WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 9 lutego 2024 r.

Znak: K-2.431.1.53.2023.4.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	Prezydent Miasta Świnoujście, ul. Wojska Polskiego 1/5, 72-600 Świnoujście.
Osoba pełniąca funkcję Prezydenta Miasta Świnoujście w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Janusz Żmurkiewicz
Okres objęty kontrolą	od dnia 1 stycznia 2020 r. do dnia 2 października 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 83/23 z dnia 13 września 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	27 września – 2 października 2023 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoby udzielające wyjaśnień w trakcie kontroli	Pan Wiktor Szymanowski – Kierownik Biura Technologii Informacyjnych, Pani Małgorzata Bielenis - Inspektor Ochrony Danych[3].

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.
[3] Inspektor Ochrony Danych – dalej IOD.

Obszar kontroli Nr 1	Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
1.1 Współpraca systemów teleinformatycznych z innymi systemami	
Podstawa prawna	**§ 5 ust. 3 pkt 3 rozporządzenia KRI[4]:** *Interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.* **§ 16 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*
Ustalenia kontroli Na podstawie przedstawionej dokumentacji ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Miasta Świnoujście wykorzystywano jeden system centralny (aplikacja Źródło) oraz system informatyczny wspomagający obsługę spraw obywatelskich w zakresie ewidencji mieszkańców XXX. Zaprezentowane w czasie kontroli systemy informatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej spełniały minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami zarówno Urzędu, jak i innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. System centralny (aplikacja Źródło), dostępny przez stronę WWW podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu Miasta oraz zabezpieczeń związanych z dostępem do systemu. (dowód: akta kontroli str.39-42)	
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*

[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".

	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 Miasta Świnoujście 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. 31, 407)	
Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1: - nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.	
Ocena obszaru kontroli	**Pozytywna**
Obszar kontroli Nr 2	System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.
2.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu	
Podstawa prawna	**§ 20 ust. 1 rozporządzenia KRI:** *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność działań związanych z bezpieczeństwem informacji.* **§ 20 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.* **§ 20 ust. 3 rozporządzenia KRI:** *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą.*
Ustalenia kontroli Wymagania dotyczące systemów teleinformatycznych, w których przetwarzane są rejestry publiczne w postaci teleinformatycznej określone zostały w § 20 ust. 1 rozporządzenia KRI. Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność,	

integralność informacji.
W Urzędzie Miasta Świnoujście, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie Nr 31/2019 Prezydenta Miasta Świnoujście z dnia 11 stycznia 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta Świnoujście,*
- *Zarządzenie Nr 643/2020 Prezydenta Miasta Świnoujście z dnia 14 października 2020 r. w sprawie wprowadzenie „Regulamin wykorzystywania pracy zdalnej przez pracowników Urzędu Miasta Świnoujście",*
- *Zarządzenie Nr 199/2023 Prezydenta Miasta Świnoujście z dnia 14 kwietnia 2023 r. w sprawie wprowadzenia „Regulamin wykorzystywania pracy zdalnej przez pracowników Urzędu Miasta Świnoujście",*
- *Procedura sprawdzenia wykonywania kopii zapasowych,*
- *DRP – Disaster Recovery Plan. Instrukcja kopii zapasowej i plan odzyskiwania po awarii, wersja 2023-08-23.*

Prezydent Miasta Świnoujście Zarządzeniem Nr 31/2019 wprowadził do stosowania następujące dokumenty, tworzące System Zarządzania Bezpieczeństwem Informacji[5]:

- *Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta Świnoujście,*
- *Instrukcja zarzadzania systemami informatycznymi,*
- *Plan działania w zakresie incydentów w Urzędzie Miasta Świnoujście,*
- *Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektów Urzędu Miasta Świnoujście,*
- *Procedura Auditu Systemu Zarządzania Bezpieczeństwem Informacji.*

W wyniku analizy procedur związanych z bezpieczeństwem informacji stwierdzono, że określono sposób i wskazano osoby realizujące obowiązki wynikające z rozporządzenia KRI, a funkcjonująca w Urzędzie dokumentacja spełnia wymogi określone w § 20 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. Stwierdzono również, że obowiązujące regulacje zostały zaktualizowane 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)[6].

