WOJEWODA ŚWIĘTOKRZYSKI

Kielce, dnia 17-06-2024

Znak:OK.V.431.1.2024

Pan
Tomasz Socha
Wójt Gminy Kije

WYSTĄPIENIE POKONTROLNE

Zakres kontroli:	Prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej.
Okres objęty kontrolą:	od 1 stycznia 2017 r. do dnia wszczęcia kontroli tj. 15 marca 2024 r.
Kontrolerzy:	Marek Rak – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 206/2024 z 14 marca 2024 r. Maciej Terek – Główny specjalista Oddziału do spraw Informatyki w wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach – upoważnienie do kontroli nr 207/2024 z 14 marca 2024 r.
Termin przeprowadzenia kontroli:	Kontrola została przeprowadzona w dniu 15 marca 2024 r. w siedzibie Urzędu Gminy w Kijach.
Podstawa prawna do przeprowadzenia kontroli:	Kontrolę przeprowadzono na podstawie art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1], art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. *o Wojewodzie i Administracji rządowej w województwie*[2] oraz art. 25 ust.1 pkt 3 lit. a) ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[3]. Wystąpienie pokontrolne przekazano zgodnie z przepisami art. 47 ustawy o kontroli w administracji rządowej.
Ocena stanu faktycznego	Zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r.

[1] Dz. U. z 2020 r. poz. 224, dalej: Ustawa o kontroli w administracji rządowej.
[2] Dz. U. z 2023 r. poz. 190
[3] Dz. U. z 2024 r. poz. 307

wynikająca z ustaleń kontroli:

w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4] ocenie podlegały czynności podejmowane w trzech obszarach tematycznych:

1. system zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych,
2. realizacja działań z zakresu bezpieczeństwa informacji,
3. Zapewnienie dostępności w tym cyfrowej informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami zgodnie z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

Pozytywnie z nieprawidłowościami ocenia się prawidłowość działania systemów informatycznych używanych do realizowania zadań zleconych z zakresu administracji rządowej w Urzędzie Gminy w Kijach w okresie objętym kontrolą.

Ocena końcowa ustalona została na podstawie przedstawionych poniżej wniosków i oceny cząstkowej.

Kontrolą w przedmiotowym zakresie objęto systemy informatyczne używane do realizacji zadań zleconych z zakresu administracji rządowej tj.: SRP Źródło, CEIDG, Rejestr Wyborców oraz RESPONS(moduł Paliwa). W toku przeprowadzonej kontroli ustalono, że

1. **System zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych:**

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 1 i 2 Rozporządzenia KRI. Ustalono, że podstawowymi dokumentami z zakresu bezpieczeństwa informacji w Urzędzie Gminy w Kijach jest Polityka Ochrony Danych Osobowych stanowiąca załącznik nr 1 do zarządzenia nr 59/2021 Wójta Gminy Kije z dnia 12 sierpnia 2021 r. *w sprawie wprowadzenia Polityki Ochrony Danych Osobowych Wraz z późniejszymi aktualizacjami tj. wprowadzonymi zarządzeniem Wójta Gminy kije nr 120/2023 z 29 grudnia 2023 r.)*[5] oraz Instrukcja Zarządzania RODO stanowiąca załącznik nr 2 do ww. zaradzenia Wójta Gminy Kije[6].

Wspomniane regulacje obejmują swym zakresem głównie zagadnienia dotyczące ochrony danych osobowych. Nie zaobserwowano zapisów odnoszących się do wszystkich rodzajów przetwarzanych danych przez Urząd Gminy. Ponadto przyjęte w Gminie regulacje nie wykazują zbieżności z wytycznymi określonymi w Rozporządzeniu KRI – do których realizowania Gmina została zobowiązana. Można w nich znaleźć zagadnienia nawiązujące do treści Rozporządzenia KRI – jednak zdaniem kontrolujących – w zakresie niewystarczającym i niepełnym.

