WOJEWODA ŚWIĘTOKRZYSKI

Znak: OK.V.431.5.2021

Kielce, dnia 14-01-2022

Pan Bogdan Wenta
Prezydent Miasta Kielce

Wystąpienie pokontrolne

Kontrolę w Urzędzie Miasta Kielc Rynek 1 w dniach 7-9 grudnia 2021 roku przeprowadził zespół kontrolerów w składzie:

Marek Rak - Główny specjalista Oddziału ds. Informatyki w Wydziale Organizacji i Kadr ŚUW, na podstawie pisemnego upoważnienia do przeprowadzenia kontroli numer 807/2021 z dnia 02.12.2021 r. wydanego z upoważnienia Wojewody Świętokrzyskiego przez Dyrektora Wydziału Organizacji i Kadr.

Maciej Terek - Główny specjalista Oddziału ds. Informatyki w Wydziale Organizacji i Kadr ŚUW, na podstawie pisemnego upoważnienia do przeprowadzenia kontroli numer 808/2021 z dnia 02.12.2021 r. wydanego z upoważnienia Wojewody Świętokrzyskiego przez Dyrektora Wydziału Organizacji i Kadr.

Zakres kontroli i okres objęty kontrolą:

Zakres kontroli obejmował działanie systemów teleinformatycznych używanych do realizacji zadań publicznych w okresie od 1.01.2017 do dnia kontroli. Zgodnie z Rozporządzeniem 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 dnia 16 maja 2012 r. poz. 526) wydanym na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565, z późn. zm.), ocenie podlegały trzy główne obszary tematyczne:

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

2) System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

3) Zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób z niepełnosprawnościami.

Wykonywanie zadań w kontrolowanym zakresie oceniam pozytywnie z uchybieniami i nieprawidłowościami.

W wyniku przeprowadzonej kontroli ustalono, że:

USTALENIA KONTROLI	
Akty prawne, na podstawie których dokonano ustaleń w toku kontroli	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
Obszar kontroli : **1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie usług drogą elektroniczną**	
1.1 usługi elektroniczne	
Podstawa prawna	§ 5 ust.2 pkt.1 i pkt.4 rozporządzenia : Interoperacyjność na poziomie organizacyjnym osiągana jest przez : • pkt.1 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 • pkt.4 Publikowanie i aktualizowanie w BIP przez przedmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Na stronie BIP Urzędu w zakładce „Sposoby przyjmowania i załatwiania spraw" opublikowane zostały karty usług wraz ze wzorami dokumentów. Została zamieszczona również instrukcja obsługi BIP, mapa strony, deklaracja dostępności wraz z raportem oraz zakładka z informacjami o dostępie do informacji publicznej.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.2 centralne repozytorium wzorów dokumentów elektronicznych	
Podstawa prawna	**Art. 19 b 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 bezpiecznym podpisem elektronicznym.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Urząd Miasta Kielce (UM) w latach 2013 i 2017 opublikował łącznie 16 wzorów dokumentów elektronicznych w Centralnym Repozytorium Wzorów Dokumentów Elektronicznych. Na stronie BIP w zakładce „Sposoby przyjmowania i załatwiania spraw" opublikowane zostały także karty usług wraz ze wzorami dokumentów. Dowód : Strona CRWDE, Strona BIP miasta Kielce
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**

1.3 Model usługowy	
Podstawa prawna	**§ 15 ust. 2 rozporządzenia:** Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W menu górnym w zakładce „Przydatne" znajduje się link do Portalu mieszkańca . Portal został uruchomiony w roku 2017. Dane do logowania otrzymał każdy właściciel, dzierżawca nieruchomości w piśmie z UM (login z hasłem). Można dokonać rozliczenia, jest dostępny dokładny adres nieruchomości, punk wywozu śmieci, zestawienia rozliczeń za usługi, historie odbioru pojemników, ilość odebranych śmieci. Zarządzanie usługami realizowanymi przez systemy informatyczne odbywa się w oparciu o procedury zawarte w Polityce Postępowania z Danymi Osobowymi. Każdy system i usługa wykorzystywana w UM ma określonego administratora, zastępcę administratora, gospodarza, zastępcę gospodarza oraz informatyka. Dowód - akta kontroli plik: pobrane-dokumenty-UM-Kielce.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.4 Współpraca systemów informatycznych z innymi systemami	
Podstawa prawna	**§ 5 ust. 3 pkt 3 rozporządzenia:** Interoperacyjność na poziomie semantycznym osiągana jest przez, m.in. stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań. **§ 16 ust. 1 rozporządzenia:** Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	**e-SOD** (Elektroniczny System Obiegu Dokumentów) aplikacja umożliwiająca obsługę korespondencji wychodzącej i przychodzącej posiada możliwość integracji z innymi systemami. **OTAGO** kilkadziesiąt współpracujących z sobą aplikacji (UM wdrożył 29 aplikacji/podsystemów), poprzez dedykowany moduł system współpracuje z rejestrem PESEL, systemem Źródło, TERYT (GUS), wymiana danych z systemami bankowości . Integracja realizowana jest za pomocą modułu EludSrpKlient służącego do komunikacji z web service SRP na potrzeby aktualizacji Rejestru Mieszkańców. Jest to specjalny moduł pobierający dane w bezpiecznym kanale komunikacji z autoryzacją za pomocą certyfikatu wydanego przez MSWiA dla Gminy. Wymiana danych z systemami bankowości odbywa się za pomocą plików tekstowych (eksport i import danych). System OTAGO poprzez moduł JPK

