Wojewoda
Warmińsko-Mazurski
Radosław Król

WK-I.431.22.2025
Wydział Kontroli

Olsztyn, 25 lutego 2026 r

Szanowny Pan
Jan Kasprowicz
Wójt Gminy Gietrzwałd
ul. Olsztyńska 2
11-036 Gietrzwałd

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

kontrolę przeprowadzono w Urzędzie Gminy w Gietrzwałdzie[1], ul. Olsztyńska 2, 11-036 Gietrzwałd, NIP jednostki 739-10-12-808, REGON jednostki 000538277.

- W okresie objętym kontrolą oraz czasie prowadzonych czynności kontrolnych, kierownikiem kontrolowanej jednostki był Pan **Jan Kasprowicz** - Wójt Gminy, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 10 sierpnia 2017 r.

- Pani **Krystyna Dzikowska** - Sekretarz Gminy zatrudniony na podstawie umowy o pracę od dnia 1 kwietnia 2019 r. (nadzorujący bezpośrednio pracowników realizujących zadania objęte kontrolą).

- W okresie objętym kontrolą oraz w dniu rozpoczęcia czynności kontrolnych odpowiedzialnymi za realizację zadania objętego kontrolą byli:
[redacted]

[akta kontroli poz. 17]

[1] Zwanym dalej: Urzędem

telefon: (89) 5232 333, (89) 5232 444
adres email: info@uw.olsztyn.pl
strona www: gov.pl/web/uw-warminsko-mazurski
adres e-Doręczeń: AE:PL-63617-21139-RGDWI-27

Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie
adres: Al. Marsz. J. Piłsudskiego 7/9, 10-575 Olsztyn

Kontrolę przeprowadzili pracownicy Wydziału Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – starszy inspektor wojewódzki; przewodniczący zespołu kontrolnego, legitymacja służbowa nr 1/2024, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr WK-I.0030.1125.2025 z 1 grudnia 2025 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – starszy inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 6/2025, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr WK-I.0030.1126.2025 z 1 grudnia 2025 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli poz. 13]

Kontrolę przeprowadzono w dniach 5-29 grudnia, co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 7/2025.

[akta kontroli poz. 18-19]

Kontrola prowadzona była w trybie hybrydowym, tj., w dniu 5 grudnia br. – rozpoczęcie czynności kontrolnych w Urzędzie oraz oględziny serwerowni na miejscu w jednostce. Pozostałe dni (8-29 grudnia br.) kontrola była prowadzona zdalnie, bez osobistej obecności kontrolerów Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymacje oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

[akta kontroli poz. 1, 12, 13]

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2025 r., poz. 1703). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2024 r.

[akta kontroli poz. 1, 12, 13]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224 ze zm.), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tj. Dz. U. z 2025 r., poz. 428), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2024 r., poz. 1557)[2], rozdziału III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie

[2] Zwanej dalej: ustawą

Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli poz. 1, 12, 13]
Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z nieprawidłowościami.**
Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez Urząd przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są 3 systemy teleinformatyczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie:

[redacted]

[akta kontroli poz. 9]

I. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1.1. Usługi elektroniczne

Z art. 16 ust. 1a ustawy wynika, że podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.

[3] Zwanego dalej: rozporządzeniem KRI

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:

a) informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;
b) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Na podstawie ustawy z dnia 18 listopada 2020 r. O doręczeniach elektronicznych (Dz.U. z 2024 r. poz. 1045), Urząd wdrożył rozwiązania techniczne i organizacyjne niezbędne do uruchomienia publicznej usługi rejestrowanego doręczenia elektronicznego (e-Doręczenia). Dzięki tej usłudze podmioty publiczne, obywatele, firmy mogą korzystać z wygodnych i bezpiecznych doręczeń elektronicznych. Są one równoważne prawnie tradycyjnej przesyłce poleconej za potwierdzeniem odbioru.
Adres Urzędu Gminy do e-Doręczeń to: **AE:PL-35715-60853-AVBHT-30**.