Z informacji udzielonej przez Administratora Sieci Informatycznej (dalej: ASI) wynika, że w najbliższej przyszłości zostaną podjęte działania zmierzające do wdrożenia pełnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI) mając na uwadze wytyczne

[4] Dz. U. z 2017 r., poz. 2247, dalej Rozporządzenie KRI

[5] dalej: PODO, Polityka

[6] Dalej: IZRODO

wskazane w Rozporządzeniu KRI w ramach realizacji projektu „Cyberbezpieczny Samorząd" .
Przedmiotowe regulacje załączono w formie skanów elektronicznych do akt kontroli (plik pn. „PODO" oraz „IZRODO").

Ocena cząstkowa badanego zagadnienia:

Pozytywnie z nieprawidłowościami ocenia się działalność Jednostki w przedmiotowym zakresie.

2. Realizacja działań z zakresu bezpieczeństwa informacji:

Zakres kontroli przedmiotowego zagadnienia został podzielony na dwanaście obszarów badawczych:

1. Analiza zagrożeń związanych z przetwarzaniem informacji.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 3 Rozporządzenia KRI. Ustalono, że zapisy PODO określają niezbędne zagadnienia, definicje oraz procedury związane z analizą ryzyka. W Polityce określono sposób szacowania ryzyka, skalę prawdopodobieństwa jego wystąpienia, skale przewidywanych skutków wystąpienia ryzyka oraz poziom ryzyka uznany za bezpieczny do realizacji (ryzyko akceptowalne). W dokumencie określono również częstotliwość wykonywania przedmiotowej analizy ryzyka.
Do kontroli przedłożono również *Analizę Ryzyka Ogólnego i Ocenę Skutków dla przetwarzanych danych w UG w Kijach* stanowiącą załącznik PODO-01 *Polityki Ochrony Danych Osobowych w UG w Kijach*. Zapisy tejże analizy wskazują, że została opracowana na potrzeby szczególnych danych – danych osobowych. Zauważyć należy jednak, że w ocenie kontrolujących czynności przetwarzania odnoszą się wyłącznie do danych osobowych. Podobny poziom ryzyka może wystąpić w odniesieniu również do danych innych niż dane osobowe, co należało również uwzględnić w przygotowanej analizie ryzyka.
Ponadto w § 14 wspomnianej Analizy – dotyczącym monitorowania i przegląd ryzyka, w punkcie punkt 1,2 i 3 opisano częstotliwość dokonywania przeglądów. Mimo prośby kontrolujących dokumentacja z przeglądów wykonywanych w latach wcześniejszych nie została przedstawiona do kontroli.
Przedmiotową Analizę załączono w formie skanów elektronicznych do akt kontroli (plik pn. „PODO" oraz „Analiza ryzyka").

2. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 2 Rozporządzenia KRI. Ustalono, że inwentaryzacja sprzętu i oprogramowania nie jest prowadzona w zakresie, o którym mowa w Rozporządzeniu KRI. Sprzęt komputerowy i oprogramowanie inwentaryzowane jest przy pomocy systemu antywirusowego, za którego pomocą administrator systemu informatycznego (dalej: ASI) sporządza wykaz sprzętu i oprogramowania. Taki sposób monitorowania wykorzystywanego sprzętu nie umożliwia prowadzenia aktualnej i pełnej inwentaryzacji urządzeń i systemów, o którą chodzi w KRI.
Ewidencja stworzona za pomocą programu antywirusowego nie obejmuje sprzętu, który funkcjonuje poza siecią Urzędu Gminy lub

niektórego sprzętu funkcjonującego w sieci Urzędu Gminy jak np.: switch, UTM, UPS czy serwer.

Wobec powyższego należy uznać, że przyjęty przez UG Kije sposób inwentaryzacji sprzętu i oprogramowania nie jest wystarczający w rozumieniu Rozporządzenia KRI.

Raport zawierający wykaz sprzętu i oprogramowania wygenerowany z systemu antywirusowego załączono w formie skanów elektronicznych do akt kontroli (folder pn. „pobrane dokumenty – UG Kije").

3. Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 4 oraz 5 Rozporządzenia KRI. Ustalono, że procedurę nadawania uprawnień do przetwarzania danych osobowych określa pkt 4 IZRODO. Zgodnie z procedurą nadawanie, modyfikacja i odbieranie uprawnień określonemu pracownikom Urzędu odbywa się zgodnie z załącznikiem pn. PODO-10, a także kartą obiegową określoną w załączniku pn. IZRODO-02 i IZRODO-03.