	generuje JPK (jednolity plik kontrolny do celów podatkowych), a poprzez moduł SZYNA odbywa się komunikacja z innymi usługami. **SOWA** (System Obiegu Wniosków Administracyjnych) powiązany jest z Ewidencją Gruntów i Budynków (EGIB) stanowiącą część GEO-INFO, Ewidencją Miejscowości, Ulic i Adresów (EMUiA) oraz Systemem Otago (Rejestr mieszkańców, Generalny Rejestr Umów). **SIP GEO-INFO** (powiatowy zasób geodezyjny i kartograficzny, geodezyjna ewidencja sieci uzbrojenia terenu) powiązany jest z Internetowym Serwerem Danych Przestrzennych (ISDP) oraz Systemem Obsługi Wniosków Administracyjnych (SOWA) **ŹRÓDŁO** (Ewidencja ludności) zarejestrowane dane są przesyłane do systemów lokalnych OTAGO w części dotyczącej mieszkańców miasta Kielce. **CEIDG** (Centralna Ewidencja i Informacja o Działalności Gospodarczej) przesyła dane do Urzędu Skarbowego, ZUS, KRUS,GUS. CEIDG korzysta z informacji zawartych w rejestrach publicznych w zakresie danych objętych wnioskiem o wpis do CEIDG, w szczególności w celu weryfikacji danych wpisanych do CEIDG. Dowód - akta kontroli plik: Załącznik 2 – zbiorówka.xlsx
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.5 Obieg dokumentów w urzędzie	
Podstawa prawna	**§ 20 ust. 2 pkt 9 rozporządzenia:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególność 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.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Obieg dokumentów w UM Kielce jest realizowany w sposób tradycyjny. Do wspomagania papierowego obiegu dokumentów jest wykorzystywany system e-SOD wyłącznie w zakresie rejestru korespondencji.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
1.6 Formaty danych udostępniane przez systemy informatyczne	
Podstawa prawna	**§ 17 ust. 1 rozporządzenia:** Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą. **§ 18 ust. 1 rozporządzenia:** Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2

	do rozporządzenia. **§ 18 ust. 2 rozporządzenia:** Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Wzory dokumentów publikowane są w formatach DOC, DOCX, RTF oraz PDF.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
Ocena obszaru kontroli nr 1	**Pozytywna**
Obszar kontroli : **2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych**	
2.1 Dokumenty z zakresu bezpieczeństwa informacji . Zaangażowanie kierownictwa podmiotu	
Podstawa prawna	**§ 20 ust. 1 rozporządzenia:** 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:** 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:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Głównym dokumentem z zakresu bezpieczeństwa informacji jest Polityka Postępowania z Danymi Osobowymi (PPzDO) stanowiąca załącznik do Zarządzenia 194/2019 Prezydenta Miasta Kielce z dnia 28 maja 2019r. Polityka ta została wydana dnia 3 czerwca 2019 roku. W instrukcji numer 1 do PPzDO dość często wymieniane jest stanowisko Inspektora ds. bezpieczeństwa który odpowiedzialny jest za realizację wielu procedur opisanych w PPzDO. 1. Rozdział 5 nadawanie lub odbieranie uprawnień pracownikom UM patrz punkt 5.14 cytuję „Inspektor ds. bezpieczeństwa aktualizuję listę osób upoważnionych do przebywania na terenie UM po godzinach pracy bez przepustki” 2. Podobna sprawa jest w tym samym rozdziale w punkcie 5.15 jak również w rozdziale 6 patrz punkt 6.2-6.5 dalej 6.8 3. Rozdział 11 przegląd zasobów i uprawnień patrz punkt 11.3 Stanowisko Inspektora ds. bezpieczeństwa przewija się w całej