Ponadto, Urząd posiada aktywną Elektroniczną Skrzynkę Podawczą **/l0i1g6cm9d/skrytka**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie głównej BIP Urzędu (zakładka - Pozostałe - ESP), podano informacje dotyczące Elektronicznej Skrzynki Podawczej (ESP) Urzędu na platformie ePUAP. Wskazano wymagania dotyczące dokumentów, formaty danych przyjmowane za pośrednictwem ESP oraz wymagania odnośnie wielkości załączników.

[akta kontroli poz. 20]

Na stronie portalu www Urzędu, znajduje się bezpośredni odnośnik do serwisu Elektronicznego Biura Obsługi Klienta (e-BOK). Jest on przeznaczony dla mieszkańców, którzy chcą korzystać ze wskazanych usług drogą elektroniczną. Zalogowany użytkownik może: przeglądać wystawione faktury, dokonane zapłaty, sprawdzić stan salda na koncie rozrachunkowym, sprawdzić ewentualne windykacje oraz wydrukować obraz faktury.

[akta kontroli poz. 21]

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP, w zakładce *„Procedury załatwiania spraw"*, opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne stanowiska Urzędu, drogą tradycyjną (osobiste złożenie dokumentów lub przesłanie w sposób elektroniczny).
Natomiast w zakładce *„Wzory pism i druki"* opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych stanowisk w Urzędzie.

Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą kontrolowanych systemów teleinformatycznych.

[akta kontroli poz. 22-23]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b ust. 3 ustawy, organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym.

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych. Z informacji uzyskanych podczas kontroli wynika, że Urząd nie przekazywał do CRWDE wzorów dokumentów elektronicznych.

[akta kontroli poz. 45]

Jednocześnie na stronie BIP, w zakładce „Procedury załatwiania spraw", opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne stanowiska Urzędu, drogą tradycyjną (osobiste złożenie dokumentów lub przesłanie w sposób elektroniczny). Natomiast w zakładce „Wzory pism i druki" opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych stanowisk w Urzędzie.

[akta kontroli poz. 22-23]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.3. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 9 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i

egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.

Zgodnie z wyjaśnieniem uzyskanym z Urzędu w przedmiotowej sprawie, cyt [redacted]

Realizacja zasad obiegu dokumentacji w formie elektronicznej zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.

Jednocześnie kontrolujący poddają pod rozważenie Kierownictwu kontrolowanej jednostki wprowadzenie na stałe (nie jako system wspomagający) w Urzędzie elektronicznego systemu zarządzania dokumentami, który z pewnością wpłynie na usprawnienie przepływu dokumentów w podmiocie, znacząco usprawni ich archiwizację oraz zapewni łatwy dostęp do dokumentów archiwalnych, co z kolei wpłynie na przyspieszenie załatwianych spraw w tym realizowanych przez podmiot usług oraz pozwoli na minimalizowanie nakładu pracy a także podniesie poziom Bezpieczeństwa Informacji. Celem wdrożenia systemu elektronicznego zarzadzania dokumentacją jest wyeliminowanie z obiegu wewnętrznego podmiotu dokumentów papierowych, co spowodowałoby dodatkowo obniżenie kosztów.

[akta kontroli poz. 45]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 1 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) 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;
- § 20 ust. 2 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.)

zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;

- § 20 ust. 2 pkt 1 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 1 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, 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) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO", w celu ustanowienia zasad bezpieczeństwa przetwarzania informacji w Podmiocie, przyjęto:

[redacted]

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego opracowania dokumentacji **SZBI** (System Zarządzania Bezpieczeństwem Informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia.

[redacted]

Mając powyższe na uwadze, należy wskazać, że podstawowym elementem SZBI jest **Polityka Bezpieczeństwa Informacji**. Zgodnie z definicją zawartą w rozporządzeniu KRI §2 pkt 15 polityka bezpieczeństwa informacji jest to zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania.

Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji. PBI może określać aktywa oraz ich właścicieli, oraz sposób szacowania ryzyka i postępowania z ryzykiem. Zazwyczaj w ramach SZBI funkcjonują inne polityki, regulaminy i procedury np.:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.
- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywaniem testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dokumentację SZBI stanowią także:

- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka BI;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;
- Dokumentacja audytów z zakresu BI;
- Dokumentacja incydentów naruszenia BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

[redacted] Mając na względzie przepisy § 20 (19) ust. 1-2 rozporządzenia KRI należy uznać, że przyjęta w Urzędzie polityka stanowi tylko jedną ze składowych dokumentacji ustanawiającej SZBI w jednostce i nie dopełnia w całości obowiązku wynikającego z cytowanych powyżej przepisów.

Powyższe stanowi nieprawidłowość, skutkującą naruszeniem § 20 (19) ust. 1-2 rozporządzenia KRI. Przyczyną nieprawidłowości jest niestosowanie przepisów i wytycznych w tym zakresie. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

Ponadto, z § 20 (19) ust. 3 rozporządzenia KRI wynika ponadto, że wymagania określone w ust. 1 tego paragrafu uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (Polska Norma PN-EN ISO/IEC 27001:2017 Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą (PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem).
Jednocześnie w pkt 5.1 Polskiej Normy PN-EN ISO/IEC 27002, wskazano wymóg opracowania i stosowania **Polityki Bezpieczeństwa Informacji** - PBI.

[akta kontroli poz. 24-27]

Z przekazanej kontrolującym listy wynika, że pracownicy Urzędu zapoznali się i przyjęli do stosowania obowiązujące w okresie objętym kontrolą dokumenty SZBI.

[akta kontroli poz. 45]

W myśl § 20 (§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.
Z informacji uzyskanej z Urzędu w przedmiotowym zakresie wynika, że cyt.: *„Urząd na bieżąco aktualizuje i wdraża Politykę Ochrony Danych (aktualizowanie rejestru czynności przetwarzania danych, analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych)."*

[redacted]

W udostępnionej dokumentacji, w ramach prowadzonych czynności kontrolnych nie stwierdzono dowodów (np. raporty z czynności, notatki służbowe) świadczących o podejmowaniu w okresie objętym kontrolą dodatkowych działań w zakresie monitoringu utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji. Brak udokumentowania przeprowadzania okresowych przeglądów i monitoringu SZBI w jednostce, należy **ocenić jako uchybienie** skutkujące naruszeniem § 20 (§ 19) ust. 1 rozporządzenia KRI. Przyczyną uchybienia jest niestosowanie przepisów i przyjętych regulacji w tym zakresie. Osobami odpowiedzialnymi za powstanie uchybienia jest IOD pełniący funkcję w okresie objętym kontrolą oraz obsługa informatyczna Urzędu.
Jednocześnie należy wskazać, że rola podmiotu nie kończy się tylko i wyłącznie na opracowaniu i wdrożeniu do eksploatacji systemu zarządzania bezpieczeństwem informacji. Obowiązkiem podmiotu jest także monitorować, przeglądać i utrzymywać jak również doskonalić ten system tak, aby zapewniać poufność, dostępność i integralność informacji. Powyższe oznacza, że

realizacja obowiązku wynikającego z § 20 (§ 19) ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.

[akta kontroli poz. 45]

Wójt Gminy powołał w jednostce Inspektora Ochrony Danych IOD (Zarządzenie Nr 145/2021 Wójta Gminy Gietrzwałd z dnia 31 grudnia 2021 r.) oraz Administratora Systemów Informatycznych (zakresy czynności informatyków). W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO, prowadzony jest rejestr czynności przetwarzania.

[akta kontroli poz. 28-31]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z nieprawidłowościami.**

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Z § 20 ust. 2 pkt 3 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 3 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) wynika, że 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.

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu. Analiza ryzyka jest ważnym wymaganiem nałożonym na administratorów i podmioty przetwarzające. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.

