WOJEWODA
ZACHODNIOPOMORSKI

Szczecin, dnia 12 października 2022 r.

Znak: K-2.431.1.31.2022.7.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 Ińska, ul. Bohaterów Warszawy 38, 73-140 Ińsko.
Osoba pełniąca funkcję Burmistrza Ińska w okresie objętym kontrolą / okresie prowadzenia kontroli	Pan Jacek Liwak
Okres objęty kontrolą	od dnia 1 stycznia 2019 r. do dnia 1 czerwca 2022 r.
Kontrolujący	Pracownicy Wydziału Kontroli Zachodniopomorskiego Urzędu Wojewódzkiego w Szczecinie: Pani Anna Dąbska – kierownik oddziału, *kierownik zespołu kontrolnego,* Pani Iwona Olesińska – inspektor wojewódzki.
Nr upoważnienia	Nr 37/22 z dnia 24 maja 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	27 maja – 1 czerwca 2022 r.
Rodzaj i tryb kontroli	kontrola planowa, tryb zwykły
Osoba udzielająca wyjaśnień w trakcie kontroli	Pan Jarosław Leśkiw – Sekretarz Gminy.

[1] Dz. U. z 2020r., poz. 224.
[2] Dz. U. z 2021r., poz. 2070.

Obszar kontroli Nr 1	Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
1.1 Współpraca systemów teleinformatycznych z innymi systemami	
Podstawa prawna	**§ 5 ust. 3 pkt 3 rozporządzenia KRI[3]:** *Interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.* **§ 16 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*
Ustalenia kontroli Na podstawie przedstawionej dokumentacji ustalono, że do realizacji zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy i Miasta Ińsko wykorzystywano jeden system centralny (aplikacja Źródło) oraz systemy informatyczne wspomagające obsługę spraw obywatelskich: Program do obsługi Lokalnego Rejestru Mieszkańców wraz z modułem Meldunki - do obsługi Rejestru Cudzoziemców i Program do obsługi Rejestru Wyborców XXX. System centralny (aplikacja Źródło), dostępny przez stronę WWW podlegał kontroli w zakresie formalnego posiadania uprawnień przez pracowników Urzędu. 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. 29, 37-38)	
1.2 Formaty danych udostępniane przez systemy teleinformatyczne	
Podstawa prawna	**§ 17 ust. 1 rozporządzenia KRI:** *Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą.* **§ 18 ust. 1 rozporządzenia KRI:** *Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia.*

[3] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247), zwane dalej „rozporządzeniem KRI".

	§ 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 Gminy i Miasta Ińsko, zgodnie z informacją przekazaną przez Sekretarza Gminy 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. (dowód: akta kontroli str. 29)	
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 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 Gminy i Miasta w Ińsku, w okresie objętym kontrolą obowiązywały następujące uregulowania w zakresie bezpieczeństwa informacji:

- *Zarządzenie Nr 30/2018 Burmistrza Ińska z dnia 25 maja 2018 r. w sprawie wprowadzenie Polityki Ochrony Danych.*
- *Zarządzenie Nr 28/2022 Burmistrza Ińska z dnia 30 maja 2022 r. w sprawie zmiany zarządzenia nr 30/2018 Burmistrza Ińska z dnia 25 maja 2018 r. w sprawie wprowadzenie Polityki Ochrony Danych.*

Powyższe regulacje wprowadziły w Urzędzie System Zarządzania Bezpieczeństwo Informacji[4]. Na SZBI składają się następujące dokumenty:

- *Polityka Ochrony Danych Osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38*.
- *Instrukcja Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38.*
- *Analiza i szacowanie ryzyka w bezpieczeństwie informacji w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38.*
- *Instrukcja Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38.*
- *Polityka Bezpieczeństwa Informacji w zakresie bezpieczeństwie informacji ochrony danych osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38.*

W wyniku analizy obowiązującej dokumentacji związanej z bezpieczeństwem informacji stwierdzono, że określono sposób i wskazano osoby realizujące obowiązki wynikające z rozporządzenia KRI, a funkcjonująca dokumentacja spełnia wymogi określone w § 20 ust. 2 pkt 1 rozporządzenia KRI w zakresie bezpieczeństwa informacji. Procedury 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].

Mając na względzie powyższe, należy stwierdzić, że w Urzędzie Gminy i Miasta Ińsko wdrożono system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność działań.

(dowód: akta kontroli str. 60-152)

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.*

[4] System Zarządzania Bezpieczeństwo Informacji dalej SZBI.
[5] Dz. Urz. UE L2016.119, zwane dalej rozporządzeniem RODO.

