



Wydział Kontroli
WK-I.431.1.2025

**Szanowna Pani
Marta Kamińska Wójt Gminy
Urząd Gminy w Barcianach
ul. Szkolna 3
11-410 Barciany**

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

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Gminy w Barcianach¹, ul. Szkolna 3, 11-410 Barciany, NIP URZĘDU: 742-10-13-713, REGON URZĘDU: 000532777.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych, kierownikiem kontrolowanej jednostki była Pani **Marta Kamińska** – Wójt Gminy, wybrana na stanowisko w wyniku wyborów bezpośrednich w dniu 7 kwietnia 2023 r.
- W okresie objętym kontrolą oraz w dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą był [REDAKTOWANE]
- Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania była [REDAKTOWANE]

[akta kontroli poz. 23]

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.0030.101.2025 z 5 lutego 2025 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

¹ Zwany dalej: Urzędem
Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie
Al. Marsz. J. Piłsudskiego 7/9
10-575 Olsztyn

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.0030.102.2025 z 5 lutego 2025 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli poz. 17]

Kontrolę przeprowadzono w dniach 17 lutego – 7 marca 2025 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 1/2025.

[akta kontroli poz. 24-25]

Kontrola prowadzona była w trybie hybrydowym, tj., w dniu 17 lutego br. – rozpoczęto czynności kontrolne w Urzędzie, dokonano oględzin serwerowni na miejscu w jednostce. Pozostałe dni (18 lutego – 7 marca 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, 14]

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 2024 r., poz. 1557). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2024 r.

[akta kontroli poz. 1, 14]

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), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tj. Dz. U. z 2023 r., poz. 190), 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 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, 14, 16]

² Zwanej dalej: ustawą

³ Zwanego dalej: rozporządzeniem KRI

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 niżej wymienione systemy teleinformatyczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie:



[akta kontroli poz. 10]

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.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągnana 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.

Urząd posiada aktywną Elektroniczną Skrzynkę Podawczą **/UGBarciany/Skrytka**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie głównej BIP Urzędu, podano adres do Elektronicznej Skrzynki Podawczej. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Podczas kontroli ustalono, że Urząd dysponuje Elektroniczną Skrzynką Podawczą (ESP), która działa zgodnie z określonymi prawnie wymogami. Na stronie internetowej BIP Urzędu wprowadzie opublikowano informację o adresie ESP, jednakże nie opublikowano informacji o metodach dostarczania i wymaganiach dla dokumentów elektronicznych, wynikających z § 3 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 poz.180). Brak spełnienia powyższych wymogów stanowi **uchybie** skutkujące niedoinformowaniem petentów o metodach dostarczania i wymaganiach dla dokumentów elektronicznych. Przyczyna uchybienia jest niestosowanie obowiązujących przepisów w przedmiotowym zakresie. Osobą odpowiedzialną jest pracownik nadzorujący działanie ESP Urzędu.

[akta kontroli poz. 28]

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 referaty Urzędu, drogą tradycyjną (osobiste złożenie dokumentów lub przesłanie pocztą). W przedmiotowej zakładce opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych referatów 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. 29]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami**.

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 udostępniana 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 w okresie objętym kontrolą Urząd nie publikował żadnych dokumentów w CRWDE, jednocześnie wykorzystuje wzory zawarte w CRWDE.

Jednocześnie na stronie BIP, w zakładce „*Procedury załatwiania spraw*”, opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne referaty Urzędu, drogą tradycyjną (osobiste złożenie dokumentów lub przesłanie pocztą). W przedmiotowej zakładce opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych referatów w Urzędzie – do wykorzystania przez petentów Urzędu.

[akta kontroli poz. 29, 46]

W związku z powyższym przedmiotowe częściowe 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, modyfikację, usunięcie lub zniszczenie.

Zgodnie z zarządzeniem

Określenie zasad obiegu dokumentacji w formie elektronicznej zgodnie z § 20 (§ 19) ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.