	dokumentacji wdrożonej zarządzeniem 194/2019. Zapewne w momencie wdrożenia Zarządzenia 194/2019 stanowisko Inspektora ds. bezpieczeństwa było obsadzone natomiast w przedziale czasowym 2019-2021 stanowisko straciło obsadę (stanowisko jest w strukturze UM) natomiast brakuje informacji kto podczas braku obsady Inspektora ds. bezpieczeństwa pełni jego funkcję, obowiązki, kto go fizycznie zastępuję. Brak jest tej informacji w PPzDO. Część obowiązków Inspektora ds. bezpieczeństwa przejął „nieoficjalnie" IOD i na tyle ile starcza mu sił i środków stara się je wykonywać. Należałoby przejrzeć PPzDO i dokonać aktualizacji związanych ze stanowiskiem Inspektora ds. bezpieczeństwa i jego obowiązkami. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf
Ustalone nieprawidłowości	Dokumentacja PPzDO nie była aktualizowana na przestrzeni lat 2019-2021. W UM w latach 2019-2021 zachodziły liczne zmiany, natomiast PPzDO nie nadążała za tymi zmianami co w efekcie końcowym doprowadziło do tego, że UM w czasie kontroli miał nieaktualną dokumentację z zakresu bezpieczeństwa informacji (patrz KRI § 20 punkt 2, ust 1). Ponadto dokumentacja ta dotyczy jedynie ochrony szczególnych danych jakimi są dane osobowe, natomiast zbiór danych przetwarzanych, gromadzonych w UM jest znacznie szerszy i również powinien podlegać ochronie a sposób ochrony tych danych powinien być ujęty w wyżej wymienionej dokumentacji.
2.2 Analiza zagrożeń związanych z przetwarzaniem informacji	
Podstawa prawna	§ 20 ust. 2 pkt 3 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolnemu została przedłożona dokumentacja a dokładnie załącznik numer 3 do instrukcji numer 4 zatytułowany „Analiza ryzyka dla danych osobowych przetwarzanych w Urzędzie" z podziałem na poszczególne wydziały i czynności. Dokumentacja jest z roku 2020. Poddano wówczas analizie czynności przetwarzania danych osobowych w poszczególnych wydziałach i biurach urzędu. Została określona wartość ryzyka dla ADO i dla podmiotu danych. Dla wszystkich czynności przetwarzania danych osobowych w UM określono poziom ryzyka jako małe (zakres wartości 1-4) czyli ryzyko tolerowane. Zgodnie z postanowieniami Instrukcji numer 4 z PPzDO raz w roku Inspektor ds. bezpieczeństwa (którego obecnie stanowisko co najmniej od 6 miesięcy jest nie obsadzone) ma przeprowadzić testy wraz

	z Obsługą informatyczną wszystkich zabezpieczeń informatyczno-technicznych które maja wpływ na przetwarzanie danych osobowych. Po przeprowadzeniu testów powinien zostać sporządzony raport który powinien być przedłożony Prezydentowi. Brak dokumentacji w tym zakresie. Brakuje dokumentu a dokładnie załącznika numer 3 Plan minimalizacji ryzyka do Instrukcji numer 4. Dowód - akta kontroli plik : Zał nr 3 - analiza ryzyka 2020.pdf Instrukcja_nr_4-Analiza_ryzyka_ODO.docx
Ustalone uchybienia	Analiza ryzyka dla danych osobowych przetwarzanych w UM jest w instrukcji nr 4 opisana jako załącznik nr 2. Przedłożony załącznik jest opisany ręcznie jako załącznik numer 3. Według Instrukcji nr 4 – Analiza ryzyka ODO załącznik numer 3 do instrukcji to „Plan minimalizacji ryzyka", którego brak. Nie obsadzone jest stanowisko Inspektora ds. bezpieczeństwa, który jest odpowiedzialny za część czynności w procesie zarządzania ryzykiem .
2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego	
Podstawa prawna	**§ 20 ust. 2 pkt 2** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolnemu została przedłożona próbka dwudziestu metryczek sprzętu komputerowego w formie elektronicznej. Metryczki wygenerowane zostały przez oprogramowanie eAuditor. Zawierają szczegółowe informacje na temat sprzętu komputerowego (procesor, dysk, bios, karty graficznej), adresy ip, mac, zainstalowany system, oprogramowanie. Przedłożono również w formie papierowej dokumentację „Przeniesienie środka trwałego" (wydruk z systemu OTAGO) dotyczącą sprzętu komputerowego (metryczki tego sprzętu komputerowego zostały udostępnione w formie elektronicznej mowa o nich jest powyżej) z których można wyczytać informacje kto jest aktualnie użytkownikiem tego sprzętu, etykietę, w jakim wydziale/pokoju pod jakim adresem znajduje się fizycznie sprzęt komputerowy którego dotyczy przedłożona dokumentacja oraz lokalizację sprzętu przed zmianą. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych	
Podstawa prawna	**§ 20 ust. 2 pkt 4:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. 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** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Cała procedura nadawania/odbierania/modyfikacji uprawnień w systemach informatycznych pracujących w UM Kielce jest realizowana w systemie EMU (autorski system UM Kielce). Począwszy od wniosku Dyrektora inicjującego nadanie/odebranie uprawnień, poprzez odpowiednich Administratorów którzy zatwierdzają wniosek, informatyków, gospodarzy czy koordynatorów, którzy fizycznie nadają/odbierają/modyfikują uprawnienia w systemach informatycznych. Po wykonaniu przypisanych czynności każda z wyżej wymienionych osób realizujących wniosek jest zobowiązana do potwierdzenia w systemie EMU ich wykonanie. IOD przedstawił działanie systemu, jego możliwości odnośnie ewidencji historii wniosku o nadanie/odebranie/modyfikacji uprawnień na wybranym przez siebie stanowisku i użytkowniku. IOD przedłożył załącznik numer 4 do instrukcji numer 1 czyli Rejestr systemów informatycznych w UM Kielce. Trzeba dodać iż cały proces nadawania/odbierania/modyfikacji uprawnień w systemach informatycznych w UM został przeniesiony do systemu autorskiego EMU. Oprogramowanie zaprojektowane zostało w sposób umożliwiający ciągłą, bieżąca kontrolę nadanych uprawnień praktycznie „od ręki" co nadaje całemu procesowi, procedurze atrybuty autentyczności, rozliczalności, niezawodności i niezaprzeczalności. System robi „wrażenie" a trzeba podkreślić, że jest systemem autorskim rozwijanym przez pracowników UM. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji	
Podstawa prawna	**§ 20 ust. 2 pkt 6** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. 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.
Ustalenie stanu faktycznego, stanowiące	Zespołowi kontrolnemu została przedłożona dokumentacja (listy obecności z podpisami osób biorących udział w szkoleniu) ze szkoleń