Ustalenia kontroli

Metody przeprowadzania analizy ryzyka utraty integralności, dostępności lub poufności informacji, zasady zarządzania ryzykiem ujęto w dokumencie *Analiza i szacowanie ryzyka w bezpieczeństwie informacji w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38.* Procedura uwzględnia wytyczne do oceny prawdopodobieństwa wystąpienia i następstw ryzyka oraz określa metodykę jego szacowania. W dokumencie zidentyfikowano następujące zagrożenia: nielegalny dostęp, błędy i pomyłki, celowe uszkodzenie, nielegalne oprogramowanie, wirusy, personel, awarie, klęski żywiołowe, pokonanie i omijanie zabezpieczeń, nielegalne kopiowanie, nieuprawnione naprawy, podsłuch i podgląd, niedyskrecja. Dla wskazanych zasobów (nośniki informacji, zgromadzone dane, oprogramowanie, sprzęt komputerowy) określono skutki i podatność, a w rezultacie poziom ryzyka utraty integralności, dostępności i poufności informacji. Z przedstawionej analizy wynika, że dla zdefiniowanych w Jednostce zasobów zidentyfikowano niski lub średni poziom 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. Zaleca się, aby zarządzanie ryzykiem w bezpieczeństwie informacji było integralną częścią wszystkich działań związanych z tym obszarem oraz zostało zastosowane w ciągłej eksploatacji SZBI.

(dowód: akta kontroli str. 65-82, 153-172, 243)

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:

- *Wykaz sprzętu w Urzędzie Gminy i Miasta w Ińsku,*
- *Wykaz oprogramowania w Urzędzie Gminy i Miasta w Ińsku,*
- Karty ewidencyjne jednostek komputerowych oraz sprzętu użytkowanego w Urzędzie.

Przedłożone dokumenty zawierały informacje dotyczące rodzaju użytkowanego w Jednostce sprzętu (nazwa i jego charakterystyka), zainstalowanego oprogramowania oraz współpracujących urządzeń peryferyjnych.

Mając na uwadze powyższe należy stwierdzić, że w Urzędzie prowadzona jest inwentaryzacja sprzętu i oprogramowania, zgodnie z wymogami rozporządzenia KRI.

(dowód: akta kontroli str.192-207)

2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych

Podstawa prawna	**§ 20 ust. 2 pkt 4 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem*

	informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. **§ 20 ust. 2 pkt 5 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Ustalenia kontroli

Przepisy § 20 ust. 2 pkt 4 i pkt 5 rozporządzenia KRI stanowią m.in, że kierownictwo podmiotu publicznego w celu zapewnienia bezpieczeństwa informacji powinno podjąć działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, adekwatne do realizowanych zadań, a także podjąć bezzwłoczne działania w przypadku zmiany zadań tych osób. Przetwarzanie informacji w systemach teleinformatycznych wymaga dostępu do danych przez uprawnione osoby, w ustalonym zakresie.

Kwestie nadawania i odbierania uprawnień (upoważnień) do przetwarzania danych osobowych oraz nadawania, modyfikacji oraz odbierania uprawnień użytkownikom do pracy w systemach informatycznych uregulowano w *Instrukcji Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38.* Upoważnienia wydaje Administrator Danych Osobowych na podstawie wniosku o nadanie uprawnień do systemów sporządzonego przez Kierownika Komórki Organizacyjnej przy współpracy z Administratorem Systemu Informatycznego.

Kontrolującym przedstawiono:

- *oświadczenie pracownika o zachowaniu poufności i przestrzeganiu zasad przetwarzania danych osobowych oraz informacji stanowiących tajemnicę służbową,* zobowiązujące między innymi do zachowania w tajemnicy danych osobowych, do których pracownik ma lub będzie miał dostęp w związku z wykonywaniem zadań powierzonych przez pracodawcę. W dokumencie wskazano czas trwania tego zobowiązania, rozszerzając go także na okres po ustaniu stosunku pracy,
- upoważnienia do przetwarzania danych osobowych wystawione pracownikom realizującym zadania zlecone z zakresu administracji rządowej. Dokument upoważnienia określa jego obszar (ustalony w oparciu o zakres obowiązków) oraz okres jego ważności,
- wniosek o założenie profilu/nadanie uprawnień/modyfikację uprawnień. Dokument ten poświadcza realizowanie wymogu dokumentowania czynności nadawania i odbierania uprawnień do pracy w systemach informatycznych. Pisemny wniosek osób upoważnionych powoduje, że proces nadawania i odbierania uprawnień jest w pełni potwierdzony.

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.

W systemach operacyjnych użytkowanych w Urzędzie nie zastosowano polityki automatycznego wymuszania zmiany haseł co pewien interwał czasowy.