Kontroli poddano zlecenie nadania, zmiany, anulowania zakresu uprawnień użytkownika – PDOO-10, dla wybranej próby – czterech użytkowników Urzędu.

Ustalono, że:

- pierwsze zlecenie PODO-10 poddane kontroli (dla pracownika o inicjałach: P. K.) dotyczyło nadania a później anulowania uprawnień. Na druku brakowało podpisu bezpośredniego przełożonego lub innej upoważnionej osoby inicjującej złożenie zlecenia. Dokument nie zawierał daty przy podpisie Administratora Systemu Informatycznego. Dokument zawierający wymienione braki uniemożliwia identyfikację inicjatora zlecenia. Uniemożliwia również oszacowanie czasu podjętej reakcji od momentu złożenia zlecenia do momentu, w którym uprawnienia ostatecznie zostały nadane / odebrane użytkownikowi.
- zlecenie drugie PODO-10 poddane kontroli (dla pracownika o inicjałach: A. W.) dotyczyło zmiany uprawnień. Zlecenie nie zawierało podpisu Administratora Systemu Informatycznego. Dokument uniemożliwia identyfikację osiągniętego celu oraz określenia czasu w jakim został podjęty od momentu złożenia.
- zlecenie trzecie i czwarte PODO-10 poddane kontroli (dla pracownika o inicjałach I. N. H) dotyczy nadania uprawnień (dla pracownika o inicjałach N. S.) dotyczyły zmiany uprawnień. W obydwu przypadkach brakowało daty podpisu Administratora Systemu Informatycznego umożliwiającej oszacowanie czasu podjęcia reakcji od momentu złożenia zlecenia do momentu wprowadzenia zmian uprawnień użytkownikom.

Wobec powyższego zauważyć należy, ze każdy z druków PODO-10 przedłożonych do kontroli zawierał uchybienia względem procedury nadawania, odbierania czy modyfikacji tychże uprawnień przyjętej i obowiązującej w Urzędzie.

Druki PODO-10 poddane kontroli załączono w formie skanów

elektronicznych do akt kontroli (folder pn. „pobrane dokumenty – UG Kije").
Druki PODO-10 poddane kontroli załączono w formie skanów elektronicznych do akt kontroli (folder pn. „pobrane dokumenty – UG Kije").

4. Szkolenia pracowników zaangażowanych w proces przetwarzania danych.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 6 Rozporządzenia KRI. Kontrolowana Jednostka przedłożyła listy zrealizowanych szkoleń dla pracowników Urzędu w latach 2018 – 2023 w przedmiotowym zakresie zawierające również podpisy obecnych na szkoleniach pracowników. Kontrolowana Jednostka dołączyła również programy zrealizowanych szkoleń – określający ich ramowy zakres.
Zostały przedłożone listy szkoleń wraz z podpisami biorących w nich udział pracowników Urzędu z lat 2018-2023. Do list dołączono programy szkoleń, z których wynika zakres szkolenia.
W przedmiotowym zakresie nie stwierdzono uchybień i nieprawidłowości.
Wspomniane listy załączono w formie skanów elektronicznych do akt kontroli (folder pn. „pobrane dokumenty – UG Kije").

5. Praca na odległość i mobilne przetwarzanie danych.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 8 Rozporządzenia KRI. Ustalono, że obowiązująca IZRODO określa procedurę zabezpieczenia systemu informatycznego. Praca na odległość (poza budynkiem UM) opisana została w sześciu punktach. Ponadto procedura pracy zdalnej koreluje z załącznikiem nr 6 do IZRODO – Regulamin użytkowania komputerów przenośnych oraz nr 7 do IZRODO – Regulamin bezpieczeństwa podczas wykonywana pracy zdalnej w Urzędzie Gminy. Kontroli poddano wnioski dotyczące wykonywania pracy zdalnej poza budynkiem Urzędu jak też część protokołów dotyczących przekazania i zwrotu mienia – sprzętu komputerowego w związku z podjęciem pracy zdalnej.
Z informacji uzyskanej od Administratora Systemu Informatycznego wynika, że połączenia zewnętrznych firm są monitorowane i inicjowane przez ASI. Ponadto firmy zewnętrzne nie mają możliwości połączenia zdalnego z siecią Urzędu bez zgody ASI.