podstawę do oceny	z zakresu „Ochrony Danych Osobowych "przeprowadzonych w roku 2020. Brak dodatkowych szkoleń dla osób które z różnych przyczyn nie wzięły udziału w szkoleniach głównych. Zespołowi kontrolnemu nie została przedłożona dokumentacja ze szkoleń z roku 2019 i ewentualnych szkoleń z roku 2021. Brak szkoleń z zakresu PPzDO. Co prawda każdy pracownik przynajmniej raz zapoznał się z PPzDO ale w większości przypadkach było to 3 lata temu. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf
Ustalone uchybienia	Brak dowodów na realizację szkoleń z zakresu PPzDO. Brak doraźnych szkoleń z zakresu zagrożeń bezpieczeństwa informacji (phishing, stosowanie zabezpieczeń), chyba że takie doraźne szkolenia, ostrzeżenia prowadzą ASI. Brak dokumentacji w tym zakresie.
2.6 Praca na odległość i mobilne przetwarzanie danych	
Podstawa prawna	**§ 20 ust. 2 pkt 8:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zasady bezpiecznej pracy mobilnej zostały zapisane w PPzDO w rozdziale 15 „Praca z urządzeniami przenośnymi oraz nośnikami danych". Jeżeli chodzi o pracę zdalną to została ona opisana w rozdziale 14 jedynie w odniesieniu do przypadków serwisowania programów informatycznych przez firmy zewnętrzne. W przypadku oprogramowania OTAGO podpisana została umowa „na świadczenie usług i asysty technicznej i konserwacji" w której zdefiniowano parametry zdalnego, bezpiecznego, stabilnego dostępu do zasobów UM (bardzo ogólnie ale może to i dobrze) na których zainstalowany został system OTAGO. W pozostałych przypadkach zapewne ASI zgodnie z PPzDO ma obowiązek ustawić „odpowiednie kanały łączności pomiędzy firmą świadczącą umowę a Urzędem". W umowie z HyperView Sp. z o.o. jest zapis w § 5, „Obowiązki zamawiającego", który brzmi: „zamawiający zezwoli na zdalny dostęp poprzez wykonanie szyfrowanego łącza internetowego do serwerów na których znajduje się MSIP" ASI jest prawdopodobnie w stanie z logów „wyciągnąć" połączenia zdalne i na ich podstawie odpowiedzieć kiedy na jak długo i kto łączył się z urządzeniami UM, ale na bieżąco nie jest wstanie odpowiedzieć czy w danej chwili jakaś firma zewnętrzna korzysta z połączenia zdalnego. W PPzDO w rozdziale 14 „ Dostęp do sieci informatycznej oraz

	serwerów Urzędu" punkty 14.6-14.7. wymieniona jest osoba inspektora ds. bezpieczeństwa, której uprawnienia w tym zakresie wyglądają na strategiczne a jak stanowisko to nie jest obsadzone. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf
Ustalone uchybienia	Zasady pracy na odległość dotyczą wyłącznie przypadków serwisowania programów informatycznych przez firmy zewnętrzne.
2.7 serwis sprzętu komputerowego i oprogramowania	
Podstawa prawna	**§ 20 ust. 2 pkt 10:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zespołowi kontrolującemu została udostępniona umowa z firmą Asseco na świadczenie usług asysty technicznej i konserwacji systemu OTAGO. Do umowy została dołączona umowa „Powierzenia danych osobowych" do której dołączono załącznik numer 1 w którym określono zakres, rodzaj danych osobowych oraz kategorie osób, które powierzono Przetwarzającemu. Instrukcja numer 12 do PPzDO zawiera opisane czynności jakie mają być wykonywane w przypadku wykonywania prac na obszarze UM przez pracowników firm zewnętrznych. Wyszczególniony jest przypadek wykonywania prac na terenie strefy I. Podczas oględzin zespół kontrolny sprawdził prowadzenie „Ewidencji osób przebywających w I strefie bezpieczeństwa" (patrz protokół oględzin). Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf Protokol_ogledzin_pomieszczen.docx
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.8 Procedury zgłaszania incydentów naruszenia BI	
Podstawa prawna	**§ 20 ust. 2 pkt 13:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określonym i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	PPzDO zawiera rozdział 27 w którym opisano procedurę postepowania w przypadku naruszenia bezpieczeństwa. Dodatkowo załącznik numer 2 do PPzDO „Obsługa problemów bezpieczeństwa" zawiera procedury, instrukcję postępowania z problemami IT, problemami z systemem OTAGO oraz naruszeniem ochrony danych osobowych. Zespół kontrolny zwrócił uwagę na punkt 27.3. Zapisano w nim, że