W trakcie kontroli nie dokonano sprawdzenia blokowania dostępu do systemów informatycznych, ponieważ w okresie podlegającym badaniu, nie wystąpiły przypadki cofania

uprawnień nadanych pracownikom realizującym zadania zlecone z zakresu administracji rządowej.

(dowód: akta kontroli str. 137-139, 233-243)

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:

- Szkolenie przeprowadzone 24 października 2019 r. - *Ochrona danych osobowych w świetle nowego rozporządzenia Parlamentu Europejskiego i Rady UE. Postępowanie w sytuacji naruszeń bezpieczeństwa danych*,
- Szkolenie przeprowadzone 21 grudnia 2020 r. - *Ochrona danych osobowych w świetle nowego rozporządzenia Parlamentu Europejskiego i Rady UE. Postępowanie w sytuacji naruszeń bezpieczeństwa danych. Bezpieczeństwo danych podczas pracy zdalnej. Ochrona danych osobowych czasie pandemii COVID 19.*

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. Zakres tematyczny szkoleń obejmował zagadnienia wskazane w § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 208-200)

2.6 Praca na odległość i mobilne przetwarzanie danych

Podstawa prawna	**§ 20 ust. 2 pkt 8 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Ustalenia kontroli

Kwestie trybu pracy przy przetwarzaniu mobilnym i pracy na odległość zostały unormowane w *Regulaminie pracy zdalnej w Urzędzie Gminy i Miasta w Ińsku,* wprowadzonym *Zarządzeniem Nr 62/2021 Burmistrza Ińska z dnia 31 grudnia 2021 r.* oraz *Instrukcji Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38* – w punkcie 8 *Procedury korzystania za sprzętu przenośnego.*

W związku z wprowadzonymi w Jednostce uregulowaniami należy stwierdzić, że w Urzędzie opracowano i wdrożono procedurę w zakresie bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, w myśl dyspozycji § 20 ust. 2 pkt 8 rozporządzenia KRI.

Zgodnie z wyjaśnieniami Sekretarza Gminy do realizacji zadań zleconych z zakresu administracji rządowej nie wykorzystywano urządzeń w przetwarzaniu mobilnym i pracy na odległość.

	(dowód: akta kontroli str.144-152)
2.7 Serwis sprzętu informatycznego i oprogramowania	
Podstawa prawna	**§ 20 ust. 2 pkt 10 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*
Ustalenia kontroli Obsługa informatyczna Urzędu realizowana jest na podstawie umowy o świadczenie usług informatycznych, zawartej z firmą prowadzącą działalność gospodarczą XXX[6]. Obsługa informatyczna obejmuje między innymi następujące czynności: administrowanie siecią komputerową, wykonywanie kopii danych, instalację oprogramowania, nadzór nad sprzętem, konfigurację sprzętu i oprogramowania, pełnienie funkcji Administratora Sieci Komputerowej. W powyższej umowie uregulowano kwestię czasu reakcji na zgłoszenie związane z awarią sieci komputerowej, sprzętu lub oprogramowania. Kontrolującym przedstawiono *Umowę powierzenia przetwarzania danych osobowych* zawartą XXX 25 maja 2018 r., *stanowiącą uzupełnienie Umowy z dnia 4 stycznia 2016 r.* Z treści powyższej umowy nie wynika, że obowiązuje ona również w trakcie realizacji aktualnie wiążącej strony *Umowy o świadczenie usług informatycznych* zawartej w dniu 3 stycznia 2022 r. W celu wykonywania zadań z zakresu administracji rządowej XXX zawarto umowę serwisową, której przedmiotem jest udostępnienie i nadzór serwisowy Programu do obsługi Lokalnego Rejestru Mieszkańców oraz Programu do obsługi Rejestru Wyborców.[7] (dowód: akta kontroli str. 221-232)	
2.8 Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji	
Podstawa prawna	**§ 20 ust. 2 pkt 13 rozporządzenia KRI:** *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*
Ustalenia kontroli W *Instrukcji Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38* przedstawiono katalog przypadków zakwalifikowanych jako naruszenie lub podejrzenie naruszenia zabezpieczenia systemu informatycznego oraz określono sposób postępowania w przypadku naruszenia bezpieczeństwa, w tym naruszenia danych osobowych. W trakcie kontroli uzyskano oświadczenie zastępcy Burmistrza, iż w Jednostce nie był prowadzony rejestr incydentów naruszenia bezpieczeństwa informacji, ze względu na brak zgłoszenia tego typu zdarzeń. (dowód: akta kontroli str.83-93, 242)	
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.*

[6] Umowa o świadczenie usług informatycznych z dnia 3 stycznia 2022 r.

