WOJEWODA ŚWIĘTOKRZYSKI

Kielce, dnia 02-08-2023

Znak: OK.V.431.4.2023

Wystąpienie pokontrolne

Kontrolę w Urzędzie Miasta w Skarżysku - Kamiennej w dniu 28 czerwca 2023 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 465 z dnia 22 czerwca 2023 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 466 z dnia 22 czerwca 2023r. 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) 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.

Kontrolą objęto następujące systemy informatyczne używane do realizacji zadań zleconych z zakresu administracji rządowej: Źródło, CEIDG, Korelacja oraz SELWIN (rejestr wyborców RWWIN).

Wykonywanie zadań w kontrolowanym zakresie oceniam pozytywnie z 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. System Zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych.	
1.1 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	Zasady zarządzania bezpieczeństwem informacji w Urzędzie Miasta w Skarżysku – Kamiennej określa Zarządzenie nr 358/2019 Prezydenta Miasta z dnia 12.12.2019r. w sprawie przyjęcia dokumentacji ochrony danych osobowych w Urzędzie. Wprowadza ono Politykę Ochrony Danych Osobowych (PODO) oraz Instrukcję Zarządzania Systemem Informatycznym (IZSI) do przetwarzania danych osobowych, która jest załącznikiem numer 2 do PODO. W PODO w dziewięciu rozdziałach opisane są procedury, instrukcje, zalecenia dotyczące szeregu zagadnień związanych z ochroną danych osobowych: • podana została podstawa prawna która posłużyła jako wykładnia do opracowanej PODO; • opisano podstawowe obowiązki osób biorących udział w przetwarzaniu danych osobowych (w tym ASI, ADO, IOD); • przeprowadzono inwentaryzację zasobów danych, zasobów informatycznych; • określono zasady przetwarzania danych osobowych; • opisano temat naruszenia ochrony danych; • określono procedury bezpieczeństwa danych osobowych w tym pisano proces analizy ryzyka; • zdefiniowano dokumentację dotyczącą miejsca, sposobu i zakresu przetwarzania danych osobowych; • opracowano schemat planu ciągłości działania; • określono środki bezpieczeństwa (techniczne, organizacyjne) niezbędne do zapewnienia poufności, integralności

	i rozliczalności przetwarzanych danych osobowych; • zdefiniowano 30 załączników do PODO. W IZSI która jest załącznikiem numer 2 do PODO w 17 rozdziałach opisano zasady eksploatacji i zarządzania systemem informatycznym oraz zdefiniowano: • procedury nadawania uprawnień w systemach informatycznych; • metody, środki i procedury uwierzytelniania; • procedury rozpoczęcia i zakończenia pracy; • procedury tworzenia kopii zapasowych; • procedury przechowywania nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych; • sposoby zabezpieczenia systemu informatycznego; • procedury w przypadku informacji o udostepnieniu danych; • procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji; • procedury bezpiecznego użytkowania urządzeń mobilnych; • procedury korzystania z poczty elektronicznej i Internetu; • procedury bezpiecznej transmisji; • procedury dostępu podmiotów zewnętrznych do systemów Urzędu; • zasady wydawania lub unieważniania certyfikatów podpisu kwalifikowanego; • procedury zasilania awaryjnego; • procedury w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego. Zarządzeniem numer 336/208 Prezydenta Miasta Skarżyska-Kamiennej z dnia 30 października 2018r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta w Skarżysku – Kamiennej powołano także Zespół ds. Zarzadzania Bezpieczeństwem Informacji, w którego w skład weszły osoby : • sekretarz miasta (przewodniczący zespołu) • IODO • Pełnomocnik ds. Ochrony Informacji Niejawnej • Kierownik Zespołu Informatycznego • Administrator Systemów Informatycznych Zespół ten zajmuje się między innymi doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji, analizą incydentów naruszenia bezpieczeństwa informacji, przeglądami dokumentacji oraz analizą ryzyka. Dowód - akta kontroli plik : Załącznik Nr 1 do Zarządzenia Nr-1.pdf, Instrukcja Zarzadzania Systemami Informatycznymi od sławka-1.pdf
Ustalone nieprawidłowości	Całość dokumentacji poświęcona jest szczególnym danym jakie są dane osobowe (np. patrz procedura naruszeń dotyczy tylko i wyłącznie danych osobowych). Znaczna cześć zapisów z PODO i IZSI w

