WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 13 sierpnia 2024 r.

Znak: K-2.431.1.21.2024.7.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	Burmistrz Dobrzan, ul. Staszica 1, 73-130 Dobrzany.
Osoba pełniąca funkcję Burmistrza Dobrzan w okresie objętym kontrolą	Pan Paweł Filip
Okres objęty kontrolą	od dnia 1 stycznia 2021 r. do dnia 13 maja 2024 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego,* Pani Iwona Olesińska – główny specjalista.
Nr upoważnienia	Nr 29/24 z dnia 26 kwietnia 2024 r.
Podstawy prawne do przeprowadzenia kontroli	– art. 6 ust. 4 pkt 3 w związku z art. 2 ust. 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1]; – art. 25 ust. 1 pkt 3 lit. a, w związku z ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2].
Kryteria prowadzenia kontroli	legalność, rzetelność
Termin kontroli	7-13 maja 2024 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Damian Szmidt – Inspektor Ochrony Danych, na mocy umowy zajmujący się obsługą informatyczną Urzędu[3].

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2023r., poz. 57.
[3] W zakresie dotyczącym obsługi informatycznej zwany dalej Informatykiem.

Obszar kontroli Nr 1	Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
1.1 Współpraca systemów teleinformatycznych z innymi systemami	
Podstawa prawna	**§ 5 ust. 3 pkt 3 rozporządzenia KRI** zwane dalej „rozporządzeniem 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 Miejskim w Dobrzanach wykorzystywano system centralny (aplikacja Źródło) oraz system informatyczny wspomagający obsługę spraw obywatelskich w zakresie rejestru mieszkańców XXX. System informatyczny wspomagający realizację zadań zleconych z zakresu administracji rządowej, spełniał minimalne wymogi interoperacyjności w zakresie współpracy z innymi aplikacjami Urzędu, jak i innych jednostek administracji publicznej, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI. System centralny podlegał kontroli jedynie w zakresie formalnego posiadania uprawnień przez pracowników Urzędu oraz zabezpieczeń związanych z dostępem do systemu. (dowód: akta kontroli str. 34, 64-67)	
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*

[4] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773). Numeracja paragrafów została dostosowana do zmian obowiązującego do 22 maja 2024 r. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247), wprowadzonych wyżej opisanym aktem prawnym z dnia 21 maja 2024 r.

	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 Dobrzanach wymieniał dane w formatach określonych w § 18 ust. 1 rozporządzenia KRI o udostępnianiu zasobów informacyjnych w co najmniej w jednym z formatów wymienionych w załączniku nr 2 do rozporządzenia.	
Stwierdzone uchybienia / nieprawidłowości w obszarze Nr 1: - nie stwierdzono uchybień oraz nieprawidłowości skutkujących naruszeniem przepisów.	
Ocena obszaru kontroli	**Pozytywna**
Obszar kontroli Nr 2	System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.
2.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu	
Podstawa prawna	**§ 19 ust. 1 rozporządzenia KRI:** *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.* **§ 19 ust. 2 pkt 1 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.* **§ 19 ust. 3 rozporządzenia KRI:** *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą.*
Ustalenia kontroli Wymagania dotyczące systemów teleinformatycznych, w których przetwarzane są rejestry publiczne w postaci teleinformatycznej określone zostały w § 19 ust. 1 rozporządzenia KRI. Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność, integralność informacji.	

W Urzędzie Miejskim w Dobrzanach, w okresie objętym kontrolą obowiązywały następujące dokumenty z zakresu bezpieczeństwa informacji:

- *Zarządzenie nr 93/2019 Burmistrza Dobrzan z dnia 13.09.2019 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Dobrzanach,*
- *Zarządzenie nr 26/2023 Burmistrza Dobrzan z dnia 10 marca 2023 r. zmieniające zarządzenie w sprawie Systemu Zarzadzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Dobrzanach,*
- *Zarządzenie nr 55/2024 Burmistrza Dobrzan z dnia 10 maja 2024 r. w sprawie zmiany zarządzenia nr 26/2023 Burmistrza Dobrzan z dnia 10 marca 2023 r. zmieniające zarządzenie w sprawie Systemu Zarzadzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Dobrzanach.*

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 § 19 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)[5]. Dyrektywa § 19 ust. 2 pkt 1 rozporządzenia KRI wskazuje na konieczność *zapewnienia aktualizacji regulacji wewnętrznych (...)*. Powyższy wymóg uznaje się za spełniony, czego dowodem są zapisy dokumentujące powyższe czynności w Rejestrze zmian w PBI[6].