Zgodnie z wymogiem wynikającym z § 20 (obecnie § 19) ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko. W tym miejscu należy wyraźnie uwypuklić, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. przeprowadzania okresowych analiz. Oznacza to, iż zgodnie z § 20 ust. 2 (obecnie § 19 ust. 2) kierownictwo podmiotu musi w swoich procedurach wewnętrznych dotyczących przeprowadzania okresowych analiz ryzyka, wprowadzić mechanizmy umożliwiające zarówno realizację jak i egzekwowanie tego działania,

co w tym przypadku oznacza konieczność określenia okresu, co jaki takie działanie będzie podejmowane.
Kontrolującym przedstawiono dokumentację (stanowiącą akta kontroli) świadczącą o przeprowadzeniu (w okresie objętym kontrolą), procesu okresowej analizy ryzyka oraz zagrożeń przy przetwarzaniu danych osobowych, w okresie objętym kontrolą zgodnie z przyjętymi założeniami.

[akta kontroli poz. 32-34]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Z § 20 ust. 2 pkt 2 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 2 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.), wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Kontrolującym przedstawiono inwentaryzację (w formie elektronicznej) sprzętu komputerowego użytkowanego w Urzędzie, sporządzoną w oparciu o § 20 (§19) ust. 2 pkt 2 rozporządzenia KRI.

[akta kontroli poz. 35-36]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 4 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) 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 (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 5 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Istotnym elementem polityki BI (bezpieczeństwa informacji) jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zasady nadawania uprawnień i upoważnień do przetwarzania danych osobowych oraz do pracy w określonym zbiorze danych (systemie informatycznym), określone zostały w:

[redacted]

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania oraz do przetwarzania danych osobowych w określonym zbiorze danych (systemie), wynikającym z zakresu czynności danego pracownika. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych i pracy w określonym zbiorze danych.

[akta kontroli poz. 24-25, 37-38]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 6 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) wynika, że 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.

Zasady dotyczące szkolenia pracowników zaangażowanych w proces przetwarzania informacji, określone zostały w:

[redacted]

Zgodnie z zapisami **Art.12 POD**:

[redacted]

Zgodnie z zapisami **rozdziału IV IZSI**:

[redacted]

[redacted]

Z informacji uzyskanych w przedmiotowej sprawie z Urzędu wynika, że cyt [redacted]

Brak zapewnienie w okresie objętym kontrolą 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, **stanowi nieprawidłowość**. Przyczyną powstania nieprawidłowości było niestosowanie obowiązujących przepisów prawa (KRI) oraz przyjętych regulacji wewnętrznych (POD, IZSI), w przedmiotowym zakresie. Skutkiem zaistnienia nieprawidłowości było niedoinformowanie oraz ograniczenie wiedzy pracowników uczestniczących w procesie przetwarzania informacji w zakresie przepisów prawa regulujących powyższą tematykę. Osobami odpowiedzialnymi za powstanie uchybienia jest IOD pełniący funkcję w okresie objętym kontrolą oraz obsługa informatyczna Urzędu.

[akta kontroli poz. 24-25, 45]

Mając powyższe na uwadze, przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z nieprawidłowościami.**

2.6. Praca na odległość i mobilne przetwarzanie danych

Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 8 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.)zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

Podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, określone zostały w [redacted]

[akta kontroli poz. 25]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 10 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy

systemu w przypadku awarii oraz gwarantującymi bezpieczeństwo informacji (BI) dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

W Urzędzie (zgodnie z przedstawionym wykazem zał. nr 2) użytkowany jest jeden system teleinformatyczny przeznaczony do realizacji zadań zleconych z zakresu administracji rządowej, zakupiony u zewnętrznego dostawcy, tj.: [redacted]

W związku z zakupem ww. systemu podpisane zostały z dystrybutorem stosowne umowy licencyjne, umożliwiające prawidłową eksploatację i rozwój, poprzez możliwość zgłaszania błędów pytań i roszczeń, dotyczących użytkowanego systemu.
W umowie licencyjnej zawarto również stosowne zapisy w zakresie powierzenia danych gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantujące bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umów.

[akta kontroli poz. 39-40]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 13 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) wynika, że 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.