Przedmiotową Analizę załączono w formie skanów elektronicznych do akt kontroli (plik pn. „PODO" oraz „IZRODO").

6. Serwis sprzętu komputerowego i oprogramowania.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 10 Rozporządzenia KRI. Ustalono, IZRODO zawiera stosowne zapisy dotyczące wykonywania przeglądów i konserwacji urządzeń. Zapisy te wskazują rekomendacje dotyczące konserwacji, przeglądów i napraw sprzętu. Administrator Systemów Informatycznych potwierdził, że czynności te wykonywane są na podstawie zawartych umów z firmami zewnętrznymi. Kontrolującym przedłożono umowę zawartą z firmą ZETO SOFTWARE.

Kontrolujący wystąpili o przedstawienie równie innych umów w tym umowy dotyczącej obsługi serwisowej sprzętu wielofunkcyjnego oraz drukarek. Kontrolowany nie przedstawił tejże umowy. Z wyjaśnienia Administratora Systemów Informatycznych wynika, że urządzenia wielofunkcyjne i drukarki są naprawiane na bieżąco zgodnie z potrzebą – zaś umowa nie została zawarta (UG zawarł jedynie umowę na dostawę tonerów do druku).

Kontrolujący zalecają zawarcie umowy dotyczącej obsługi serwisowej sprzętu w tym drukarek i urządzeń wielofunkcyjnych.

Wspomniane procedury dotyczące przeglądów, konserwacji i napraw sprzętu komputerowego załączono w formie skanów elektronicznych do akt kontroli (folder pn. „pobrane dokumenty – UG Kije" IZRODO).

7. Procedury zgłaszania incydentów naruszenia Bezpieczeństwa Informacji.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 13 Rozporządzenia KRI. Ustalono, że PODO zawiera stosowne zapisy stanowiące Instrukcję Postępowania z Incydentami. Ponadto PODO zawiera skróconą instrukcje postępowania w przypadku naruszenia bezpieczeństwa danych osobowych.

Zauważyć należy, że zagadnienia z zakresu zgłaszania incydentów naruszenia bezpieczeństwa informacji zawiera jedynie PODO i dotyczą wyłącznie danych szczególnych – tj. danych osobowych. Instrukcja postępowania w przypadku naruszenia danych osobowych zawarta w PODO nie wskazuje osoby, której należy przekazać dotyczące wątpliwych zdarzeń i incydentów.

Przedmiotową Instrukcję załączono w formie skanów elektronicznych do akt kontroli (plik pn. „PODO").

8. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 14 Rozporządzenia KRI. Ustalono, że UG dysponuje dokumentacją dotyczącą przeprowadzonych audytów w latach 2019 – 2024. Kontrolujący poprosili o przedstawienie informacji audytowych z roku bieżącego oraz za rok poprzedni. W roku 2023 zadanie audytowe dotyczyło badania zgodności przetwarzania danych osobowych z przepisami rozporządzenia PE i RADY 679/2016, z przyjętymi w UG regulacjami. W roku bieżącym przeprowadzono zadanie audytowe pn. „Ocena wdrożenia i skuteczności funkcjonowania SZBI zgodnego z wymaganiami KRI".

Kontrolujący zwrócili uwagę na brak wskazania odpowiedniej podstawy prawnej w przedłożonych dokumentach tj. nie wskazano jako podstawy wdrożenia oraz późniejszego stosowania wiodącego aktu wykonawczego w tym zakresie – Rozporządzenia KRI.

Zadanie audytowe przeprowadzone w 2023 r. dotyczyło zgodności KRI – również i tam audytor nie powołał się na przepisy wiodące w tym zakresie tj. Rozporządzenie KRI.

Zdaniem kontrolujących zgodność Systemu Zarządzania Bezpieczeństwem Informacji przyjęty w jednostce z wytycznymi o których mowa w Rozporządzeniu KRI nie zachodzi w stopniu wystarczającym. Przyjęte w Jednostce regulacje dotyczą wyłącznie ochrony danych osobowych, nie nawiązując do Rozporządzenia KRI.