	praktyce nie jest wdrożona, patrząc na rozdział IX PODO o odpowiedzialności służbowej. Nie ma świadomości, kontroli w tym zakresie. Zespołowi kontrolnemu nie przedstawiono także dowodów na wykonywanie przeglądów i aktualizacji PODO i IZSI w rozumieniu rozporządzenia o KRI na przestrzeni lat 2019-2023 (patrz audyt w ramach „Cyfrowa Gmina" A.18.2.1). O braku przeglądania świadczy też błąd w numeracji rozdziałów PODO. Brak numeru VII, dwa razy występuje rozdział VIII. Potwierdzają to również ustalone uchybienia i nieprawidłowości opisane dalej w niniejszym dokumencie.
Ocena obszaru kontroli nr 1	Pozytywna z nieprawidłowościami
Obszar kontroli : 2. Realizacja działań z zakresu bezpieczeństwa informacji	
2.1 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*	Przedłożono dokumenty w których szczegółowo opisano cały proces związany z analizą ryzyka, rozdział V PODO z roku 2019 oraz załącznik numer 27 do PODO „Zasady i tryb zarządzania ryzykiem ochrony danych osobowych przetwarzanych w UM Skarżysku - Kamiennej". Wyznaczono osoby odpowiedzialne za zebranie informacji (Zespół ds. Zarzadzania Bezpieczeństwem Informacji, pracownicy UM którym przypisano poszczególne ryzyka), wyznaczono konkretne terminy. Zespół ds. Zarządzania Bezpieczeństwem Informacji miał rozesłać kwestionariusze oceny ryzyka do pracowników tak aby zebrać pożądane informacje maksymalnie do 30 kwietnia każdego roku. Podobnie kierownik pionu informatyki do 30 kwietnia każdego roku ma przeprowadzać analizę ryzyk w obszarze przetwarzania danych osobowych w systemie informatycznym. Na podstawie zebranych danych Zespół ds. Zarządzania Bezpieczeństwem Informacji maksymalnie do 30 czerwca każdego roku ma oszacować ryzyka w ochronie danych osobowych a następnie w formie raportu przedłożyć do zapoznania Administratorowi Danych Osobowych. Zespołowi kontrolnemu przedłożono „Analizę ryzyka dla wykonywania prac zdalnej" (pisownia oryginalna) z roku 2020. Analizę przeprowadzono w dniach 6-26.10.2020 roku. Dodatkowo jako analizy ryzyka można uznać przedłożone „sprawozdanie z oceny (analizy) zagrożeń i oceny bezpieczeństwa przetwarzanych informacji (w tym danych osobowych) za pomocą systemu informatycznego w Urzędzie Miasta w Skarżysku – Kamiennej" z roku 2021 oraz „sprawozdanie z oceny zagrożeń bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta w Skarżysku – Kamiennej z roku 2023.