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Miejskim w Dobrzanach wdrożono system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji.

(dowód: akta kontroli str. 94-276)

2.2 Analiza zagrożeń związanych z przetwarzaniem informacji

Podstawa prawna	**§ 19 ust. 2 pkt 3 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

Ustalenia kontroli

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

Metodykę przeprowadzania analizy ryzyka ujęto w dokumencie *Instrukcja przeprowadzenia analizy ryzyka w Urzędzie Gminy w Dobrzanach, wersja 1.1.*

Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- Raport z przeprowadzonej analizy ryzyka w Urzędzie Gminy w Dobrzanach, Dobrzany 2022.

[5] Dz. Urz. UE L2016.119, zwane dalej rozporządzeniem RODO.
[6] PBI - Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach.

- Raport z przeprowadzonej analizy ryzyka w Urzędzie Gminy w Dobrzanach, Dobrzany 2023.

Kontrolujący uznają za oczywistą pomyłkę pisarską określenie *Urząd Gminy w Dobrzanach* użyte w tytułach i treści okazanych dokumentów.
Zaprezentowane analizy ryzyka obejmują aktywa Jednostki. W dokumentach określono zagrożenia dla wskazanych zasobów, źródła tych zagrożeń oraz prawdopodobieństwo i skutki wpływu zdarzeń na czynniki decydujące o bezpieczeństwie informacji. Raporty zawierają również plany postępowania z ryzykiem.
Stwierdzono, że wyżej przywołane analizy ryzyka obejmujące zidentyfikowane aktywa Jednostki, wypełniają dyspozycję, o której mowa w § 19 ust. 2 pkt 3 rozporządzenia KRI
(dowód: akta kontroli str. 70, 147-188, 277-283)

2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego

Podstawa prawna	**§ 19 ust. 2 pkt 2 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

Ustalenia kontroli
Zgodne z § 19 ust. 2 pkt 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ponadto, zgodnie z pkt 8.1.1 normy PN-ISO/IEC 27002:2014, wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis. Inwentaryzacja m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie jego odtworzenie po katastrofie lub innym zdarzeniu losowym.
Kontrolującym przedstawiono karty raportów inwentaryzacji dla sprzętu komputerowego użytkowanego w Urzędzie oraz ewidencję sprzętu i urządzeń peryferyjnych (w postaci arkusza kalkulacyjnego). Dokumenty zawierały między innymi informacje o rodzaju użytkowanego w Jednostce sprzętu (nazwie i jego charakterystyce), nazwie oraz wersji systemu operacyjnego, nazwie procesora, zainstalowanego oprogramowania, pojemności pamięci oraz współpracujących urządzeniach peryferyjnych. Okazane formularze potwierdzają prowadzenie w Urzędzie inwentaryzacji sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych

Podstawa prawna	**§ 19 ust. 2 pkt 4 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.* **§ 19 ust. 2 pkt 5 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Ustalenia kontroli
Przepisy § 19 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI stanowią m.in, że kierownictwo podmiotu publicznego w celu zapewnienia bezpieczeństwa informacji powinno podjąć działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne

uprawnienia, adekwatne do realizowanych zadań, a także podjąć bezzwłoczne działania w przypadku zmiany zadań tych osób. Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby, w ustalonym zakresie.
Kwestie nadawania i odbierania uprawnień do pracy w systemie informatycznym uregulowano w następujących dokumentach:

- *Polityce Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach*, w rozdziale 10 - Kontrola dostępu (Wymagania wobec kontroli dostępu, Zarządzanie dostępem użytkowników);
- *Polityce Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach Procedury eksploatacyjne*, stanowiącej załącznik nr 6 do *Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach,* w rozdziale 6 - Zarządzanie uprawnieniami;
- *Polityce Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach w obszarze bezpieczeństwa zasobów ludzkich*, stanowiącej załącznik nr 4 do *Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach.*

Zgodnie z zapisami procedur użytkownicy otrzymują dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie Administratora Danych Osobowych, po wcześniejszym złożeniu stosownego wniosku. Nadawanie uprawnień dostępu realizowane jest na podstawie formalnych dokumentów, przy czym wprowadzono zasadę rozdzielenia ról związanych z wnioskowaniem, autoryzacją, zarządzaniem i kontrolą nadawania uprawnień. Ponadto nałożono wymóg okresowego (nie rzadziej niż raz w roku) przeglądu nadanych uprawnień.

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 w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia* złożone przez pracowników realizujących zadania zlecone z zakresu administracji rządowej. W dokumencie wskazano okres obowiązywania zobowiązania zarówno w trakcie zatrudnienia, jak również po ustaniu stosunku pracy;
- *wniosek o nadanie/modyfikację/wyrejestrowanie uprawnień użytkownika w systemie informatycznym.* Przedstawione dokumenty potwierdzają nadanie oraz modyfikację uprawnień użytkowników w systemie podlegającym kontroli.
  Pisemny wniosek dotyczący nadawania oraz modyfikowania uprawnień, podpisany przez osoby upoważnione powoduje, że proces nadawania i odbierania uprawnień jest w pełni potwierdzony.

Z uwagi na fakt, że w okresie podlegającym badaniu, nie wystąpiły przypadki cofania uprawnień nadanych pracownikom realizującym zadania zlecone z zakresu administracji rządowej, nie dokonano sprawdzenia blokowania dostępu do systemów informatycznych.

(dowód: akta kontroli str. 68-69, 123, 218-221, 368-374)

2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Podstawa prawna	**§ 19 ust. 2 pkt 6 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*

Ustalenia kontroli

W okresie objętym kontrolą w Urzędzie Miejskim w Dobrzanach przeprowadzono następujące szkolenia pracowników z zakresu bezpieczeństwa informacji i ochrony danych osobowych:

- *Szkolenie wewnętrzne pracowników Urzędu Gminy w Dobrzanach w dniu 13 października 2021 r.;*
- *Szkolenie wewnętrzne pracowników Urzędu Gminy w Dobrzanach w dniu24 maja 2022 r.;*
- *Szkolenie wewnętrzne pracowników Urzędu Gminy w Dobrzanach w dniu 31 maja 2023 r.*

Udział w szkoleniach dokumentowała lista obecności zawierająca imię i nazwisko uczestnika oraz własnoręczny podpis. Stwierdzono, że w przeprowadzonych szkoleniach wzięli udział pracownicy wskazani jako osoby realizujące zadania zlecone z zakresu administracji rządowej.

Z przedstawionej dokumentacji wynika, że zakres tematyczny szkoleń przeprowadzonych w Urzędzie obejmował zagadnienia wskazane w § 19 ust. 2 pkt 6 rozporządzenia KRI.

Kontrolujący uznają za oczywistą pomyłkę pisarską określenie *Urząd Gminy w Dobrzanach* użyte w treści dokumentów, potwierdzających przeprowadzenie powyżej opisanych szkoleń.

(dowód: akta kontroli str. 348-356)

2.6 Praca na odległość i mobilne przetwarzanie danych

Podstawa prawna	**§ 19 ust. 2 pkt 8 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Ustalenia kontroli

Kwestie trybu prowadzenia pracy zdalnej zostały uregulowane w *Procedurze bezpieczeństwa informacji i ochrony danych osobowych podczas wykonywania okazjonalnej pracy zdalnej w Urzędzie Miejskim w Dobrzanach, wersja 1.0*, wprowadzonej *Zarządzeniem Nr 55/2024 Burmistrza Dobrzan z dnia 10 maja 2024 r.* Zasady bezpiecznego korzystania z urządzeń przenośnych określono w załączniku nr 6 (rozdziale 5 i 9) do *Polityki Bezpieczeństwa Informacji.*

W wyżej wymienionych dokumentach ustalono zasady wynoszenia poza obszar organizacji nośników z danymi osobowymi, wprowadzając wymóg uzyskania zgody Administratora Danych Osobowych. Wdrożono obowiązek szyfrowania danych zapisanych na komputerach przenośnych oraz innych urządzeniach mobilnych, a także wymóg zabezpieczenia hasłem użytkowanych laptopów.