Zgodnie z wyjaśnieniami złożonymi przez Inspektora Ochrony Danych dokumentacja dotycząca bezpieczeństwa informacji podlega okresowym przeglądom. Efektem tych działań są przygotowane i stosowane jako dokument wewnętrzny Jednostki procedury z zakresu wykonywania kopii zapasowych oraz planu odzyskiwania danych po awarii. Powyższe regulacje zostaną zaimplementowane do końca roku kalendarzowego zarządzeniem Prezydenta Świnoujścia jako element dokumentacji SZBI.
Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miasta Świnoujście wdrożono system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

(dowód: akta kontroli str. 61-233, 413)

[5] System Zarządzania Bezpieczeństwem Informacji – dalej SZBI.
[6] Dz. Urz. UE L2016.119, zwane dalej rozporządzeniem RODO.

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 następujące dokumenty dotyczące okresu objętego weryfikacją:

- *Analiza ryzyka, Plan postępowania, Zagrożenia i zabezpieczenia - 2022 r.,*
- *Analiza ryzyka, Plan postępowania, Zagrożenia i zabezpieczenia - 2021 r.,*
- *Analiza Ryzyka Ogólnego i Ocena Skutków dla Przetwarzania Danych (DPIA) Urząd Miasta Świnoujście, data opracowania 31 grudnia 2022 r.,*
- *Analiza Ryzyka Ogólnego i Ocena Skutków dla Przetwarzania Danych (DPIA) Urząd Miasta Świnoujście, data opracowania 30 listopada 2020 r.,*
- *Analiza Ryzyka Ogólnego i Ocena Skutków dla Przetwarzania Danych (DPIA) Urząd Miasta Świnoujście, data opracowania 11 grudnia 2021r.*

Zaprezentowane analizy ryzyka obejmują aktywa Jednostki, a w dokumentach określono zagrożenia dla wskazanych zasobów, źródła tych zagrożeń oraz prawdopodobieństwo i skutki wpływu zdarzeń na czynniki decydujące o bezpieczeństwie informacji. Opracowano również plan postępowania z ryzykiem.

Analiza ryzyka, obejmująca wszystkie aktywa Jednostki oraz odpowiednie i pogłębione szacowanie zidentyfikowanych ryzyk jest jednym z najistotniejszych elementów zarzadzania bezpieczeństwem informacji, pozwalającym na zastosowanie odpowiednich mechanizmów przeciwdziałania w sytuacji materializacji ryzyk. Procedura szacowania ryzyka powinna być przeprowadzana okresowo, jednak zawsze w przypadku pojawienia się nowych zagrożeń, co wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od istotności informacji podlegających ochronie.

Stwierdzono, że wyżej przywołane analizy ryzyka obejmujące zidentyfikowane aktywa Jednostki, wypełniają dyspozycję, o której mowa w § 20 ust. 2 pkt 3 rozporządzenia KRI.

(dowód: akta kontroli str. 234-367)

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 inwentaryzację urządzeń wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej zawierającą informacje dotyczące sprzętu i oprogramowania oraz użytkowanych urządzeń peryferyjnych.
Mając na uwadze powyższe stwierdzono, że w Urzędzie jest prowadzona inwentaryzacja sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str. 399)

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 uprawnień do przetwarzania danych osobowych oraz udzielania dostępu do systemu informatycznego zostały uregulowane w rozdziale 9 *Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta Świnoujście (Zasady udzielania uprawnień do przetwarzania danych pracownikom Urzędu)* oraz w rozdziale 2 *Instrukcji zarzadzania systemami informatycznymi (Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych).* Zgodnie z regulacjami przyjętymi w Jednostce uprawnienia w zakresie dostępu do systemu informatycznego nadaje się na podstawie upoważnienia wydanego przez administratora danych osobowych[7]. Wniosek o wydanie upoważnienia do przetwarzania danych w formie pisemnej składa do ADO przełożony pracownika. Natomiast nadawanie i odbieranie uprawnień dostępu do sieci komputerowej następuje na pisemny wniosek przełożonego pracownika, gdzie wskazuje się systemy i aplikacje, do których pracownik uzyskuje dostęp.
Kontrolującym przedstawiono:

- Wniosek o założenie profilu/ nadanie uprawnień/ modyfikacje uprawnień,
- Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem pracownika o zapoznaniu się z treścią polityki bezpieczeństwa informacji. W dokumencie zawarto między innymi zobowiązanie pracownika do zachowania w tajemnicy przetwarzanych danych. Kontrolujący wskazują, by zaktualizować powyższy dokument, wprowadzając zapisy pod kątem wskazania okresu obowiązywania zobowiązania, rozszerzając go na okres po ustaniu stosunku pracy. Tym bardziej, że w *Polityce Bezpieczeństwa*

[7] Administrator danych osobowych- dalej ADO.