	przypadek braku klucza, otwartego okna w pomieszczeniu, przebywania pracownika bez odpowiednich uprawnień lub inne problemy związane z bezpieczeństwem zgłaszane są bezpośrednio do Inspektora ds. bezpieczeństwa (wiemy że od pewnego czasu stanowisko nie jest obsadzone personalnie). Podobna sytuacja powtarza się w załączniku numer 2 Obsługa problemów bezpieczeństwa (patrz 2.5). Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf Polityka_Postępowania_z_Danymi_Osobowymi.docx
Ustalone uchybienia	Zasadniczy problem to brak obsadzenia stanowiska inspektora ds. bezpieczeństwa, który jest wymieniony w dokumentacji i który ma określone obowiązki. Stan ten świadczy o tym, że dokumentacja we tym zakresie nie była aktualizowana.
2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji	
Podstawa prawna	**§ 20 ust. 2 pkt 14:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zarządzeniem 194/2019 z maja 2019 roku wprowadzono nową PPzDO wraz z instrukcją numer 3 dotyczącą audytów (audyt w roku 2019 został przeprowadzony16 grudnia 2019) . Dokument ten zawiera opis dotyczący procedur związanych z planowaniem (załącznik numer 1 plan audytów wraz ze zbiorczym raportem), przeprowadzeniem (załącznik numer 2 zawiadomienie o audycie) oraz raportowaniem po audytowym (załącznik numer 3 karta niezgodności jeżeli jakieś niezgodności były oraz załącznik numer 4 raport z audytu). Zespołowi kontrolnemu przedłożono w postaci elektronicznej dokumentację z przeprowadzonych audytów BI z lat 2017-2020. Prawdopodobnie są to raporty po audytowe podpisane przez powołany zespół audytowy. Forma tych raportów nie jest zgodna ze wzorem opublikowanym w PPzDO z tego samego roku (patrz załącznik numer 4 do instrukcji numer 3). Oczywiście formularz jest tylko formularzem, wzór jest tylko wzorem ale świadczy o tym iż sam zespół audytorów nie stosował się do zapisów z PPzDO. Jednym z zagadnień audytów z lat 2019-2020 jest „stosowanie się pracowników UM Kielce do zapisów obowiązujących w UM Kielce instrukcji, ze szczególnym uwzględnieniem zapisów zawartych w PPzDO…". Pisze to zespół kontrolny, który sam nie stosował się do zapisów instrukcji w PPzDO UM Kielce. Dodam, że w trakcie przeprowadzonych audytów z lat 2018-2020 nie stwierdzono naruszeń obowiązujących przepisów. Instrukcja numer 3 jest dość szczegółowa i jasna. W punktach 7.1-7.2 są zapisy mówiące o identyfikacji dokumentów związanych z audytem. Brak kompletnie opisanych parametrów w przedłożonej dokumentacji. Kontrolujący zwrócili uwagę na audyt z roku 2020, gdzie ówczesny IOD Pani ABM na „raporcie" opisana jest jako ABI (stosowany nadal stary wzór raportu z 2018 roku) natomiast pieczęć jest IOD. Oczywiście dane zawarte w przedłożonym raporcie i we

	wzorze zawartym w instrukcji numer 3 są w jakimś procencie tożsame. Natomiast świadczą o tym, że przynajmniej zespół audytorów w latach 2019-2020 jeżeli chodzi o dokumentację po audytową nie stosuje się do instrukcji zawartych w PPzDO. Zespół kontrolny stwierdza, iż ustalenia w wyniku audytów z lat 2019-2020 mijają się z prawdą (patrz uchybienia zawarte w niniejszym dokumencie).Pojawia się pytanie czy audyt w takim składzie osobowym jak w latach 2019-2020 ma sens i czy wnosi coś konstruktywnego, czy wnosi jakąś wartość dodaną do ochrony danych w urzędzie. Podobnie ma się sprawa z IOD który jest zobowiązany poprzez PPzDO do prowadzenia załącznika numer 1 do Instrukcji numer 3 oraz do sporządzenia raportu po audytowego i przedłożenia raportu Prezydentowi. Brak dokumentacji w tym zakresie. (Zespół kontrolny ma na uwadze iż w ówczesnym czasie obowiązki IOD pełniła inna osoba). Co prawda za rok 2021 IOD przedłożył dokumentację związaną z Audytem czyli plan audytu na rok 2021 oraz zawiadomienia wysłane do Kierowników Komórek Organizacyjnych. Audyt był zaplanowany na I i II półrocze roku 2021, ale nie został przeprowadzony w zaplanowanym terminie. Brak dokumentacji w tym zakresie. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf
Ustalone uchybienia	Zespoły audytowe nie stosują się do zapisów z instrukcji nr 3. Przedłożona dokumentacja z audytów jest wątpliwej jakości. Audyt zaplanowany na I i II półrocze 2021 nie został przeprowadzony w zaplanowanym terminie.
2.10 Kopie zapasowe	
Podstawa prawna	**§ 20 ust. 2 pkt 12 lit. b:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. minimalizowanie ryzyka utraty informacji w wyniku awarii.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Kopie zapasowe wykonywane są codziennie (pełne kopie) i przechowywane są na dyskach urządzeń wchodzących w skład infrastruktury informatycznej UM. Kopie przechowywane są w dwóch lokalizacjach. Dział IT nie wykonuje kopii na nośniki zewnętrzne. Natomiast z przeprowadzonej rozmowy z ASI wynika, że ASI testują kopie odtwarzając je produkcyjnie, jak również na bieżąco sprawdzają pobieżnie czy wykonane kopie nie są np. „zerowe". Nie prowadzą natomiast żadnej dokumentacji w tym zakresie. Testy kopii zapasowych przeprowadzane są raz w roku a wynika to z zapisów dotyczących ciągłości działania UM. Dokumentacja w tym zakresie została przedłożona zespołowi kontrolującemu. Przedłożone protokoły z testowania ciągłości działania z lat 2019-2021 nie zawierają informacji na temat wyniku testów, choć w samym