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

(dowód: akta kontroli str. 189-196, 234-235, 374)

2.7 Serwis sprzętu informatycznego i oprogramowania

Podstawa prawna	**§ 19 ust. 2 pkt 10 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

Ustalenia kontroli

Obsługa informatyczna Urzędu realizowana jest na podstawie umowy o świadczenie usług w zakresie obsługi informatycznej XXX[7]. Obsługa informatyczna obejmuje między innymi następujące czynności: konfigurację sprzętu komputerowego; konfigurację i administrowanie systemami operacyjnymi; instalację sprzętu i oprogramowania; wykonywanie kopii baz danych;

[7] Umowa Nr 117/2023, z dnia 27 grudnia 2023 r.

pełnienie funkcji administratora systemu informatycznego; nadzór i konserwację sieci LAN; opracowanie i aktualizację dokumentacji bezpieczeństwa systemu teleinformatycznego; szkolenia pracowników z zakresu procedur bezpiecznej eksploatacji systemów informatycznych; kontrolowanie funkcjonowania mechanizmów zabezpieczeń systemów użytkowanych w Jednostce. W powyższej umowie nie uregulowano kwestii czasu reakcji na zgłoszenie związane z np. awarią sieci komputerowej, sprzętu lub oprogramowania. Z XXX zawarto umowę powierzenia przetwarzania danych osobowych.[8]

W celu realizacji zadań z zakresu administracji rządowej XXX zawarto umowę serwisową, której przedmiotem jest *nadzór serwisowy nad Programem XXX*[9]. W umowie nie ujęto zapisów określających maksymalny czas skutecznej naprawy oprogramowania, powyższym nie wypełniono dyspozycji § 19 ust. 2 pkt 10 rozporządzenia KRI, zawierającego zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

(dowód: akta kontroli str. 357-367)

2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Podstawa prawna	**§ 19 ust. 2 pkt 13 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Ustalenia kontroli

Kwestie zgłaszania incydentów naruszenia bezpieczeństwa informacji uregulowano w następujących dokumentach:

- *Polityce Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach*, w rozdziale 12 - Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- *Polityce Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach Procedury eksploatacyjne*, stanowiącej załącznik nr 6 do *Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach,* w rozdziale 13 - Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych oraz rozdziale 14 - Obowiązek zachowania poufności i ochrony danych osobowych.

W procedurach określono zasady i sposób postępowania w przypadku naruszenia bezpieczeństwa informacji, wskazując jednocześnie katalog zdarzeń, które mogą sygnalizować wystąpienie naruszenia danych. Ponadto instrukcje postępowania w sytuacji wystąpienia incydentów przypisują odpowiednie zadania IOD[10], ADO[11] oraz ASI[12] w przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji.

Kontrolującym przedstawiono *Rejestr incydentów bezpieczeństwa informacji*, w którym odnotowano pięć zdarzeń oraz *Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych naruszeniu ochrony danych osobowych* , w którym odnotowano dwa zdarzenia. W przypadku jednego wpisu, zaewidencjonowanego w rejestrze jako *zagubienie nośnika danych pendrive* kontrolujący przyjęli wyjaśnienia, że we wskazanej sytuacji nie nastąpiło naruszenie ochrony danych osobowych, skutkujące koniecznością zgłoszenia tego faktu organowi nadzorczemu.