Przetwarzania Danych Osobowych w Urzędzie Miasta Świnoujście, w rozdziale 9 - *Zasady udzielania uprawnień do przetwarzania danych pracownikom Urzędu* widnieje zapis, że *użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia*.

W trakcie kontroli dokonano sprawdzenia odbierania uprawnień dostępu do systemów informatycznych pracownikom, z którymi rozwiązano stosunek pracy. Stwierdzono, że w przypadku jednego pracownika o inicjałach A.S. konto zablokowano po 5 miesiącach. W pozostałych przypadkach nie stwierdzono odstępstw w tym zakresie.

(dowód: akta kontroli str. 79, 106-107, 379-386)

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 Miasta Świnoujście przeprowadzano następujące szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych, w kontekście obowiązujących aktów prawnych – rozporządzenia KRI oraz RODO:

- Szkolenie z cyberbezpieczeństwa (2022 r., 2023 r.),
- Szkolenie z zakresu realizacji obowiązku informacyjnego oraz retencji danych w BIP (2022 r.),
- Szkolenie z zakresu podpisu elektronicznego (2021 r.).

Ponadto, zgodnie z wyjaśnieniami Kierownika Biura Technologii Informacyjnych na stronie miasta, na bieżąco udostępniane są informacje o występujących zagrożeniach dotyczących bezpieczeństwa informacji.

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 przedstawionej dokumentacji oraz wyjaśnień IOD wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 377, 387-397)

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 uregulowane w następujących procedurach wewnętrznych Urzędu:

- *Polityce Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta Świnoujście*, stanowiącej załącznik nr 1 do *Zarządzenia Nr 31/2019 Prezydenta Miasta Świnoujście z dnia 11 stycznia 2019 r., w rozdziale 34 - Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe poza siedzibą Urzędu,*
- załączniku nr 3 do *Regulaminu wykorzystywania pracy zdalnej przez pracowników Urzędu Miasta Świnoujście, wprowadzonego Zarządzeniem Nr 199/2023 Prezydenta Miasta Świnoujście z dnia 14 kwietnia 2023 r. – Zasady korzystania z urządzeń technicznych w związku z pracą zdalną,*
- załączniku nr 4 do *Regulaminu wykorzystywania pracy zdalnej przez pracowników Urzędu Miasta Świnoujście, wprowadzonego Zarządzeniem Nr 199/2023 Prezydenta Miasta Świnoujście z dnia 14 kwietnia 2023 r. – Procedura ochrony danych osobowych przetwarzanych w ramach pracy zdalnej.*

Zgodnie z wyjaśnieniami IOD do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie nie wykorzystywano urządzeń mobilnych i nie realizowano pracy na odległość.

(dowód: akta kontroli str. 95-96, 122-185, 182-190, 415)

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 pracowników zatrudnionych w Biurze Technologii Informacyjnych, w Urzędzie Miasta Świnoujście.

W celu realizacji zadań z zakresu administracji rządowej z firmą XXX zawarto umowę serwisową systemu XXX[8]. W umowie wprowadzono zapisy dotyczące poziomu dostępności oferowanych usług oraz sposobu dostarczania ich na zadeklarowanym poziomie, określono maksymalny czas skutecznej naprawy oprogramowania, zdefiniowano grupy błędów i maksymalny czas ich usunięcia. Z firmą zawarto również *Umowę powierzenia przetwarzania danych osobowych*[9], co przekłada się na realizację dyspozycji § 20 ust. 2 pkt 10 rozporządzenia KRI w zakresie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

(dowód: akta kontroli str. 400-406, 409-412)

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 Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Świnoujście* wprowadzonej *Zarządzeniem Nr 31/2019 Prezydenta Miasta Świnoujście z dnia 11 stycznia*

[8] Umowa BTI.271.2.4.2023 z 3 stycznia 2023 r.

[9] Umowa z dnia 3 stycznia 2023 r.