Instrukcja postępowania w przypadku stwierdzenia incydentu zagrożenia w postaci naruszenia ochrony danych, jak również podejmowanych działań korygujących, uregulowana została w: [redacted]

[akta kontroli poz. 24-25]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 14 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Audyt bezpieczeństwa informacji jest procesem przeprowadzanym w celu zidentyfikowania zagrożeń mogących skutkować utratą poufności, integralności lub dostępności informacji. Celem

audytu wewnętrznego bezpieczeństwa informacji jest ocena zakresu zgodności Systemu Zarządzania Bezpieczeństwem Informacji jednostki z kryteriami audytu.

W dniu 21 maja 2024 r. przeprowadzony został w Urzędzie Gminy w Gietrzwałdzie audyt bezpieczeństwa informacji przez firmę: [redacted] Celem audytu było przedstawienie stanu bezpieczeństwa informacji w jednostce oraz wskazanie ewentualnych podatności mających wpływ na przetwarzane dane. Audyt został przeprowadzony pod kątem zgodności z obowiązującymi przepisami prawa w zakresie przetwarzania informacji oraz dobrych praktyk i standardów bezpieczeństwa. Audyt został zrealizowany na podstawie udostępnionej dokumentacji (procedur), sprzętu oraz w oparciu o obowiązujące przepisy prawne.
Mając powyższe na uwadze należy uznać, że obowiązek wynikający z § 20 (§ 19) ust. 2 pkt 14 rozporządzenia KRI który stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok – w 2024 r. został zrealizowany.

[akta kontroli poz. 41]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 12 lit. b rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Tworzenie kopi zapasowych jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć wykonując regularnie kopie zapasowe całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

Zasady tworzenia i testowania kopii zapasowych m.in. z kontrolowanych systemów teleinformatycznych, uregulowane zostały w:

[redacted]

Zgodnie z wyjaśnieniem uzyskanym z Urzędu w przedmiotowej sprawie, cyt.: [redacted]

[redacted]

[akta kontroli poz. 45, 48-51]

Na podstawie udostępnionej dokumentacji (dziennik testowania kopii zapasowych), kontrolujący stwierdzili, że w Urzędzie są wykonywane testy odtworzeniowe kopii zapasowych. Zgodnie z przekazanym kontrolującym dziennikiem testowania, sprawdzenia wytworzonych kopii zapasowych dokonuje się raz w miesiącu.

[akta kontroli poz. 47]

Regularne tworzenie i testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Prawidłowo zdefiniowana polityka kopii bezpieczeństwa oraz gruntownie przetestowane procesy odtwarzania systemów teleinformatycznych są istotnymi aspektami w każdej jednostce, której procesy opierają się na działaniu systemów informatycznych. Prawidłowo zdefiniowana i wykonana procedura pozwala mieć pewność, że w razie awarii systemu, wytworzone backupy spełnią swoje zadanie i nie odbije się to negatywnie na ciągłości działania jednostki.
Ponadto niezwykle istotnym aspektem wpływającym na bezpieczeństwo wytworzonych kopii zapasowych jest w miarę możliwości finansowych Urzędu tzw. **odmiejscowienie kopii zapasowych**, czyli przechowywanie kopii zapasowych nie tylko na fizycznie odrębnym sprzęcie (np. serwerze), ale także w odrębnej lokalizacji pozwalającej uniknąć uszkodzeń spowodowanych katastrofą, która dotknęłaby ośrodek podstawowy. W przypadku niewłaściwego przechowywania kopii zapasowych danych z systemów informatycznych, tj. w sposób, który nie minimalizuje ryzyka utraty informacji, urząd może utracić zarówno dane źródłowe, jak i ich kopie zapasowe. [redacted]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 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.

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej, dzieliły się na systemy centralne lub przekazane, [redacted]

Na obsługę zainstalowanego w okresie objętym kontrolą oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

[akta kontroli poz. 9, 39-40]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) wynika, że 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.

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

Zgodnie z wyjaśnieniem uzyskanym z Urzędu, cyt.: [redacted]

[akta kontroli poz. 45]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

- § 20 ust. 2 pkt 12 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 2 pkt 12 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.), 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 (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 19 ust. 4 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) 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.