	Dowód - akta kontroli plik: pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone uchybienia	Na podstawie przedstawionych zapisów można stwierdzić, że realizowany w praktyce proces analizy ryzyka nie jest zgodny z tym, co opisano w dokumentacji. Przypomnę, powołano w roku 2018 specjalny Zespół ds. Bezpieczeństwa Informacji, skład zespołu jest znany, rozpisano obowiązki, wdrożono w tym zakresie PODO w tym opracowano załącznik numer 27 do PODO, określono cel tego dokumentu, wyznaczono konkretne terminy.
2.2 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	Inwentaryzacja sprzętu prowadzona jest w oparciu o oprogramowanie do inwentaryzacji AssetsNinja. Zespołowi kontrolnemu przedłożono przykładowy zrzut ekranu z różnym sprzętem począwszy od czytników kart, router, sprzęt komputerowy, switche oraz drukarki. Ewidencja posiada informacje typu: numer inwentarzowy, nazwę, imię i nazwisko osoby do której sprzęt jest przyporządkowany. Ewidencja jest prowadzona, chociaż zespół kontrolny nie jest wstanie stwierdzić czy jest kompletna. Dowód - akta kontroli plik: pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone uchybienia, nieprawidłowości	BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI
2.3 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	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie odpowiedzialnej za te czynności są zawarte w rozdziale II IZSI. Zespół kontrolny wytypował trzech pracowników aktualnie zatrudnionych w UM o inicjałach: SN,KS,AB oraz dwóch pracowników którzy zakończyli pracę w UM: AK i MA. Została przedłożona dokumentacja dotycząca wyżej wymienionych pracowników czyli: • upoważnienie do przetwarzania danych osobowych (patrz

	załącznik numer 10 z PODO). Upoważnienie zawiera niepowtarzalny identyfikator pracownika w systemie informatycznym, dokument posiada podpis Prezydenta Miasta, IODO oraz pracownika. • Uprawnienia (patrz załącznik numer 12 z PODO) do przetwarzania danych osobowych w systemie informatycznym. W dokumencie wymienione są systemu informatyczne wraz z uprawnieniami użytkownika w tych systemach . • Wniosek (patrz załącznik numer 9 z PODO) o wydanie, zmianę lub cofnięcie upoważnienia do przetwarzania danych osobowych. • Zlecenie o ustalenie uprawnień dla użytkownika w systemie informatycznym (patrz załącznik numer 1 do IZSI) • Oświadczenie o poufności (patrz załącznik numer 3 do PODO).
Ustalone uchybienia	Pracownik AB : Wniosek (załącznik numer 9 do PODO) dla pracownika AB nie posiada wpisanej daty złożenia wniosku przez bezpośredniego przełożonego, brak daty przekazania zlecenia, brak podpisu kierownika ZI. Brak daty na łączniku numer 1 do IZSI (jest tylko podpis bezpośredniego przełożonego). Pracownik KS : Wniosek (załącznik numer 9 do PODO) dla pracownika KS nie ma podpisów i dat w części III. Zalecenie (patrz załącznik numer 1 do IZSI) nie posiada części II i III Pracownik SN : Brak zlecenia o ustalenie uprawnień dla użytkownika w systemie informatycznym (patrz załącznik numer 1 do IZSI). Są „uprawnienia" brak zlecenia do posiadanego uprawnienia. Pracownik MA: Brak dokumentu wniosku o cofnięcie uprawnień w związku z cofnięciem upoważnienia do przetwarzania danych osobowych, brak zlecenia o odebranie uprawnień w systemie informatycznym. Brak również Karty odebrania uprawnień (patrz załącznik numer 1 do IZSI). Z punktu widzenia zespołu kontrolnego proces odbierania uprawnień pracownikom, który kończą pracę w UM jest nie dopracowany podobnie jak proces modyfikacji uprawnień w momencie zmiany stanowiska czy zakresu czynności. Osoby odpowiedzialne za wytworzenie we właściwym czasie odpowiedniej dokumentacji (patrz załącznik numer 2 do PODO) bezpośredni przełożeni nie przestrzegają zasad opisanych w PODO. Efektem tego jest brak wiedzy ASI o odebraniu uprawnień zwolnionym pracownikom. Informacja ta w efekcie końcowym trafia do ASI z opóźnieniem większym lub mniejszym ale inną droga niż procedura opisana w PODO. Dokumenty nie są oznaczone zgodnie z PODO (patrz strona 109 PODO) wykaz załączników. Upoważnienia: brak oznaczenia że to załącznik numer 10 z PODO Uprawnienia: brak oznaczenia że to załącznik numer 12 z PODO. Wniosek: brak oznaczenia że to załącznik numer 9 z PODO. Brak tych oznaczeń wprowadza pewien „zamęt" w poruszaniu się po