2019 r., w § 27 określono pojęcie incydentu bezpieczeństwa, natomiast w załączniku nr 3 do wyżej wymienionego zarządzenia *Plan działania w zakresie incydentów w Urzędzie Miasta Świnoujście* określono zasady i sposób postępowania w przypadku naruszenia bezpieczeństwa informacji. Ponadto w procedurze postępowania w sytuacji wystąpienia incydentów, w przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji przypisano odpowiednie zadania pracownikom Urzędu oraz IOD.
Kontrolującym przedstawiono *Rejestr incydentów bezpieczeństwa teleinformatycznego,* w którym odnotowano cztery zdarzenia W przypadku dwóch wpisów kotrolujący zwrócili się o dodatkowe informacje. IOD wyjaśnił, że we wskazanych przypadkach, po przeprowadzeniu analizy ryzyka zdarzenia zostały zaklasyfikowane jako naruszenie niskiego stopnia nie skutkujące koniecznością zgłoszenia tego faktu organowi nadzorczemu. W przypadku powyższych wpisów kontrolujący przyjęli wyjaśnienia. (dowód: akta kontroli str. 92, 130 -138, 398, 414)

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.
Kwestie celów, zasad i sposobu przeprowadzania audytów wewnętrznych z zakresu bezpieczeństwa informacji uregulowano w postaci *Procedury Auditu Systemu Zarządzania Bezpieczeństwem Informacji,* stanowiącej załącznik nr 5 do *Zarządzenia Nr 31/2019 Prezydenta Miasta Świnoujście z dnia 11 stycznia 2019 r.*
Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- Raport z audytu bezpieczeństwa informacji w Urzędzie Miasta Świnoujście, data dokumentu 31 grudnia 2022r.
- Raport z audytu bezpieczeństwa informacji w Urzędzie Miasta Świnoujście, data dokumentu 11 grudnia 2021r.
- Raport z audytu bezpieczeństwa informacji w Urzędzie Miasta Świnoujście, data dokumentu 30 listopada 2020r.

Audyty wewnętrzne realizowane w Jednostce, w latach 2020 - 2022 obejmowały swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego w tym okresie spełniono wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.
(dowód: akta kontroli str. 152-160, 368-376)

2.10 Kopie zapasowe

Podstawa prawna	**§ 20 ust. 2 pkt 12 lit. b, e rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych.*

Ustalenia kontroli

Zgodnie z wymogami określonymi w § 20 ust. 2 pkt 12 lit. b) i e) rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.

Zasady tworzenia kopii zapasowych zbiorów danych oraz programów uregulowane zostały w Procedurze tworzenia kopii zapasowych danych, w rozdziale 5 *Instrukcji Zarządzania Systemami i Sprzętem Informatycznym w Urzędzie Miasta Świnoujście*. Kwestie przechowywania i testowania kopii bezpieczeństwa unormowano w *Procedurze sprawdzenia wykonywania kopii zapasowych* oraz dokumencie *DRP – Disaster Recovery Plan. Instrukcja kopii zapasowej i plan odzyskiwania po awarii.*

Treść zasadnicza danych tworzonych w Jednostce przechowywana jest w serwerowni. Podstawowa, codzienna kopia zapasowa gromadzona jest w innym pomieszczeniu. Zapisane taśmy z systemu wykorzystywanego do tworzenia kopii zapasowych przechowywane są w pomieszczeniu innym niż serwerownia i innym niż podstawowa codzienna kopia zapasowa. Ponadto w Jednostce wykonywana jest codzienna szyfrowana kopia zapasowa najcenniejszych plików i automatycznie przesyłana na odmiejscowiony serwer. Z wyjaśnień Kierownika Biura Technologii Informacyjnych wynika, że realizowane jest próbne testowanie kopii zapasowych, oraz dodatkowych kopii zapasowych w celu sprawdzenia poprawności ich wykonania. Z powyższych czynności sporządzane są protokoły.

Mając na uwadze powyższe stwierdzono, że w Urzędzie wypełniono w pełni dyspozycję § 20 ust. 2 pkt 12 lit. b, e rozporządzenia KRI.

(dowód: akta kontroli str. 111-112, 201-235, 377-378)

2.11 Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Podstawa prawna	**§ 15 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.*

Ustalenia kontroli

W celu wykonywania zadań z zakresu administracji rządowej z firmą XXX zawarto umowę serwisową systemu XXX.