Według zespołu kontrolnego SZBI funkcjonujący w kontrolowanej jednostce nie jest zgodny z KRI, ponieważ istniejąca dokumentacja dotyczy wyłącznie ochrony danych osobowych i nigdzie nie powołuje się na KRI.

W świetle występujących uchybień na uwagę zasługuje fakt, że w raportach z wykonanych zadań audytowych nie sformułowano wniosków ani też uwag sugerujących powiązanie przedmiotowych dokumentów.

Przedmiotowe informacje załączono w formie skanów elektronicznych do akt kontroli (plik pn. Audyt 2019, Audyt 2021, Audyt 2022 oraz Audyt 2023).

9. Kopie zapasowe.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 12 Rozporządzenia KRI. Ustalono, że Instrukcja zarządzania RODO (IZRODO) zawiera procedurę tworzenia kopii zapasowych. Opisany jest sposób wykonywania kopii zapasowych, podany jest również harmonogram przechowywania oraz sposób zabezpieczenia kopii zapasowych. Wymieniona są osoby odpowiedzialne oraz osoby, które mają dostęp do kopii zapasowych. Administrator Systemu Informacji udostępnił informacje zawierające harmonogram wykonywania kopii zapasowych systemu Respons.

W kontrolowanym zakresie nie stwierdzono uchybień ani nieprawidłowości.

Przedmiotowe informacje załączono w formie skanów elektronicznych do akt kontroli (plik pn. backup policy.png, backup dane.png).

10. Bezpieczeństwo techniczno-organizacyjne dostępu do informacji.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 7, 9 oraz 11 Rozporządzenia KRI. Ustalono, że budynek Urzędu Gminy w Kijach posiada dwa wejścia zabezpieczone drzwiami z zamkiem. Na budynku rozmieszczone są kamery monitoringu wizyjnego. W budynku funkcjonuje system przeciwwłamaniowy, rozmieszczone są urządzenia systemu przeciwpożarowego, okna na parterze budynku zabezpieczone są kratami. Wejście do serwerowni zabezpieczone jest metalowymi drzwiami wyposażonymi w zamek wraz z elektrozamkiem. Pomieszczenie wyposażone jest w szafy dystrybucyjne, urządzenie systemu klimatyzacji, gaśnicę, urządzenie służące do pomiaru temperatury. System monitoringu wizyjnego przechowuje obraz przez co najmniej 14 dni. Wdrożona jest polityka kluczy, wskazano pomieszczenie, w którym przechowuje się klucze zapasowe do pomieszczeń.

W trakcie kontroli stwierdzono, że przyjęta Polityka kluczy nie zawiera szczegółowych regulacji w zakresie pobierania i zdawania kluczy do pomieszczeń, w których na co dzień przebywają pracownicy urzędu. Nie zostały określone zasady dotyczące zdawania i przekazywania kluczy właściwej osobie przed i po zakończeniu wykonywania pracy.

Przedłożono również dokument pn. „Ewidencja pobrań kluczy 2023". Dokument określa kwestię pobierania kluczy do poszczególnych pomieszczeń np., serwerownia, tablica rozdzielcza.

Kontrolującym nie przedstawiono upoważnień do pobrania kluczy do których zobowiązuje przyjęta zgodnie Polityka kluczy (pkt 3 Polityki).

Przedmiotowe informacje załączono w formie skanów elektronicznych do akt kontroli (plik pn. protokół oględzin pomieszczeń).

11. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.

Oceny stanu faktycznego dokonano zgodnie z §20 ust. 2 pkt 12, oraz ust. 4 Rozporządzenia KRI. Ustalono, że kontroler domeny Active Directory ma zainstalowany system Windows Serwer 2019. System RESPONS zainstalowany jest na serwerze z systemem Linux Debian (wersja 12.) Stacje robocze pracują na systemie operacyjnym Windows 10 i 11 oraz wyposażone są w system antywirusowy. Urządzenie UTM posiada aktualne licencje. Wdrożona jest polityka haseł zgodna z IZRODO.