	formularzu jest zaprojektowane miejsce na taką informację. Z tego powodu nie wiemy jakim rezultatem zakończyły się testy ciągłości działania. Brak informacji strategicznej, jaki jest wynik testu ma bezpośrednie przełożenie na ciągłość działania UM. Nie wiemy czy ciągłość działania jest zachowana, utrzymana czy należy dokonać jakiś korekt organizacyjnych, technicznych aby tą ciągłość działania osiągnąć lub utrzymać. Punkt 9.2 z PPzDO nie jest realizowany. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf
Ustalone uchybienia	Wybiórcze przestrzeganie zapisów, procedur zdefiniowanych w PPzDO. Brak wyników testów w protokołach z testowania planu ciągłości.
2.11 Projektowanie, wdrażanie i eksploatowanie systemów teleinformatycznych	
Podstawa prawna	**§ 15 ust. 1 rozporządzenia:** 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.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W instrukcji nr 1 do PPzDO pn. Zarządzanie uprawnieniami w punkcie 10 opisano zasady zakupu zasobów lub programów informatycznych. Zespół kontrolny zapoznał się z funkcjonowaniem następujących systemów informatycznych: - EMU aplikacja autorska UM - HelpDesk aplikacja autorska UM - OTAGO Zintegrowany System Wspomagania Zarządzania Miastem, składa się z kilkudziesięciu aplikacji zestawione w jeden zintegrowany system. Współpraca z wieloma systemami. - SOWA System obsługi wniosków aplikacyjnych (Ministerstwo Funduszy i Polityki Regionalnej) - ŹRÓDŁO to bezpłatna aplikacja ogólnopolska służąca do obsługi Systemu Rejestrów Państwowych. - SIP GEO-INFO powiatowy zasób geodezyjny i kartograficzny, geodezyjna ewidencja sieci uzbrojenia terenu - CEIDG Centralna Ewidencja i Informacja o Działalności Gospodarczej
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.12 Bezpieczeństwo techniczno-organizacyjne dostępu do informacji	
Podstawa prawna	**§ 20 ust. 2** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in.: **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:** zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. **pkt 11 rozporządzenia:** ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W budynku UM (lokalizacja Rynek 1) wydzielone zostały trzy strefy bezpieczeństwa (przedłożony został wykaz strefy I i IA) wraz wchodzącymi w skład strefy pokojami. W pokoju ASI znajduje się prowadzona od roku 2008 książka „Ewidencja osób przebywających w strefie I ". Zabezpieczenia wejścia do strefy I, zabezpieczenia wybranych pomieszczeń oraz głównego wejścia do budynku zostały opisane w protokole oględzin z dnia 8 grudnia 2021 roku. Przeglądy centralnego UPS'a wykonywane są przez firmę zewnętrzną. Przeglądy agregatu prądotwórczego wykonywane są raz na 3 miesiące również przez firmę zewnętrzną. Zespołowi kontrolnemu przedłożono dokumentację w tym zakresie (Protokół przeglądu/naprawy z roku 2021). Zespołowi kontrolnemu została udostępniona informacja dotycząca ochrony ppoż. w budynkach administrowanych przez UM Kielce. Praca w UM w zakresie działu IT jest dwuzmianowa, przygotowana jest aplikacja autorska UM, w której wymienione są czynności wykonywane regularnie na drugiej zmianie działu IT. Do PPzDO załączono Instrukcję numer 12 „Zarządzanie dostępem do pomieszczeń". Instrukcja zawiera wytyczne w obszarach : - dostęp do stref bezpieczeństwa, - nadzór nad pracami firm zewnętrznych, - dostęp do kluczy do pomieszczeń urzędu, - nadzór nad kluczami zapasowymi do pomieszczeń urzędu - przebywanie na terenie urzędu po godzinach pracy. W tym przypadku zespół kontrolny nie otrzymał załącznika numer 6 tj. listy osób upoważnionych do przebywania na terenie UM bez przepustki. - sprzątanie pomieszczeń urzędu - zabezpieczenie budynków urzędu po zakończeniu pracy W instrukcji numer 12 (patrz punkt 4.5) wymienione jest stanowisko inspektora ds. bezpieczeństwa, któremu miedzy innymi należy zgłaszać fakt otwarcia worka z kluczami lub uszkodzenia plomby(wymieniony jest jeszcze pracownik portierni i kierownik komórki organizacyjnej). Wiemy że od 6 miesięcy stanowisko