██████████ jest systemem teleinformatycznym do elektronicznego zarządzania dokumentacją umożliwiającą wykonywanie w nim czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw oraz gromadzenie i tworzenie dokumentów elektronicznych. Pozwala on na zamianę dokumentów, które mają formę papierową na ich elektroniczne wersje. Umożliwia też tworzenie w pełni elektronicznych dokumentów, które mogą być przesyłane pomiędzy pracownikami.

[akta kontroli poz. 37]

Przedmiotowe częściowe 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.

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. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie.

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.

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 danych w Podmiocie,



Przedmiotową dokumentację sporządzono na podstawie obowiązujących przepisów prawa w tym zakresie, tj. RODO oraz rozporządzenia KRI. Dokumentacja w zakresie bezpieczeństwa informacji dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności oraz integralności ich przetwarzania, jak również monitorowania zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa przetwarzanych danych. Przyjęta dokumentacja wchodziła w skład System Zarządzania Bezpieczeństwem Informacji, wymaganego zgodnie z § 20 ust. 1 rozporządzenia KRI, i zapewniała poufność, dostępność i integralność przetwarzanych informacji.

Kontrolującym przedstawiono potwierdzenie świadczącego o fakcie zapoznali się pracowników z przyjętą do stosowania Polityką Bezpieczeństwa Informacji.

[akta kontroli poz. 38, 46-47]

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.



W udostępnionej dokumentacji, w ramach prowadzonych czynności kontrolnych nie stwierdzono dowodów (np. raporty z czynności), świadczących o podejmowaniu w okresie objętym kontrolą dodatkowych działań w zakresie utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji.



Z informacji uzyskanych z urzędu w przedmiotowej sprawie wynika, że cyt.: „Nie były prowadzone dodatkowe przeglądy. Wszystkie czynności były realizowane na bieżąco.”

Odnosząc się do przekazanego wyjaśnienia, należy stwierdzić, że w Urzędzie w 2024 r. nie były prowadzone dodatkowe działania w zakresie utrzymania i doskonalenia systemu zarządzania

bezpieczeństwem informacji, a jedynie doraźne działania w ramach codziennych zadań, z których brak jest dokumentacji potwierdzającej ich przeprowadzenie.

Brak okresowych przeglądów i monitoringu SZBI w jednostce, należy **ocenić jako uchybienie** skutkujące naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną jest ADO.

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. 38, 46]

Wójt Gminy powołał w jednostce Inspektora Ochrony Danych IOD (zarządzenie Nr 80/A/2022 z dnia 22 sierpnia 2022 r.) oraz Administratora Sieci Informatycznych ASI (zarządzenie Nr 111/2021 z dnia 31 grudnia 2021 r.).

W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO, prowadzony jest rejestr czynności przetwarzania.

[akta kontroli poz. 39-40, 48]

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

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. Bez tak doprecyzowanych zapisów nie będzie możliwe cykliczne realizowanie a tym bardziej egzekwowanie wykonania opisywanego działania, tym samym takie niedookreślone regulacje będą stały w sprzeczności z treścią § 20 ust. 2 (obecnie § 19 ust. 2).

Ponadto, zgodnie z wyjaśnieniem uzyskany z Urzędu w przedmiotowej sprawie, cyt.: „

Kontrolującym nie przedstawiono dokumentacji świadczącej o przeprowadzeniu procesu analizy ryzyka utraty integralności, dostępności lub poufności informacji, w okresie objętym kontrolą. Ponadto kontrolujący stwierdzili, że pełnego oszacowania ryzyka utraty integralności, dostępności lub poufności informacji dokonano w jednostce w dniu 31.12 2022 r., a od tego czasu (zgodnie z przedłożoną dokumentacją), nie były dokonywane przeglądy czyli okresowe analizy ryzyka.