[7] Umowa serwisowa nr K058/2022 z dnia 22 grudnia 2021r.

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:

- *Raport z audytu ochrony danych osobowych w zakresie zgodności z RODO (...) oraz Rozporządzenia z dnia 12 kwietnia 20212 r. w sprawie Krajowych Ram Interoperacyjności (...),* data sporządzenia 7.10.2019 r.
- *Raport z audytu ochrony danych osobowych w zakresie zgodności z RODO (...) oraz Rozporządzenia z dnia 12 kwietnia 20212 r. w sprawie Krajowych Ram Interoperacyjności (...),* data sporządzenia 30.12.2020 r.
- *Raport z audytu ochrony danych osobowych w zakresie zgodności z RODO (...) oraz Rozporządzenia z dnia 12 kwietnia 20212 r. w sprawie Krajowych Ram Interoperacyjności (...),*data sporządzenia 14.05.2021 r.
- *Diagnoza cyberbezpieczeństwa w ramach grantu Cyfrowa Gmina* (ocena zgodności KRI, CERT) data sporządzenia 17.05.2022 r.

Audyty wewnętrzne realizowane corocznie w Jednostce obejmowały swym zakresem zagadnienia związane z bezpieczeństwem informacji, wobec czego spełniono wymogi określone w § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 173-189)

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 przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii i zapewnieniu bezpieczeństwa plików systemowych.

Kopie zapasowe oprogramowania wykorzystywanego do realizacji zadań zleconych z zakresu administracji rządowej wykonywane są na szyfrowanym pendrive, z częstotliwością raz w miesiącu. Urządzenie z zapisanymi kopiami przechowywane jest w kasie pancernej.

Zgodnie z wyjaśnieniami Burmistrza z dnia 31 maja 2022 r. w okresie objętym kontrolą wykonano jeden test (w dniu 31 maja 2022 r.) odtwarzania kopii na potrzeby weryfikacji poprawności i stanu wykonywania tych kopii.

Z Instrukcji Zarządzania Systemem Informatycznym (...) wynika, że osobą odpowiedzialną za sporządzanie kopii jest użytkownik systemu. W procedurze wskazano miejsce przechowywania kopii oraz możliwe sposoby ich sporządzania. Nie określono natomiast zasad i częstotliwości testowania kopii zapasowych danych i systemów, nie określono również sposobu dokumentacji tych działań.

(dowód: akta kontroli str. 138-139, 243-245)

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 *Polityce Bezpieczeństwa Informacji w zakresie bezpieczeństwie informacji ochrony danych osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38*, pkt 9 *Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych* określono działania związane z wdrażaniem nowych systemów teleinformatycznych oraz wprowadzaniem zmian w eksploatowanych systemach, a także wskazano osoby odpowiedzialne za realizację i nadzór nad tymi procesami. Do wykonania zadań zleconych z zakresu administracji rządowej w Urzędzie wykorzystywano systemy informatyczne wspomagające obsługę spraw obywatelskich: Program do obsługi Lokalnego Rejestru Mieszkańców wraz z modułem Meldunki (do obsługi Rejestru Cudzoziemców) i Program do obsługi Rejestru Wyborców. W celu realizacji powyższych obowiązków zawarto umowę XXX, której przedmiotem jest wytworzenie i udostępnienie nowych wersji wyżej wymienionego oprogramowania, korzystanie z bezpłatnych porad i konsultacji telefonicznych, internetowych oraz udział pracowników Jednostki w szkoleniach w zakresie korzystania z tych aplikacji. (dowód: akta kontroli str. 107-108, 223-224)	
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. Dostęp do	

danych upoważniony użytkownik uzyskuje po wpisaniu hasła. Pracownicy złożyli oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będą mieli dostęp w trakcie wykonywania obowiązków służbowych, jak również po ustaniu zatrudnienia w Urzędzie.
W *Instrukcji Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Urzędzie Gminy i Miasta w Ińsku, 73-140 Ińsko, ul. Bohaterów Warszawy 38,* w pkt 13 *Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji* określono zasady związane z bezpieczną utylizacją sprzętu informatycznego i nośników danych, a także zasady przekazywania sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie bezpieczeństwa informacji.
Serwer umieszczono w oddzielnym pomieszczeniu, zlokalizowanym na parterze budynku Urzędu. Pomieszczenie serwerowni wyposażono w czujkę dymu, lecz nie posiada ono wydajnego systemu chłodzącego (nie jest pomieszczeniem klimatyzowanym); co bezpośrednio wpływa na brak możliwości utrzymania odpowiedniego poziomu temperatury powietrza. Ponadto wejście do serwerowni nie dysponuje należytymi zabezpieczeniami, co w oczywisty sposób wpływa na obniżenie bezpieczeństwa teleinformatycznego Jednostki. Dostęp osób nieupoważnionych do serwerowni jest ograniczony – dysponentem klucza do pomieszczenia, zgodnie z wyjaśnieniami Sekretarza Gminy jest on sam. W pomieszczeniu serwerowni znajdują się dokumenty przeznaczone do archiwizacji. Zgodnie z wyjaśnieniami Sekretarza Gminy dokumenty przechowywane są czasowo, a serwerownia nie jest miejscem docelowym dla umieszczonych tam (znajdujących się w dniu kontroli) materiałów.