(dowód: akta kontroli str. 132, 238, 343-347, 375)

[8] Umowa powierzenia przetwarzania danych osobowych w związku z usługami informatycznymi stanowiąca uzupełnienie umowy nr 117/2023 z dnia 27.12.2023 r.
[9] Umowa serwisowa nr M037/2024 z dnia 21 grudnia 2023 r.
[10] Inspektor Ochrony Danych
[11] Administrator Danych Osobowych
[12] Administrator Systemów Informatycznych

2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji	
Podstawa prawna	**§ 19 ust. 2 pkt 14 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

Ustalenia kontroli

W myśl § 19 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Kontrolującym przedstawiono następujące dokumenty dotyczące okresu objętego weryfikacją:

- *Raport z audytu bezpieczeństwa informacji w Urzędzie Gminy Dobrzany*, data opracowania: 20 grudnia 2021 r.,
- *Raport z przeprowadzonej diagnozy cyberbezpieczeństwa w Urzędzie Miejskim w Dobrzanach z ramach realizacji projektu grantowego „Cyfrowa gmina*", data opracowania: 23 maja 2022 r.,
- *Raport z audytu bezpieczeństwa informacji w Urzędzie Gminy w Dobrzanach*, Dobrzany 2023.

Kontrolujący uznają za oczywistą pomyłkę pisarską określenie *Urząd Gminy w Dobrzanach* użyte w tytule dokumentu z 2021 oraz w tytule i treści dokumentu z 2023 r.

Funkcję IOD i ASI pełni w Urzędzie Miejskim w Dobrzanach ta sama osoba. Ponadto ta sama osoba w 2021 i 2023 roku przeprowadziła na zlecenie Burmistrza Dobrzan okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji.

Konsolidacja funkcji IOD z funkcją ASI może powodować zagrożenia dla bezpieczeństwa przetwarzania danych osobowych. Osoba odpowiadająca za bieżące prowadzenie przetwarzania danych osobowych i bezpieczeństwo danych w systemach informatycznych sprawuje jednocześnie nadzór nad zgodnością z prawem wykonywanych przez siebie działań. Sytuacja taka wzbudza obawy o brak skutecznego nadzoru nad zgodnością przetwarzania danych z przepisami prawa, w tym przepisami określającymi wymogi co do bezpieczeństwa danych osobowych.

Kolejnym dylematem jest sporządzenie audytu wewnętrznego przez osobę pełniącą funkcję IOD i ASI. Problem stanowi ta część audytu, w której Inspektor Ochrony Danych przeprowadzający audyt powinien zweryfikować swoje własne kompetencje i działania, zgodnie z wymaganiami RODO oraz przeprowadzający audyt, pełniący również funkcję ASI weryfikuje własne działania pod kątem zgodności z wymogami rozporządzenia KRI. W tym zakresie najlepszym rozwiązaniem jest wyznaczenie innego audytora, np. innej osoby z organizacji lub podmiotu zewnętrznego. Audytor wewnętrzny powinien powstrzymać się bowiem od oceny działalności operacyjnej, za którą jest odpowiedzialny, ze względu na ograniczenie obiektywizmu w ocenie tych działań.

(dowód: akta kontroli str. 71-84, 284-336)

2.10 Kopie zapasowe	
Podstawa prawna	**§ 19 ust. 2 pkt 12 lit. b, e rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych.*

Ustalenia kontroli

Zgodnie z wymogami określonymi w § 19 ust. 2 pkt 12 lit. b) i e) rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in.

odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych. Zasady wykonywania kopii bezpieczeństwa oraz kwestie ich testowania uregulowano w *Polityce Bezpieczeństwa Informacji w Urzędzie Miejskim w Dobrzanach,* rozdziale 9 - Zarządzanie systemami i sieciami (Kopie zapasowe). Kopie zapasowe baz danych, zgodnie z oświadczeniem Informatyka z dnia 10 maja 2024 r. wykonywane są przy użyciu systemu pamięci masowej z dyskami twardymi oraz komputera, zlokalizowanego poza miejscem wytworzenia kopii. Dwa razy w tygodniu na płyty DVD tworzone są kopie zapasowe z programu uznanego za najistotniejszy dla funkcjonowania Urzędu. Płyty DVD są przechowywane poza serwerownią. Kopie zapasowe z komputera, który jest wykorzystywany do pracy w systemie Źródło oraz programie XXX wykonywane są na dysk zewnętrzy USB. W Urzędzie realizowane jest próbne testowane kopii zapasowych na potrzeby weryfikacji poprawności i stanu ich wykonywania. Kontrolującym przedstawiono *Protokoły z odtwarzania kopii zapasowych*, dokumentujące te czynności. (dowód: akta kontroli str. 117, 377-388)	
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 serwisową, której przedmiotem jest nadzór serwisowy nad Programem XXX. W procedurach wewnętrznych uregulowano zasady projektowania i rozwoju systemów informatycznych, wdrażania nowych wersji użytkowanego oprogramowania, działania związane z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności. (dowód: akta kontroli str. 357-362)	
2.12 Zabezpieczenia techniczno – organizacyjne dostępu do informacji	
Podstawa prawna	**§ 19 ust. 2 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:* **pkt 7:** *zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;* **pkt 9:** *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;* **pkt 11:** *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

Ustalenia kontroli

W celu ustanowienia zabezpieczeń uniemożliwiających osobom nieuprawnionym modyfikację, usunięcie lub zniszczenie informacji każdemu pracownikowi nadano identyfikator i hasło wejścia do systemów zainstalowanych na komputerach oraz do programów, z których korzystają. W przypadku systemu „Źródło" dostęp jest możliwy wyłącznie z użyciem karty, na której zapisany jest certyfikat umożliwiający zalogowanie się do centralnego systemu.

Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych.

W wyniku oględzin stanowiska komputerowego wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonych w toku czynności kontrolnych ustalono, że:

- dostęp do systemu operacyjnego na urządzeniu możliwy był jedynie po wprowadzeniu nazwy użytkownika i hasła,
- komputer miał zainstalowane oprogramowanie antywirusowe oraz skonfigurowany wygaszacz ekranu,
- złożoność hasła była zgodna z wymogami rozporządzenia w sprawie dokumentacji i warunków technicznych,
- ustawienie monitora stanowiska obsługi systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej uniemożliwiało odczyt wyświetlanych danych przez osoby postronne,
- użytkownikom systemów wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej nie nadano uprawnień administratora, uniemożliwiając w ten sposób instalowanie oprogramowania niewiadomego pochodzenia lub zmianę ustawień systemu operacyjnego a także ingerencję w rejestry zdarzeń.

Serwerownię wyposażono w okienną roletę antywłamaniową i gaśnicę. W pomieszczeniu brak czujki dymu, a wejście do serwerowni nie dysponuje należytymi zabezpieczeniami.

Polityka Bezpieczeństwa Informacji Urzędu Miejskiego w Dobrzanach w obszarze bezpieczeństwa fizycznego i środowiskowego, w rozdziale 3 (Bezpieczeństwo środków przetwarzania informacji, podrozdział 1 Lokalizacja i ochrona środków przetwarzania informacji**)** reguluje sposób organizowania w serwerowni wizyt osób spoza Urzędu. Zgodnie z zapisami procedury wizytę osób spoza Jednostki należy odnotować, wpisując dane identyfikacyjne osoby, a także datę oraz godziny wejścia i wyjścia. Zgodnie z wyjaśnieniami Informatyka w Urzędzie nie jest prowadzony rejestr, o którym mowa w przywołanej powyżej procedurze.

(dowód: akta kontroli str. 85-93, 224-225)

2.13 Zabezpieczenia techniczno – organizacyjne systemów informatycznych

Podstawa prawna	**§ 19 ust. 2 pkt 12 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie (...) odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.*

