowego eAuditor, generującego raporty zawierające informacje dotyczące sprzętu i oprogramowania, rodzaju systemu operacyjnego oraz współpracujących urządzeń peryferyjnych. Inwentaryzacja urządzeń wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej prowadzona jest przy użyciu arkusza kalkulacyjnego. Kontrolującym przedstawiono karty ewidencyjne jednostek komputerowych użytkowanych w Urzędzie oraz spis sprzętu, prowadzony w formie arkusza kalkulacyjnego.
Mając na uwadze powyższe stwierdzono, że w Urzędzie jest prowadzona inwentaryzacja sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str.175-183, 209)

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. W obowiązującej w Jednostce *Polityce Ochrony Danych Osobowych w Urzędzie Miejskim w Moryniu* uregulowano kwestie udzielania upoważnień do przetwarzania danych osobowych. Nadawanie, zmiana i odbieranie pracownikom uprawnień do pracy w systemie informatycznym unormowano w dokumencie - *Instrukcja Zarządzania RODO - wykaz zabezpieczeń RODO w Urzędzie Miejskim w Moryniu*, w ten sposób, że proces odbywa się na polecenie przełożonych lub innych osób upoważnionych, a za wykonanie czynności odpowiada informatyk. Procedurę wykonuje się na ustne polecenie przełożonego. Zapisy procedury dotyczące nadawania i odbierania uprawnień w systemach informatycznych nie korespondują z wydawanymi *Upoważnieniami (poleceniami) do przetwarzania danych osobowych*, z treści których wynika do jakich zasobów informatycznych otrzymują dostęp poszczególni pracownicy. Wskazanym jest doprecyzowanie zapisów procedury poprzez wskazanie, że

nadawanie/modyfikowanie/odbieranie uprawnień dokonywane jest na pisemny wniosek uprawnionych osób, co czyni, że proces jest w pełni udokumentowany.

Kontrolującym przedstawiono *Oświadczenie o poufności* zobowiązujące między innymi do zachowania w tajemnicy danych osobowych, do których pracownik ma lub będzie miał dostęp w związku z wykonywaniem zadań powierzonych przez Administratora Danych. W dokumencie o zachowaniu tajemnicy nie wskazano czasu trwania tego zobowiązania. Kontrolujący sugerują, by zrewidować powyższy dokument pod kątem wskazania okresu obowiązywania zobowiązania i rozszerzyć go także na okres po ustaniu stosunku pracy.

W okresie objętym kontrolą wystąpił jeden przypadek rozwiązania stosunku pracy z pracownikiem realizującym zadania zlecone z zakresu administracji rządowej. Przypadek ten był przedmiotem badania pod kątem podjęcia niezwłocznych działań, mających na celu cofnięcie dostępu do systemu informatycznego. Mimo wniosku kontrolujących o udokumentowanie wydrukiem z logów faktu zablokowania (z poziomu administratora systemu) dostępu użytkownika do środowiska operacyjnego, nie przedstawiono takiego dowodu. Z wyjaśnień złożonych przez Burmistrza Morynia z dnia 16 marca 2022 r. wynika, że producent oprogramowania nie zaimplementował funkcji związanej z *generowaniem logów mogących udokumentować czynności blokowania użytkownika*. Powyższa funkcjonalność ma, zgodnie z powyżej przywołanymi wyjaśnieniami Burmistrza zostać dodana w kolejnej wersji systemu.
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. Braku 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(...).*

W celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem wprowadzono zabezpieczenia polegające m.in. na konieczności logowania się do systemów informatycznych z wykorzystaniem unikalnego identyfikatora oraz hasła o odpowiedniej złożoności.
Z uwagi na fakt, że kontrola prowadzona była w trybie zdalnym nie dokonano oględzin stanowisk komputerowych.

(dowód: akta kontroli str. 55, 60, 66, 73, 157-163, 211)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Podstawa prawna	**§ 20 ust. 2 pkt 6 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*

Ustalenia kontroli
W okresie objętym kontrolą w Urzędzie przeprowadzono następujące szkolenia pracowników Jednostki, z zakresu bezpieczeństwa informacji:

- *Ochrona danych osobowych zgodnie z RODO* (31 stycznia 2019 r.),
- *Zasady ochrony danych osobowych* (22 grudnia 2020 r.),

- *Zasady ochrony danych osobowych* (6 grudnia 2021 r.).