(dowód: akta kontroli str. 128-130, 137-138)

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

W celu minimalizowania ryzyka utraty informacji w Urzędzie zastosowano firewall programowy. Stacje robocze wyposażono w zasilacze zapasowe UPS zabezpieczające sprzęt przed zanikiem zasilania. W procedurach wewnętrznych Jednostki określono zasady przesyłania danych poza obszar przetwarzania oraz zasady bezpiecznej wymiany informacji, poprzez zastosowanie między innymi ochrony kryptograficznej.
Zgodnie z wyjaśnieniami Burmistrza Ińska z dnia 31 maja 2022 r. na komputerach użytkowanych

w Urzędzie zainstalowane jest oprogramowanie antywirusowe DEFENDER. Z załączonego do wyższego wymienionego pisma zrzutu ekranu (*Zabezpieczenia w skrócie, ochrona przed wirusami i zagrożeniami*), ze stanowiska komputerowego wykorzystywanego do realizacji zadań z zakresu administracji rządowej wynika, że definicje ochrony są nieaktualne. (dowód: akta kontroli str. 243, 246)	
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 § 21 rozporządzenia KRI. Logi systemów przechowywane są przez okres 2 lat, co jest zgodne z § 21 ust. 4 rozporządzenia KRI. Zgodnie z wyjaśnieniami Burmistrza z dnia 31 maja 2022 r. w Jednostce nie są prowadzone działania związane z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych. (dowód: akta kontroli str. 243, 245, 247)	

Stwierdzone nieprawidłowości w obszarze Nr 2:

- niewykonywanie cyklicznie testów odtwarzania kopii bezpieczeństwa na potrzeby weryfikacji poprawności i stanu wykonywania tych kopii, do czego zobowiązują przepisy § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI,
- niedokonywanie przeglądów logów oraz ich analizy w celu identyfikacji działań niepożądanych, zgodnie ze wskazaniem § 20 ust. 2 pkt 12 rozporządzenia KRI,
- brak aktualnie obowiązującej umowy powierzenia przetwarzania danych osobowych XXX, zgodnie z dyspozycją § 20 ust. 2 pkt 10 rozporządzenia KRI,
- nieaktualizowanie oprogramowania antywirusowego, do czego zobowiązują przepisy § 20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI,
- pomieszczenie serwerowni nie dysponuje należytymi zabezpieczeniami, zgodnie z dyspozycją § 20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI.

Ocena obszaru kontroli	**Pozytywna z nieprawidłowościami**
Wpis do książki kontroli	Nr 7
Wnioski dotyczące uzyskanych efektów zrealizowanego zadania	Korekty wymagają działania zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, poprzez kontrolę logów systemów; czynności związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych i aplikacji, przez stosowanie systemów antywirusowych oraz działania związane z zapewnieniem ochrony fizycznej informacji, minimalizujące wystąpienie ryzyka ich utraty poprzez zabezpieczenie w sposób kompleksowy pomieszczenia serwerowni.
Zalecenia	• przeprowadzać cyklicznie testy odtwarzania kopii bezpieczeństwa na potrzeby weryfikacji poprawności i stanu wykonywania tych kopii, do czego zobowiązują przepisy § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, • prowadzić działania związane z przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych, zgodnie ze wskazaniem § 20 ust. 2 pkt 12 rozporządzenia KRI, • zawrzeć umowę powierzenia przetwarzania danych osobowych XXX, zgodnie z dyspozycją § 20 ust. 2 pkt 10 rozporządzenia KRI, • dokonać aktualizacji oprogramowania antywirusowego, do czego zobowiązują przepisy § 20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI, • dostosować pomieszczenie serwerowni, zgodnie ze wskazaniami dyspozycji § 20 ust. 2 pkt 12 oraz ust. 4 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 Mateusz Wagemann II Wicewojewoda Zachodniopomorski