	dokumentacji. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
2.4 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 podstawę do oceny	Z rozmowy przeprowadzonej z IOD wynika, że przeprowadza szkolenia z ochrony danych osobowych podczas procesu zatrudniania nowego pracownika w Urzędzie. Pracownicy podpisują oświadczenie, iż zapoznali się z przepisami dotyczącymi ochrony danych osobowych, w szczególności z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku. Oświadczają również, że zapoznali się z Polityką Ochrony Danych Osobowych w Urzędzie Miasta w Skarżysku - Kamiennej oraz Instrukcją Zarzadzania Systemem Informatycznym służącym do przetwarzania danych osobowych. IOD przedłożył dokument z podpisami dziewięciu osób uczestniczących w procesie przetwarzania danych osobowych w rejestrach państwowych. Dokument pochodzi z roku 2022. IOD przedłożył dokumentację w postaci notatek służbowych ze szkoleń pracowników z lat 2019-2023. Zakres przeprowadzonych szkoleń obejmował : • Podstawowe definicje z zakresu ochrony danych osobowych • Podstawy przetwarzania danych osobowych • Wypełnianie obowiązku informacyjnego • Powierzenia przetwarzania danych • PODO i IZSI • Incydenty, naruszenia ochrony danych osobowych • Konsekwencje za nieprzestrzeganie przepisów o ochronie danych osobowych. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone uchybienia	W niektórych przypadkach (patrz SN) pracownik brał udział w szkoleniu z zakresu ochrony danych w tym ochrony szczególnych danych jakimi są dane osobowe oraz z PODO i IZSI w roku 2019 a więc 4 lata temu. Zapewne jest więcej pracowników UM które ostatni raz w podobnym szkoleniu brały udział 4 lata temu. Szkolenia powinny obywać się systematycznie. Brak systematycznych szkoleń z PODO i IZSI widać na przykładnie procedury odbierania uprawnień w systemach informatycznych pracownikom którzy odeszli