W kontrolowanym zakresie nie stwierdzono uchybień ani nieprawidłowości.

Przedmiotowe informacje załączono w formie fotografii pulpitu i załączono do akt kontroli (plik pn. windows 2019, gpo dc, utm licencje, utm wersja).

12. Rozliczalność działań w systemach teleinformatycznych.

Oceny stanu faktycznego dokonano zgodnie z §21 ust. 2, 3 oraz 4 Rozporządzenia KRI. Ustalono, że System RESPONS odpowiedzialny m. in. za wsparcie współpracy z jednostkami odległymi w zakresie

sprawozdawczości budżetowej – posiada funkcjonalność monitorującą pracę użytkowników. Podobnie jest z systemami serwerowymi Windows Serwer 2019, Linux Debian 12 oraz systemami Windows zainstalowanymi na sprzęcie komputerowym użytkowanym przez pracowników Urzędu. Raporty danych historii aktywności użytkowników (tzw. Logi systemowe) są systematycznie gromadzone.
W trakcie kontroli ustalono, że Logi systemowe przechowywane są na tych samych maszynach, na których są wytwarzane. Nie ma procedury, narzędzi czy oprogramowania do systematycznego przeglądania logów systemowych co w efekcie końcowym skutkuje brakiem przeglądania logów a tym samym brakiem monitorowania zdarzeń.
Kontrolowana jednostka nie przedstawiła dokumentacji w przedmiotowym zakresie.
Dowód - akta kontroli plik: logi respons.png, logi utm.png
Do akt kontroli załączono pliki pn. logi respons, logi utm.

Ocena cząstkowa badanego zagadnienia:

Pozytywnie z nieprawidłowościami ocenia się działalność Jednostki w przedmiotowym zakresie.

3. Zapewnienie dostępności w tym cyfrowej informacji zawartych na stronach internetowych urzędów dla osób z niepełnosprawnościami zgodnie z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych:

Zakres kontroli przedmiotowego zagadnienia został podzielony na dwa obszary badawcze:

1. **Czy system teleinformatyczny spełnia wymagania WCAG 2.0 z uwzględnieniem poziomu AA, określonym w załączniku nr 4 do rozporządzenia KRI.**

Oceny stanu faktycznego dokonano zgodnie z §19 Rozporządzenia KRI. Ustalono, że połączenie ze stronami internetowymi Urzędu tj.: https://kije.pl oraz https://kije.biuletyn.net realizowane jest poprzez protokół https. Obie strony zostały przetestowane za pomocą oprogramowania NVDA (czytnik ekranu), Color Contrast Analyser CCA, https://validator.utilitia.pl zostały również wyświetlone w przeglądarce FireFox i EDGE oraz na telefonie.
Na stronie https://kije.pl umieszczono stronę (popup) z życzeniami świątecznymi „Wesołego Alleluja". Nie ma możliwości zamknięcia i wyłączenia strony przy pomocy klawiatury, co czyni cały serwis niedostępnym, ponieważ strona z życzeniami zasłania zamieszczone na stronie informacje. Brak możliwości wyłączenia dźwięku przy pomocy klawiatury. Ponadto zaobserwowano nieaktywne pozycje w panelu ustawienia dostępności (prawdopodobnie przez stronę popup).
Brak wyróżnienia aktywnego obiektu:
- „zadaj pytanie wójtowi",
- „druki do pobrania",
- „komunikaty i ogłoszenia",
- „komunikaty zdrowotne",

Brak możliwości przejścia do górnego menu:
- Gmina,
- dla mieszkańca,
- dla przedsiębiorcy,
- dla turysty,

– projekty,

co powoduje, że duża część informacji jest niedostępnych. Podobnie wygląda dostępność menu po lewej stronie witryny: aktualności, ogłoszenia, sport, kultura, oświata, seniorzy, inwestycje, komunikaty zdrowotne, praca i pomoc społeczna.

Strony E-urzędu dalej platforma mieszkańca. Zakładanie nowego konta w pozycji „rodzaj zamieszkania" brak możliwości wyboru za pomocą klawiatury dostępnych opcji (miasto, wieś). Po zalogowaniu się do e-usług brak możliwości wyboru tych usług: usługi obywatela, usługi firmy, usługi instytucji, usługi podmiotu publicznego. Praktycznie usługi nie są dostępne.