	§ 19 ust. 4 rozporządzenia KRI: *Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*
Ustalenia kontroli • Sieć informatyczną Urzędu zabezpieczono XXX. • Urządzenia informatyczne Jednostki są podłączone do zasilacza awaryjnego UPS. • Na komputerze podlegającym badaniu zainstalowano oprogramowanie antywirusowe. • Systemy Windows zarządzane są przy użyciu programu XXX. • XXX. • W procedurach wewnętrznych Jednostki określono zasady: - przesyłania danych poza obszar przetwarzania, - bezpiecznej wymiany informacji poprzez zastosowanie między innymi ochrony kryptograficznej, - naprawy urządzeń komputerowych, - niszczenia elektronicznych nośników informacji. (dowód: akta kontroli str. 389)	
2.14 Rozliczalność działań w systemach teleinformatycznych	
Podstawa prawna	**§ 20 ust. 2 rozporządzenia KRI:** *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.* **§ 20 ust. 3 rozporządzenia KRI:** *Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.* **§ 20 ust. 4 rozporządzenia KRI:** *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*
Ustalenia kontroli Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy) w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie teleinformatycznym. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszelkie działania dostępu do systemu teleinformatycznego z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i jego zabezpieczeń a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych). Kontrolującym nie przedstawiono logów z programu XXX. Zgodnie z wyjaśnieniami Informatyka system objęty kontrolą *nie zapisywał logów systemowych, opcja jest domyślnie wyłączona przez firmę XXX ze względu na zbyt szybko przyrastający rozmiar bazy.* Program objęty kontrolą winien zawierać logi, w których są odnotowane działania użytkowników, zgodnie z zapisami § 20 ust. 2 rozporządzenia KRI. Ponadto logi systemu winny być	

przechowywane przez okres 2 lat. Wobec powyżej opisanych okoliczności należy stwierdzić, że w tym zakresie nie wypełniono dyspozycji § 20 ust. 2 i 4 rozporządzenia KRI.

(dowód: akta kontroli str. 376)

Stwierdzone nieprawidłowości w obszarze nr 2:

- W umowie serwisowej XXX oraz w umowie o świadczenie usług w zakresie obsługi informatycznej XXX brak zapisów określających maksymalny czas skutecznej naprawy sprzętu lub oprogramowania, czym nie wypełniono dyspozycji § 19 ust. 2 pkt 10 rozporządzenia KRI.
- Realizowanie audytów wewnętrznych przez osobę pełniącą równocześnie funkcję IOD i ASI, w konsekwencji czego dokonywanie oceny własnej działalności w odniesieniu do rozporządzenia KRI i RODO.
- Nieodnotowywanie w dziennikach systemów działań użytkowników z uprawnieniami administracyjnymi, co nie wypełnia dyspozycji § 20 ust. 2 rozporządzenia KRI. Nie przechowywanie informacji w dziennikach systemów przez okres 2 lat od dnia ich zapisu, co jest sprzeczne z wymogami § 20 ust. 4 rozporządzenia KRI.
- Nieprowadzenie rejestru wejść osób spoza Urzędu do pomieszczenia serwerowni, zgodnie z wewnętrznymi regulacjami Jednostki.
- Pomieszczenie serwerowni nie dysponuje należytymi zabezpieczeniami, zgodnie z dyspozycją § 19 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.

Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 3/2024
Zalecenia	• w umowie serwisowej XXX oraz w umowie o świadczenie usług w zakresie obsługi informatycznej XXX wprowadzić zapisy określające maksymalny czas skutecznej naprawy oprogramowania, zgodnie z dyspozycją § 19 ust. 2 pkt 10 rozporządzenia KRI; • powierzyć realizację audytów wewnętrznych osobie (podmiotowi), która nie pełni w Urzędzie równocześnie funkcji IOD i ASI; • odnotowywać w dziennikach systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej działania użytkowników z uprawnieniami administracyjnymi, zgodnie z dyspozycją § 20 ust. 2 rozporządzenia KRI; • przechowywać informacje w dziennikach systemów informatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej przez okres 2 lat od dnia ich zapisu, zgodnie z wymogami § 20 ust. 4 rozporządzenia KRI; • prowadzić rejestr wejść do pomieszczenia serwerowni osób spoza Urzędu, zgodnie z wewnętrznymi regulacjami Jednostki; • w pomieszczeniu serwerowni zapewnić warunki gwarantujące utrzymanie odpowiedniego poziomu bezpieczeństwa informacji, zgodnie z dyspozycją § 19 ust. 2 pkt 12 lit. b i e oraz ust. 4 rozporządzenia KRI.
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