	z pracy z UM co zostało pisane w punkcie 2.3 niniejszego dokumentu..
2.5 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	Rozdział XIII IZSI „Procedura dostępu podmiotów zewnętrznych do systemów informatycznych" dotyczy bardziej zagadnienia powierzenia przetwarzania danych osobowych niż pracy zdalnej pracowników Urzędu lub osób trzecich z firm zewnętrznych. W Rozdziale X „Procedura bezpiecznego użytkowania urządzeń mobilnych oraz elektronicznych nośników danych" bardzo ogólnie potraktowano temat pracy zdalnej. Z procedury wynika, że dostęp do urządzeń mobilnych uzyskuje się poprzez procedurę powierzenia tych urządzeń konkretnemu pracownikowi . Z rozmowy przeprowadzonej z ASI wynika, iż urząd przystąpił do projektu „Cyfrowa gmina" i z zakresie tego projektu zostały zaplanowane działania związane z przygotowaniem UM do opracowania, wdrożenia procedur, instrukcji związanej z pracą zdalną. Na dzień kontroli ASI ma pełną kontrolę nad połączeniami zdalnymi osób trzecich, firm trzecich współpracujących z UM. Zostały udostępnione logi rejestrujące połączenia zdalne firm, osób trzecich z systemem UM. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone nieprawidłowości	Brak opisanej procedury pracy zdalnej w rozumieniu rozporządzenia o KRI. Brak określonych zasad dostępu do pracy zdalnej pracowników UM. Brak próbki logów o które prosił zespół kontrolny z monitorowania połączeń zdalnych firm trzecich.
2.6 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	W IZSI w rozdziale IX opisano procedurę oraz czynności związane z konserwacją, naprawą, serwisem sprzętu komputerowego. W punkcie 4 opisano czynności wykonywane przy serwisie sprzętu komputerowego i oprogramowania przez firmy zewnętrzne. Punkt 7 mówi o tym iż prace serwisowe prowadzone przez podmioty zewnętrzne wymagają sporządzenia **protokołu serwisowego** zawierającego odpowiednie informacje (patrz podpunkty a), b), c) d), e) punktu 7). Zespół kontrolny zapoznał się umową serwisową systemu SELWIN oraz z umową opieki autorskiej systemu Korelacja. Dowód - akta kontroli plik: pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone uchybienia	Zespołowi kontrolnemu nie przedstawiono żadnego protokołu.
2.7 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	W PODO z roku 2019 rozdział IV poświęcono tematowi naruszeń ochrony danych osobowych. Zdefiniowano i opisano procedurę postępowania w przypadku naruszenia bezpieczeństwa danych osobowych. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone uchybienia	Wspomniana powyżej procedura z PODO z roku 2019 dotyczy jedynie szczególnych danych jakimi są dane osobowe. Cytuję z PODO „*Przez pojęcie naruszenia ochrony danych należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych*". Jeżeli chodzi o systemy informatyczne jest jasne, że jeżeli chronione są dane osobowe to również inne dane chronione są w ten sam sposób co dane osobowe. Natomiast w przypadku naruszeń, incydentów można powiedzieć, że incydenty, naruszenia nie związane z danymi osobowymi nie są monitorowane, nadzorowane, analizowane. Nie ma świadomości naruszeń, incydentów innych danych niż dane osobowe. Patrz audyt w ramach „Cyfrowa gmina" z roku 2020 (patrz A.16.1.1)
2.8 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	W rozdziale V PODO „Bezpieczeństwo danych osobowych" opisano jak powinien funkcjonować audyt wewnętrzny w zakresie bezpieczeństwa informacji. Przedłożono dokumentację z audytu zewnętrznego przeprowadzonego w roku 2022 w związku z przystąpieniem Urzędu do programu Cyfrowa Gmina. Audyt został zrealizowany zgodnie z załącznikiem numer 8 „formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa programu Cyfrowa Gmina". Przedłożono dokumentację „Protokół sprawdzeń" z roku 2020 dotyczący działania systemów teleinformatycznych oraz rejestrów publicznych przeprowadzonych przez IOD i ASI a także dokumentację ze sprawdzeń „przestrzegania zasad ochrony danych osobowych" z roku 2023. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Skarżysko-

	Kamienna.pdf
Ustalone nieprawidłowości	Brak audytów wewnętrznych w latach 2019-2023 w rozumieniu rozporządzenia o KRI, co potwierdza również audyt przeprowadzony w ramach „Cyfrowej gminy". Są dokumenty ze sprawdzeń IOD które podejmował on w roku 2023 i wcześniejszych latach, ale nie są to sprawdzenia kompleksowe PODO i IZSI lecz sprawdzenia pewnych pojedynczych zagadnień.
2.9 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	Rozdział V i VI z IZSI z roku 2019 poświęcony jest zagadnieniom związanym ze sporządzaniem i przechowywaniem kopii zapasowych. Częstotliwość wykonywania kopi oraz ich czas przechowywania jest określona w rozdziale V IZSI na stronie 16 i 17 . Został przedłożony zrzut ekranu zawierający rejestr taśm użytych do backupów. Dowód - akta kontroli plik : pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone uchybienia	Nie ma wątpliwości, iż kopie zapasowe są wykonywane, przedłożone zostały przez ASI kopie logów z dnia 27 czerwca 2023 roku. Natomiast wątpliwości zespołu kontrolnego są związane z punktami 1-9 rozdziału V IZSI. Nie została przedłożona dokumentacja dotycząca ewidencji wykonania kopii zapasowych (patrz punkt 2, strona 16, rozdział V IZSI), rejestru nośników zawierających kopie danych osobowych (patrz załącznik 2 do IZSI). W związku z powyższym zespół kontrolny ma wątpliwości czy ogólne zasady sporządzania kopii zapasowych opisane w IZSI są przestrzegane.
2.10 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	Budynek wyposażony jest w system przeciwpożarowy, antywłamaniowy, system monitoringu wizyjnego (dane z monitoringu przechowywane są ok. 30 dni). Wejście główne do budynku zabezpieczone jest certyfikowanymi podwójnymi drzwiami