	inspektora bezpieczeństwa jest nieobsadzone. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf Protokol_ogledzin_pomieszczen.docx
Ustalone uchybienia	Zapis zawarty w instrukcji numer 12 do PPzDO dotyczący przechowywania wykazu stref bezpieczeństwa nie może być realizowany, ponieważ stanowisko inspektora ds. bezpieczeństwa, który za to odpowiada nie jest obsadzone. Instrukcja zarządzania dostępem do pomieszczeń wraz z załącznikami wymaga aktualizacji.
2.13 Zabezpieczenia techniczno-organizacyjne systemów informatycznych	
Podstawa prawna	**§ 20 ust. 2 pkt 12 zarządzenia:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. 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, utratą 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 zarządzenia:** 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.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Przedłożono dokumentację z wykonywania testów ciągłości (uwagi do protokołów zawarte zostały w punkcie 2.10 kopie zapasowe). Przedłożono logi z systemów tworzenia kopii zapasowych. Została udostępniona konsola systemu Windows server w parametrami haseł. Budynek UM wyposażony jest w centralny UPS oraz agregat prądotwórczy (patrz protokół oględzin). Została przedłożona dokumentacja z przeglądów technicznych z roku 2021. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf Protokol_ogledzin_pomieszczen.docx
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
2.14 Rozliczalność działań w systemach teleinformatycznych	
Podstawa prawna	**§ 21 ust. 2 rozporządzenia:** 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:** w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka. **§ 21 ust. 4 rozporządzenia:** 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
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	ASI w trakcie oględzin pokazał konsole systemu OTAGO moduł zarzadzania użytkownikami oraz uprawnieniami w systemie. Systemy Źródło i OTAGO odkładają logi z wykonywanymi przez użytkowników czynnościami w systemie. Kopie logów wykonywane są codziennie w ramach tworzenia kopii zapasowych (patrz punkt 2.10 niniejszego wystąpienia). Podobnie jest z logami urządzeń UTM, UPS i serwer domenowy. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Kielce.pdf protokół oględzin.pdf
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
Ocena obszaru kontroli nr 2	**Pozytywna z uchybieniami i nieprawidłowościami**
Obszar kontroli : **3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób z niepełnosprawnościami**	
3.1 Czy system teleinformatyczny spełnia wymagania WCAG 2.0 z uwzględnieniem poziomu AA, określonym w załączniku nr 4 do rozporządzenia KRI?	
Podstawa prawna	**§ 19 rozporządzenia:** 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.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny	ASI poinformował zespół kontrolny, że trwają przygotowania do wymiany strony BIP na nową platformę zgodną z WCAG 2.0. Strony www.um.kielce.pl i www.bip.kielce.eu zostały przetestowane za pomocą oprogramowania NVDA (czytnik ekranu), zostały również wyświetlone w przeglądarce FireFox i EDGE. Strona www.bip.kielce.eu . Strona ta posiada słabo wyróżnioną aktywną pozycję. Zakładka „Komunikacja w języku migowym". Po przejściu do tej zakładki wyświetlane jest okno z komunikatem o plikach cookies (zgodnie z RPEiR UE 2016/679 z dnia 27 kwietnia 2016r.). Po pierwsze nie da się zamknąć okna z komunikatem przy pomocy klawiatury, co powoduje że pewna część treści na stronie jest zasłonięta a przez to nieczytelna. Po drugie po przejściu do samego komunikatu nie ma powrotu do strony głównej (namiastka pułapki klawiaturowej). Ta sama sytuacja powtarza się na stronie www.um.kielce.pl. W obu przypadkach nie ma również komunikatu, że strona zostanie otwarta w nowym oknie przeglądarki. Strona nie jest wyposażona w funkcjonalności ułatwiające przeglądanie treści osobą słabowidzącym. Zdecydowana większość kart usług zamieszczona została na stronie w formatach edytowalnych. Strona posiada mapę strony jak również działającą, dostępną z klawiatury wyszukiwarkę. Strona www.um.kielce.pl . Przyciski znajdujące się pod grafikami umieszczonymi w górnym prawym rogu strony. Dostęp do nich i poruszanie się po nich nie jest intuicyjne. Wybranie za pomocą klawisza ENTER linku „ Komunikacja w języku migowym " nie powoduje przejścia do właściwej strony. Generalnie jest tak ze wszystkimi linkami umieszczonymi w prawym górnym rogu strony. Do właściwej strony z linków można przejść tylko i wyłącznie klikając w linki za pomocą myszy. Problemy są również z menu górnym głównym. Menu nie rozwija się przy użyciu klawiatury (przycisk ENTER) lub rozwija się sporadycznie. Rozwinięcie menu dostępne tylko za pomocą myszy. Na stronie dostępne są funkcjonalności dla osób słabowidzących jak przycisk zmieniający kontrast czy powiększający czcionkę. Brak informacji iż treść zostanie wyświetlona w nowej zakładce przeglądarki. Wyszukiwarka zamieszczona na stronie działa wątpliwie.
Ustalone nieprawidłowości	Strona www.bip.kielce.eu nie jest dostosowana do wymogów WCAG 2.0 ale można powiedzieć że informacje zamieszczona na stronie są dostępne bez większych problemów. Natomiast jeśli chodzi o stronę www.um.kielce.pl, jej budowa oraz funkcjonalność powoduje, że dla osób słabowidzących oraz dostępności treści za pomocą klawiatury jest praktycznie niemożliwa do obsługi, a tym samym informacje na niej zamieszczone są niedostępne.
Ocena obszaru kontroli nr 3	**Pozytywna z nieprawidłowościami**