Na stronie https://kije.biuletyn.net nie stwierdzono informacji dot. skrytki korespondencyjnej epuap Urzędu Gminy w Kijach. Jest tylko ogólny link do platformy.

Mając powyższe na uwadze, należy stwierdzić, że strona internetowa urzędu: https://kije.pl jest niedostępna dla osób posługujących się czytnikiem ekranu i klawiaturą.

2. Czy sporządzono i opublikowano deklarację dostępności oraz zawarto w deklaracji dostępności elementy wskazane w art. 10 ust. 3-5 ustawy dla stron internetowych podmiotu.

Oceny stanu faktycznego dokonano zgodnie z §10 ust. 3, 4 i 5 Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych[7].

Ustalono, że obydwie kontrolowane strony posiadają stosowne deklaracje dostępności:

- https://kije.biuletyn.net – Deklaracja dostępności aktualizowana w roku 2020 (data ostatniej istotnej aktualizacji), metryczka wskazuje na 2024 r.
- https://kije.pl – aktualizowana w 2024 r.

Ocena cząstkowa badanego zagadnienia:

Negatywnie ocenia się działalność Jednostki w przedmiotowym zakresie.

Wnioski, zalecenia oraz dodatkowe informacje:

Reasumując poczynione ustalenia, zwracam się z prośbą do Pana Wójta o niedopuszczenie do powstania nieprawidłowości wykazanych w toku kontroli w przyszłej działalności w podległej Panu Jednostce. Wobec powyższego sformułowano następujące zalecenia:

1. Zrealizować plany wdrożenia pełnego SZBI zgodnie z wytycznymi wskazanymi w Rozporządzeniu KRI w ramach realizacji projektu „Cyberbezpieczny Samorząd".
2. Rozszerzyć zakres dokumentacji ochrony danych, tak aby obejmowała wszystkie dane przetwarzane w Jednostce.
3. Systematycznie przeprowadzać analizę ryzyka utraty integralności, dostępności i poufności informacji obejmującą wszystkie wymagane dane, a nie jedynie dane osobowe.
4. W miarę możliwości prowadzić aktualną i pełną inwentaryzację urządzeń i systemów, o którą chodzi w KRI, obejmującą wszystkie urządzenia uczestniczące w przetwarzaniu informacji.

[7] Dz. U. z 2023 r. poz. 1440

5. Zapewnić, aby zarządzanie uprawnieniami do pracy w systemach informatycznych odbywało się zgodnie z zasadami opisanymi w IZRODO i posiadało atrybuty rozliczalności, takie jak daty wykonania czynności i podpisy osób w nie zaangażowanych.
6. Uszczegółowić procedurę zgłaszania incydentów naruszenia bezpieczeństwa informacji, tak aby dotyczyły wszystkich danych i wskazać osobę, której zgłasza się zdarzenia i incydenty.
7. Zaleca się, aby raporty z audytów bezpieczeństwa informacji zawierały wnioski i zalecenia dotyczące obszarów poddanych audytowi.
8. Uszczegółowić Politykę Kluczy, w tym określić zasady dotyczące zdawania i przekazywania kluczy właściwej osobie przed i po zakończeniu wykonywania pracy.
9. W miarę możliwości przechowywać logi systemowe na innych urządzeniach niż te, na których są one wytwarzane.
10. Zapewnić, aby strony internetowe Jednostki były w pełni dostępne za pomocą klawiatury.

Ponadto rozważyć należy możliwość zawarcia umowy dotyczącej obsługi serwisowej sprzętu w tym drukarek i urządzeń wielofunkcyjnych, uwzględniając możliwości finansowe Jednostki.

Jednocześnie na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę poinformować Wojewodę Świętokrzyskiego w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz o wykonaniu zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Ponadto informuję, iż zgodnie z art. 48 ustawy o kontroli w administracji rządowej od niniejszego wystąpienia pokontrolnego nie przysługują środki odwoławcze

Michał Skotnicki
Wicewojewoda Świętokrzyski