	z podwójnymi zamkami. Wejście monitorowane jest przez system kamer wizyjnych. Opracowana i została wdrożona polityka kluczy, przy wejściu głównym zamontowany został elektroniczny depozytor kluczy. Wejścia do pomieszczeń zabezpieczone są zwykłymi drzwiami z zamkiem, pomieszczenia wyposażone są w szafy zamykane na klucz. Wejście do pokoju ASI a w tym również do serwerowni zabezpieczone jest elektronicznym zamkiem. Budynek wyposażony jest w podwójną sieć zasilania. Sieć (czerwona) podłączona jest do centralnego UPS-a znajdującego się w piwnicy budynku. Szacowany czas podtrzymania napięcia to około 40 minut. Sieć (biała) podłączona jest do agregatu prądotwórczego znajdującego się poza budynkiem UM w jego najbliższym otoczeniu. Przedłożono protokół z przeglądu agregatu oraz testu agregatu z dnia 23.03.2023r. Oba pomieszczenia serwerowni są wyposażone w urządzenia monitorujące temperaturę oraz wilgotność, wyposażone są w szafy dystrybucyjne w których zamontowano urządzenia aktywne. Urząd posiada działające urządzenie UTM. Serwer domenowy jest pod kontrolą systemu Windows 2022. UM posiada skonfigurowane i podłączone urządzenia do wykonywania backupów. Dowód - akta kontroli plik: pobrane-dokumenty-UM-Skarżysko-Kamienna.pdf
Ustalone uchybienia	W pomieszczeniu serwerowni składowany jest nie używany sprzęt.
2.11 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	Jest wdrożony Active Directory, sieć jest chroniona przez urządzenie UTM, serwery, urządzenia aktywne umieszczone w serwerowni podłączone są do urządzenia podtrzymującego napięcie (szacowany czas podtrzymania napięcia około 40 minut), urządzenia umieszczone