W punkcie 2.12 wykazano mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych danych, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.
Zapewniono również środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej, poprzez stosowanie kart dostępowych, certyfikatów kwalifikowanych oraz indywidualnych loginów i haseł.

[redacted]

[akta kontroli poz. 15-16]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

- § 21 ust. 2 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 20 ust. 2 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) 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 brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 20 ust. 3 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) poza informacjami wymienionymi w § 21 (§ 20) 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 (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 20 ust. 4 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.) 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.

Zgodnie z § 21 ust. 1 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.) oraz § 20 ust. 1 rozporządzenia KRI (w brzmieniu obowiązującym od dnia 23 maja 2024 r.), rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

[redacted]

Rozliczalność jest właściwością systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie, zatem zapewnienie rozliczalności działań polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszystkie działania dostępu do systemu z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i zabezpieczeń, a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych). Informacje zawarte w dziennikach systemowych powinny być regularnie przeglądane w celu wykrycia działań niepożądanych/nieuprawnionego dostępu oraz powinny być przechowywane w bezpieczny sposób, co najmniej 2 lata.

[akta kontroli poz. 52-54]

Mając na uwadze powyższe, przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

III. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu.

Zgodnie z § 19 rozporządzenia KRI (w brzmieniu obowiązującym do dnia 23 maja 2024 r.), w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI. Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

Każda strona dostępna w Internecie powinna zapewniać maksymalne wsparcie wszystkim grupom wiekowym jak i społecznym. Warunkiem dostępności strony jest dobry kontrast zapewniający swobodny odczyt przedstawionych informacji. Im wyższy jest kontrast, tym łatwiej odróżnić obiekt, zdjęcie czy tekst pierwszego planu od tła. Niski poziom kontrastu utrudnia korzystanie z witryny przede wszystkim użytkownikom o mniejszej ostrości wzroku, a także osobom niedowidzącym. Celem ułatwienia postrzegania tekstu użytkownikom niedowidzącym można również umożliwić zmianę wielkości tekstu bez utraty jego czytelności lub funkcjonalności serwisu internetowego.

Kontrolujący stwierdzili, że zarówno strona internetowa BIP Urzędu, jak portal Urzędu zawiera elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niepełnosprawne (np. niedowidzące). Zastosowane ułatwienia to m.in.:

- możliwość doboru odpowiedniego kontrastu (wysoki /ciemny/ - domyślny /jasny/),
- możliwość powiększenia wielkości liter na stronie,
- podświetlenie linków,
- skróty klawiszowe (np. TAB – fokus do przodu, Shift+TAB – fokus do tyłu)
- moduł wyszukiwania.

[akta kontroli poz. 43-44]

Dostępność cyfrowa to cecha rozwiązań cyfrowych (np. stron, aplikacji, systemów), która umożliwia samodzielne korzystanie z nich przez osoby z niepełnosprawnościami. Jednocześnie wiele jej elementów jest uniwersalnych (np. kontrast, napisy), poprawiających użyteczność każdemu, a nie tylko osobom niepełnosprawnym.
Dostępne cyfrowo muszą być między innymi strony internetowe, aplikacje mobilne, systemy teleinformatyczne i wszystkie treści publikowane w Internecie przez podmioty publiczne. To wyzwanie wdrożeniowe, ale także szansa na dotarcie z informacjami i usługami do szerokiej grupy użytkowników, w tym osób z niepełnosprawnościami.
Jednocześnie należy zaznaczyć, że pomimo tego, że dana strona zawiera podstawowe elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niepełnosprawne (np. kontrast,

powiększenie czcionki, wyszukiwanie), to strona ta wcale nie musi z automatu spełniać kryteriów dostępności cyfrowej.

Mając na uwadze powyższe, przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:

Proszę Pana Wójta o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 14 dni od dnia otrzymania niniejszego wystąpienia, o sposobie wykorzystania uwag i wniosków oraz wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań. Jednocześnie informuję, że stosownie do art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z poważaniem

WOJEWODA
WARMIŃSKO-MAZURSKI
Radosław Król
/podpisano podpisem elektronicznym/