Mając na uwadze zapisy przyjętej do realizacji PBI oraz wyjaśnienia uzyskane z Urzędu należy zaznaczyć, że rozporządzenie KRI nie wskazuje konkretnego terminu przeprowadzania analiz ryzyka utraty integralności, dostępności lub poufności informacji, a operuje jedynie terminem okresowości. Podobnie przyjęta do stosowania w Urzędzie PBI zakłada, że przegląd procesu szacowania ryzyka dokonywany musi być regularnie, bez wskazania konkretnego czasookresu. Mając na względzie powyższe zapisy tj. okresowość wskazaną w KRI oraz regularność wskazaną w PBI, zdaniem kontrolujących dwuletni okres bez przeprowadzonego przeglądu (analizy ryzyka) nie wydaje się zbyt długi - w przypadku niestwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, jednakże brak doprecyzowanych zapisów odnoszących się do

okresowości, uniemożliwia kierownictwu realizację oraz egzekwowanie wykonania opisywanego działania, tym samym stoi w sprzeczności z §20 ust. 2 (obecnie § 19 ust. 2 KRI).

Powyższe **uznaje się za nieprawidłowość**, skutkującą naruszeniem § 19 ust. 2 pkt 3 rozporządzenia KRI. Przyczyną nieprawidłowości jest brak wskazanego w PBI konkretnego okresu (przedziału czasowego), po upływie którego należy przeprowadzić analizę ryzyka utraty integralności, dostępności lub poufności informacji. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

[akta kontroli poz. 38, 46]

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

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 (rejestr) sprzętu komputerowego użytkowanego w Urzędzie, prowadzoną w sposób papierowy, sporządzoną w oparciu o § 20 (§19) ust. 2 pkt 2 rozporządzenia KRI.

[akta kontroli poz. 33]

Mając powyższe na uwadze przedmiotowe częściowe 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.



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.

[akta kontroli poz. 38, 46, 49-51]

Mając powyższe na uwadze przedmiotowe częściowe 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.

W okresie objętym kontrolą zgodnie z § 20 (§ 19) ust. 2 pkt 6 rozporządzenia KRI przeprowadzono w Urzędzie szkolenie z zakresu RODO. Program szkolenia obejmował:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 94/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).
- Definicje, nowa metodologia, zasady stosowania.
- Polityka bezpieczeństwa informacji i ochrony danych osobowych, wdrożona w Urzędzie Gminy w Barcianach.
- Incydenty i naruszenia, czyli co się może wydarzyć.
- Jak reagować na incydenty.

Udział w szkoleniu doskonalącym, potwierdzono listą obecności.

Ponadto, wybrani pracownicy Urzędu, uczestniczyli w okresie objętym kontrolą w szkoleniu doskonalącym w zakresie ochrony danych osobowych. Udział w powyższym szkoleniu potwierdzono certyfikatami uczestnictwa.

[akta kontroli poz. 34-36]

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

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 [REDAKTOWANE]

[akta kontroli poz. 52-53]

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 odpowiednie 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) [REDAKTOWANE]

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. Zawarta została również stosowna umowa powierzenia danych gwarantująca właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantująca bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli poz. 41]

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. 38]

Przedmiotowe częściowe 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 dniach 4-18 listopada 2024 r. firma AUDYT I WYCENA Consulting Group Sp. z o.o., z siedzibą w Warszawie, zrealizowała zadanie audytowe pod nazwą: „Audyt bezpieczeństwa informacji w Urzędzie Gminy w Barcianach, w tym ochrony danych osobowych”. Celem audytu była ocena bezpieczeństwa danych osobowych oraz informacji przetwarzanych przy użyciu systemów teleinformatycznych, w tym sposobu zarządzania bezpieczeństwem informacji, z minimalnymi wymaganiami dla systemów teleinformatycznych określonych w ustawie oraz rozporządzeniu KRI. W wyniku przeprowadzonego audytu nie stwierdzono uchybień o charakterze systemowym i nie wydano rekomendacji w zakresie objętym audytem.

[REDACTED] 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. 31]

Przedmiotowe częściowe 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 kopii 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 kopii zapasowych

Mając na względzie udzielone wyjaśnienia należy zaznaczyć, że niezwykle istotnym aspektem wpływającym na bezpieczeństwo wytworzonych kopii zapasowych jest tzw.