Zalecenia	1. Rozszerzyć dokumentację o ochronę danych innych niż osobowe. System zarządzania bezpieczeństwem informacji powinien obejmować wszystkie dane przetwarzane w jednostce. 2. Regularnie dokonywać przeglądu i aktualizacji dokumentacji dotyczącej ochrony danych. 3. Rozwiązać problem związany z nieobsadzeniem stanowiska Inspektora ds. bezpieczeństwa, który jest odpowiedzialny za realizację wielu zadań w procesie zarządzania bezpieczeństwem informacji. 4. Należy okresowo organizować wewnętrzne szkolenia dla wszystkich pracowników urzędu dotyczące zagrożeń oraz środków zapewniających bezpieczeństwo informacji. 5. W dokumentacji należy określić szczegółowe zasady dotyczące pracy zdalnej oraz sposobu realizacji zdalnych połączeń. 6. Przeprowadzać audyty wewnętrzne w zakresie bezpieczeństwa informacji w zaplanowanych terminach. 7. W protokołach z testowania ciągłości działania zamieszczać wyniki testów. 8. W miarę możliwości dostosować strony internetowe urzędu do wymagań WCAG 2.0 z uwzględnieniem poziomu AA.

Na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i uchybień, a także o przekazanie w terminie **30 dni** od daty otrzymania niniejszego wystąpienia pokontrolnego informacji o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz o wykonaniu zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

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

Zbigniew Koniusz
Wojewoda Świętokrzyski

UPP - Urzędowe Poświadczenie Przedłożenia

Identyfikator Poświadczenia: ePUAP-UPP75347781

Adresat dokumentu, którego dotyczy poświadczenie
Nazwa adresata dokumentu: URZĄD MIASTA KIELCE
Identyfikator adresata: g94m13lgvz
Rodzaj identyfikatora adresata: ePUAP-ID

Nadawca dokumentu, którego dotyczy poświadczenie
Nazwa nadawcy: ŚWIĘTOKRZYSKI URZĄD WOJEWÓDZKI W KIELCACH
Identyfikator nadawcy: SUWKielce
Rodzaj identyfikatora nadawcy: ePUAP-ID

Dane poświadczenia
Data doręczenia: 2022-01-20T10:15:40.162
Data wytworzenia poświadczenia: 2022-01-20T10:15:40.162
Identyfikator dokumentu, którego dotyczy poświadczenie: DOK108892319

Dane uzupełniające (opcjonalne)
Rodzaj informacji uzupełniającej: Źródło
Wartość informacji uzupełniającej: Poświadczenie wystawione przez platformę ePUAP

Rodzaj informacji uzupełniającej: Identyfikator ePUAP dokumentu
Wartość informacji uzupełniającej: 108892319

Rodzaj informacji uzupełniającej: Informacja
Wartość informacji uzupełniającej: Zgodnie z art 39^1 par. 1 k.p.a. pisma powiązane z przedłożonym dokumentem będą przesyłane za pomocą środków komunikacji elektronicznej.

Rodzaj informacji uzupełniającej: Pouczenie
Wartość informacji uzupełniającej: Zgodnie z art 39^1 par. 1d k.p.a. istnieje możliwość rezygnacji z doręczania pism za pomocą środków komunikacji elektronicznej.

Dane dotyczące podpisu
Poświadczenie zostało podpisane - aby je zweryfikować należy użyć oprogramowania do weryfikacji podpisu
Lista podpisanych elementów (referencji):
referencja ID-c62d246f58201c518eba1fc3aa4e8f00 :
referencja ID-d5dda27438751d7e9ba94eeacea39763 : Wystapienie%20pokontrolne.xml
referencja : #xades-id-b80267a845cd5bdf49f384fbf26f67ad

Podpisy zawarte e-dokumencie:

Status Certyfikat	Podpis kwalifikowany	Profil zaufany	Czas wytworzenia	Okres ważności certyfikatu	Ostatnia weryfikacja
Właściciel: ePUAP ESP, Kancelaria Prezesa Rady Ministrow Wystawca: Centrum Kwalifikowane EuroCert, EuroCert Sp. z o.o.		**NIE**	**2022-01-20 10:15:40**	**2021-09-04 10:13:33 - 2024-09-03 10:13:33**	