Udział w szkoleniach dokumentowały listy obecności zawierające imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w szkoleniach uczestniczyli pracownicy zaangażowani w proces przetwarzania informacji w systemach teleinformatycznych oraz rejestrach publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej.
Z przedstawionej dokumentacji wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie, w badanym okresie obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 164-169)

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 na komputerach przenośnych i sprzęcie mobilnym z uwzględnieniem niezbędnych zabezpieczeń, w tym szyfrowania twardych dysków zostały unormowane w *Instrukcji zabezpieczeń RODO - wykaz zabezpieczeń RODO w Urzędzie Miejskim w Moryniu*, w rozdziale 8.1 *Bezpieczeństwo przetwarzania danych poza organizacją*.
Zgodnie z wyjaśnieniami Burmistrza Morynia z dnia 11 marca 2022 r. do realizacji zadań zleconych z zakresu administracji rządowej nie wykorzystywano urządzeń w przetwarzaniu mobilnym i pracy na odległość.

(dowód: akta kontroli str. 55, 75-76)

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 Jednostki realizowana jest przez pracownika zatrudnionego w Urzędzie Miejskim w Moryniu, na stanowisku Informatyka. W zakresie obowiązków pracownika znajduje się m.in.: zarządzanie siecią teleinformatyczną, systemami informatycznymi oraz ich eksploatacją; monitoring systemu bezpieczeństwa sieci w zakresie ochrony haseł i zasobów sieci; wykonywanie kopii bezpieczeństwa programów i archiwizacja baz danych; aktualizacja oprogramowania oraz nadzór nad pracą urządzeń wspomagających.
W celu realizacji zadań z zakresu administracji rządowej zawarto *Umowę na licencję i serwis systemu*[6] XXX. Przedmiotem umowy jest udzielenie licencji na korzystanie z systemu XXX oraz świadczenie usług serwisowych ww. systemu. Stwierdzono, że w 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. XXX zawarto umowę powierzenia przetwarzania danych osobowych.[7]

(dowód: akta kontroli str. 184-201)

[6] Umowa nr 97/COI/L/2022/SMP
[7] Umowa powierzenia przetwarzania danych osobowych nr 97/COI/L/2022/SMP/UP

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 *Polityce ochrony danych osobowych*, w rozdziale 7 *Instrukcja postępowania z incydentami* zdefiniowano *katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych.* W *Regulaminie ochrony danych osobowych, w* rozdziale 10 *Skrócona* i*nstrukcja postępowania w przypadku naruszenia ochrony danych osobowych* opisano sposób reagowania w przypadku stwierdzenia lub podejrzenia zaistnienia tego typu naruszeń.

Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (...),* wobec czego elementy systemu zarządzania bezpieczeństwem informacji powinny obejmować bezpieczeństwo informacji w całej organizacji i nie ograniczać się wyłącznie do ochrony danych osobowych.

Kontrolującym przedstawiono *Rejestr incydentów naruszenia bezpieczeństwa informacji w Urzędzie Miejskim w Moryniu*, który zawierał: dwa wpisy dotyczące 2019 roku, dwa wpisy dotyczące 2021 roku oraz jeden wpis z 2022 roku. Wpisy nie dotyczyły przypadków naruszenia ochrony danych osobowych skutkujący naruszeniem praw lub wolności osób fizycznych, wobec czego nie wystąpiła konieczność zgłoszenia tego faktu organowi nadzorczemu.

(dowód: akta kontroli str. 55, 67-68, 86,170-174)

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:

- Plan sprawdzeń/audytów na rok 2019,
- Plan sprawdzeń/audytów na rok 2020,
- Plan sprawdzeń/audytów na rok 2021,
- Sprawozdanie 1/2019 z przeprowadzonego sprawdzenia (…)
- Sprawozdanie 1/2020 z przeprowadzonego sprawdzenia (…)

Z przedstawionych sprawozdań za lata 2019 i 2020 wynika, że w trakcie przeglądów wykonano *sprawdzenie poprawności zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe.*

W efekcie analizy przedstawionej dokumentacji stwierdzono, że w okresie objętym kontrolą w Urzędzie Miejskim w Moryniu nie przeprowadzono audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 14 rozporządzenia