Na podstawie wyjaśnień oraz udostępnionej dokumentacji (zrzuty ekranowe backupów) kontrolujący stwierdzili, że w Urzędzie są wykonywane kopie zapasowe, zgodnie z harmonogramem zawartym w PBI.

[akta kontroli poz. 38, 54]

Na podstawie udostępnionej dokumentacji (Dziennik sprawdzeń kopii zapasowych), kontrolujący stwierdzili, że w Urzędzie są wykonywane testy odtworzeniowe kopii zapasowych.

[akta kontroli poz. 55]

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.

Mając powyższe na uwadze przedmiotowe częściowe 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, [REDAKTOWANE]

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. 10, 41]

Mając powyższe na uwadze przedmiotowe częściowe 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, [REDAKTOWANE]



[akta kontroli poz. 46]

Mając na uwadze powyższe przedmiotowe częściowe zagrożenie 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 informacji, 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.

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie, w obecności  (osoby wskazanej przez Kierownika kontrolowanej jednostki).



Powyższe potwierdza dokumentacja fotograficzna i protokół z przeprowadzonych oględzin, stanowiące akta kontroli.



[akta kontroli poz. 21-22]

Przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami**.

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).

Zgodnie z wyjaśnieniem uzyskanym z jednostki

Z dokumentacji przedstawionej kontrolującym (zrzuty ekranu z dziennika logów) wynika, że zapewniono rozliczalności działań prowadzonych w systemach, w szczególności poprzez gromadzenie informacji o tym, kto, kiedy i co wykonał w systemie teleinformatycznym, co pozwalał na uzyskanie wiedzy na temat ewentualnych niepożądanych działań. Logi użytkowników przechowywane są przez dwa lata.

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. 46, 56-59]

Mając na uwadze powyższe, przedmiotowe częściowe 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 niedostępszącym, 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.

Zarówno strona internetowa BIP Urzędu, jak i portal www. Urzędu, zawierała elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niedowidzące. Zastosowane ułatwienia to m.in.:

- możliwość doboru odpowiedniego kontrastu (ciemny-jasny),
- możliwość powiększenia wielkości liter na stronie,
- zmiana interlinii,
- moduł wyszukiwania.

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.

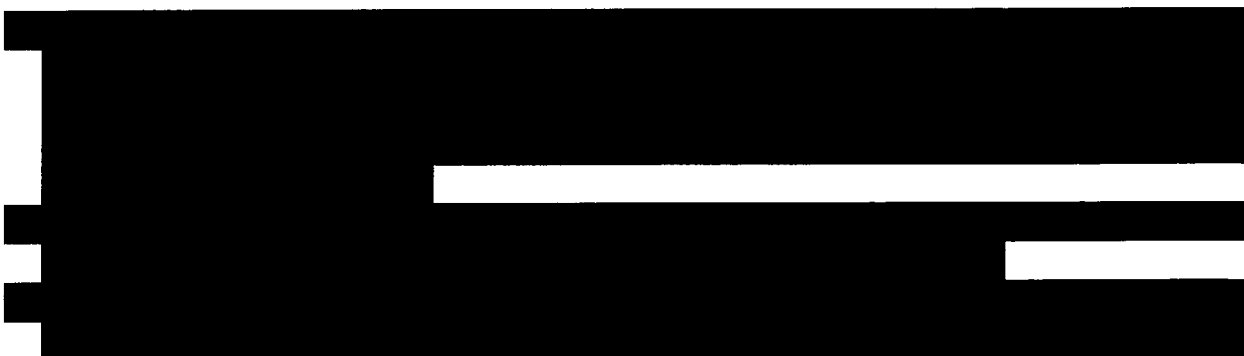
Jednocześnie należy zaznaczyć, że pomimo tego, że dana strona zawiera podstawowe elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niepełnosprawne (np. kontrast, powiększenie czcionki, wyszukiwanie), to strona ta wcale nie musi z automatu spełniać kryteriów dostępności cyfrowej.

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

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:



[REDACTED]

Proszę Panią Wójt 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.

**WOJEWODA
WARMIŃSKO-MAZURSKI**

Radosław Król
/podpisano podpisem elektronicznym/