	są w szafach dystrybucyjnych. Zainstalowany, aktualizowany na bieżąco system antywirusowy. Serwer domenowy posiada system Windows serwer 2022. Wdrożona jest polityka haseł (8 znaków, małe i duże litery, przynajmniej jedna cyfra lub znak specjalny), hasła są zmieniane co 30 dni. W PODO w rozdziale VIII - Ciągłość Działania opisano procedury związane z zapewnieniem ciągłości działania systemów Urzędu.
Ustalone uchybienia	Brak zapisów z testów związanych z przywróceniem poprawności funkcjonowania systemów informatycznych po awarii.
2.12 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	Systemy takie jak Źródło, Korelacja posiadają funkcjonalność monitorującą pracę użytkowników. Podobnie jest z systemami serwerowymi Windows Serwer 2022, systemami Windows 10 i 11 zainstalowanymi na sprzęcie komputerowym pracowników Urzędu. Logi przeglądane są w miarę możliwości.
Ustalone uchybienia	Brak systematyczności w przeglądaniu logów, brak narzędzi do przeglądania i analizy logów.
Ocena obszaru kontroli nr 2	Pozytywna z uchybieniami i nieprawidłowościami
Obszar kontroli : 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.	
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	Strony https://um.skarzysko.pl i https://bip.skarzysko.pl 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. Gdy poruszamy się po stronie https://um.skarzysko.pl za pomocą klawiatury, na starcie aktywna pozycja jest wyróżniona, tekst opisu pozycji jest czytany. Problemy zaczynają się po opuszczeniu przycisku BIP. Przycisk przełączania kontrastu jest niedostępny z klawiatury podobnie jak również przycisk powiększania i pomniejszania tekstu, niedostępne jest również pole wyszukiwarki. Po opuszczeniu zakładki (link do FB) przenoszeni jesteśmy do strony https://um.skarzysko.pl/jackpotcity/, która zapewne nie pochodzi z serwisu https://um.skarzysko.pl . Kolejne przejścia dotyczą storn : https://um.skarzysko.pl/onlinw-slots-india/ https://um.skarzysko.pl/nowe-polskie-kasyno-online/ https://um.skarzysko.pl/best-casino-ganes/ https://um.skarzysko.pl/triumph-casino/ Przypuszczalnie są to linki ze starego szablonu, który został wykorzystany na obecnej stronie Urzędu. Nie mniej jednak ten stan utrudnia poruszanie się po stronie Urzędu. Wyżej opisana sytuacja nie dotyczy wersji angielskiej strony. Na stronie aktualności https://um.skarzysko.pl znajduje się „puste" przejście pomiędzy zakładkami. Nie da się z klawiatury rozwinąć opcji w menu górnym. Sprawdzenie kontrastu aktywnej pozycji za pomocą narzędzia do sprawdzania kontrastu Colour Contrast Analyser (CCA), dało wynik negatywny praktycznie na wszystkich linkach, pozycjach aktywnych na stronie. Na stronie https://bip.skarzysko.pl nie działa wyszukiwarka Wydziałów i Referatów. Są tam również problemy z „Formularzem kontaktowym". Brak opisu konkretnych pól w formularzu, czytnik ekranu nie ma czego czytać odnośnie pół w formularzu. Podobnie ma się sprawa z błędami przy wypełnianiu formularza. Klikając na opcje RSS użytkownik dostaje informację, że strona nie istnieje lub jest czasowo niedostępna.
Ustalone uchybienia	Problemy z obsługą stron wyłącznie za pomocą klawiatury, poziom kontrastu nie zgodny z wymaganiami WCAG 2.0. Nie wszystkie elementy stron mają opisy niezbędne dla czytnika ekranu.
3.2 Czy sporządzono i opublikowano deklarację dostępności oraz zawarto w deklaracji dostępności elementy wskazane w art. 10 ust. 3-5 ustawy dla stron internetowych podmiotu	
Podstawa prawna	Art. 10 ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych

Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Obydwie badane strony tj. https://um.skarzysko.pl oraz https://bip.skarzysko.pl posiadają stosowne deklaracje dostępności cyfrowej.
Ustalone uchybienia, nieprawidłowości	BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI
Ocena obszaru kontroli nr 3	Pozytywna z uchybieniami
Zalecenia	1) Rozszerzyć dokumentację o ochronę danych innych niż osobowe. System zarządzania bezpieczeństwem informacji powinien obejmować wszystkie dane przetwarzane w jednostce. 2) Regularnie przeglądać i aktualizować dokumentację ochrony danych. 3) Proces analizy ryzyka realizować zgodnie z tym, co opisano w dokumentacji lub dokonać zmian w dokumentacji, tak aby odzwierciedlała rzeczywiste działania. 4) Dopracować proces odbierania uprawnień pracownikom, który odchodzą z pracy w Urzędzie. Dokumenty dotyczące zarządzania uprawnieniami oznaczać zgodnie z PODO (patrz strona 109 PODO - wykaz załączników). 5) Systematycznie przeprowadzać szkolenia z bezpieczeństwa informacji. 6) Ustanowić procedurę pracy zdalnej w rozumieniu rozporządzenia o KRI i określić zasady dostępu do pracy zdalnej pracowników Urzędu. 7) Przeprowadzać okresowe audyty wewnętrzne w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. 8) Przestrzegać opisanych w dokumentacji zasad wykonywania kopii zapasowych i prowadzić stosowną ewidencję. 9) W miarę możliwości usunąć z pomieszczenia serwerowni składowany tam nie używany sprzęt. 10) Dokumentować testy przywracania funkcjonowania systemów informatycznych po awarii. 11) Systematycznie przeglądać logi systemowe. 12) Poprawić obsługę stron internetowych za pomocą klawiatury. Uzupełnić opisy niezbędne dla czytnika ekranu.

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