<table>
<tr><td colspan="2">KRI, wobec czego nie zrealizowano dyspozycji, o której mowa w wyżej przywołanym rozporządzeniu. Nieprzeprowadzanie kompleksowego audytu wewnętrznego w zakresie bezpieczeństwa informacji może wpływać na oceną skuteczności przyjętych w Jednostce rozwiązań w zakresie bezpieczeństwa informacji.
(dowód: akta kontroli str. 146-156, 210)</td></tr>
<tr><td colspan="2">Stwierdzone nieprawidłowości w obszarze nr 2:
Dokumentacja regulująca kwestie bezpieczeństwa informacji, obowiązująca w Urzędzie nie zawiera wszystkich elementów wymaganych przepisami rozporządzenia KRI.
Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi, co nie wypełnia dyspozycji § 21 ust. 2 rozporządzenia KRI.
Zawężenie procedur postępowania z incydentami do przypadków naruszeń ochrony danych osobowych.
Nieprzeprowadzenie audytów wewnętrznych w zakresie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 2 pkt 14 rozporządzenia KRI.</td></tr>
<tr><td>Ocena obszaru kontroli nr 2</td><td>Zakresy opisane w pkt 2.2, 2.3, 2.5-2.7 <u>oceniono pozytywnie</u>.
Zakresy szczegółowo opisane w pkt 2.1, 2.4, 2.8 nieprawidłowości, <u>oceniono pozytywnie z nieprawidłowościami.</u>
Mając natomiast na względzie wagę stwierdzonych nieprawidłowości w obszarze 2.9, polegających na nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, do czego zobowiązują zapisy § 20 ust. 2 pkt 14 rozporządzenia KRI, wskazany zakres <u>oceniono negatywnie</u>.</td></tr>
<tr><td>Wpis do książki kontroli</td><td>Nr 82</td></tr>
<tr><td>Wnioski dotyczące uzyskanych efektów zrealizowanego zadania</td><td>Procedury regulujące kwestie bezpieczeństwa informacji wymagają skorygowania i uzupełnienia, szczególnie w zakresie postępowania w przypadku naruszenia ochrony danych osobowych o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji; jak również o elementy związane z przypisaniem odpowiedzialności za realizowane zadania. Kompleksowa dokumentacja systemu bezpieczeństwa informacji obejmująca obszary działalności Jednostki oraz zapewniająca dostępność, autentyczność, poufność, niezawodność i integralność przetwarzanych danych jest warunkiem niezbędnym skutecznego zarządzania bezpieczeństwem informacji w Jednostce.
Nieprawidłowości polegające na nieprzeprowadzaniu corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji mogą wpłynąć negatywnie na prawidłową oceną skuteczności przyjętych w Jednostce rozwiązań w zakresie bezpieczeństwa informacji. Audyt wewnętrzny stanowi bowiem istotne źródło wiedzy kierownictwa o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz wskazuje obszary wymagające podjęcia działań korygujących. Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi wymaga wdrożenia rozwiązań korygujących, gwarantujących rozliczalność pracy w systemie informatycznym.</td></tr>
</table>

Zalecenia	• uzupełnić dokumentację regulującą kwestie bezpieczeństwa informacji, zgodnie z wymogami § 20 ust. 1 i 2 rozporządzenia KRI, • uzupełnić procedury postępowania z incydentami o pozostałe obszary, w których mogą wystąpić przypadki naruszenia bezpieczeństwa przetwarzanych w Jednostce informacji, stosownie do zapisów § 20 ust. 2 pkt 13 rozporządzenia KRI, • przeprowadzać corocznie audyty wewnętrzne z zakresu bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI, • w dziennikach systemów odnotowywać obligatoryjnie działania użytkowników z uprawnieniami administracyjnymi, zgodnie z zapisami § 21 ust. 2 rozporządzenia KRI.
Pouczenie	– od wystąpienia pokontrolnego nie przysługują środki odwoławcze; – o podjętych działaniach, mających na celu wyeliminowanie stwierdzonych nieprawidłowości, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie 14 dni od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	Wz. Wojewody Zachodniopomorskiego Tomasz Wójcik I Wicewojewoda Zachodniopomorski

.....