(dowód: akta kontroli str. 400-406)

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 4 stanowisk komputerowych wykorzystywanych do realizujących zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że: - na każdym urządzeniu dostęp do systemu operacyjnego możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła, - komputery miały zainstalowane oprogramowanie antywirusowe, - na wszystkich jednostkach skonfigurowano wygaszacz ekranu, - złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych, - ustawienie monitora stanowiska obsługi systemów informatycznych uniemożliwia odczyt wyświetlanych danych przez osoby postronne, - żadnemu z użytkowników nie nadano uprawnień administratora uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń. Pomieszczenie serwerowni właściwie wyposażone i zabezpieczone. Dostęp osób do serwerowi jest ograniczony do upoważnionych osób, przy czym fakt wejścia jest odnotowywany poprzez elektroniczną rejestrację wejść na podstawie karty ID (osobistego identyfikatora). (dowód: akta kontroli str. 416-417)	
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 Sieci i systemy Urzędu zabezpieczono przy wykorzystaniu zapory sieciowej firewall XXX. W Urzędzie przeprowadzany jest w czasie rzeczywistym monitoring pracy sieci i serwerów, a doraźnie przeprowadza się monitoring podatności w systemach informatycznych. Poczta elektroniczna weryfikowana jest pod kątem wiarygodności nadawcy. XXX. W Urzędzie używane jest oprogramowanie XXX pozwalające między innymi na centralne aktualizacje, instalowanie i odinstalowywanie programów. Ponadto stosuje się szyfrowanie dysków przenośnych komputerów i wszystkich przenośnych nośników. (dowód: akta kontroli str. 377-378)	
2.14 Rozliczalność działań w systemach teleinformatycznych.	
Podstawa prawna	**§ 21 ust. 2 rozporządzenia KRI:** *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.* **§ 21 ust. 3 rozporządzenia KRI:** *w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.* **§ 21 ust. 4 rozporządzenia KRI:** *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*
Ustalenia kontroli Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych). Systemy objęte kontrolą zawierają logi, w których są odnotowanie działania użytkowników zgodnie z zapisami § 21 ust. 2 i 3 rozporządzenia KRI. Logi systemów są przechowywane przez okres ponad 2 lat, wobec czego wypełniono dyspozycję § 21 ust. 4 wyżej opisanego rozporządzenia. Ponadto wykonywana jest analiza logów, w celu identyfikacji działań niepożądanych.	

Kontrolujący wysoko oceniają kompetencje, profesjonalizm i zaangażowanie Kierownika Biura Technologii Informacyjnych Pana Wiktora Szymanowskiego oraz wdrożone przez pracowników Biura Technologii Informacyjnych rozwiązania organizacyjne i techniczne, mające na celu odpowiednie zabezpieczenie użytkowanych systemów informatycznych, szczególnie w obszarze przetwarzanych w Jednostce danych. **Stwierdzone uchybienie w obszarze nr 2:** • Niezachowanie wymogu bezzwłocznego odebrania uprawnień w systemach informatycznych jednemu pracownikowi, z którym rozwiązano stosunek pracy; zgodnie z dyspozycją § 20 ust. 2 pkt 5 rozporządzenia KRI.	
Ocena obszaru kontroli	**Pozytywna z uchybieniem**
Wpis do książki kontroli	Nr 56
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	Ważną kwestią z punktu widzenia bezpieczeństwa informacji jest ciągłe podnoszenie świadomości pracowników (poprzez realizację różnych formy szkoleń) istnienia potencjalnych zagrożeń oraz wiedza w jaki sposób unikać, zminimalizować ale także postępować w przypadku materializacji ryzyk związanych z naruszeniem bezpieczeństwa wszystkich przetwarzanych przez Jednostkę informacji (ze szczególnym uwzględnieniem naruszenia ochrony danych osobowych). Istotne jest podejmowanie działań dotyczących bezzwłocznego blokowanie dostępu do systemów informatycznych osobom pozbawionym uprawnień.
Zalecenie	• Bezzwłocznie odbierać uprawnienia w systemach informatycznych pracownikom, z którymi rozwiązano stosunek pracy, do czego zobowiązuje zapis § 20 ust. 2 pkt 5 rozporządzenia KRI
Pouczenie	– od wystąpienia pokontrolnego nie przysługują środki odwoławcze; – o podjętych działaniach, mających na celu wyeliminowanie stwierdzonych nieprawidłowości, proszę poinformować mnie za pośrednictwem Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie w terminie 14 dni od daty otrzymania niniejszego wystąpienia.
Podpis kierownika jednostki kontrolującej	z upoważnienia Wojewody Zachodniopomorskiego Bartosz Brożyński I Wicewojewoda Zachodniopomorski