WOJEWODA ŚWIĘTOKRZYSKI

Kielce, dnia 28-06-2022

Znak: OK.V.431.4.2022

Wystąpienie pokontrolne

Kontrolę w Urzędzie Miasta i Gminy Małogoszcz ul. Jaszowskiego 3a w dniach 26-27 kwietnia 2022 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 nr 199/2022 z dnia 20.04.2022 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 200/2022 z dnia 20.04.2022 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 niepełnosprawnych.

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 https://www.malogoszcz.eobip.pl/bip_malogoszcz opublikowano informacje dotyczące Elektronicznej Skrzynki Podawczej wraz z informacjami w jaki sposób za pomocą platformy epuap.gov.pl można składać dokumenty w formie elektronicznej w UMiG. W zakładce dane teleadresowe jest zamieszczona pełna nazwa skrytki /otig124o8w/skrytka. W zakładce „Jak załatwić sprawę w Urzędzie?" zamieszczono opis procedur obowiązujących przy załatwianiu spraw. Na stronie zamieszczono również informacje dotyczące działającego punktu zakładania profilu zaufanego w budynku Urzędu.
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 i Gminy Małogoszcz nie przekazuje własnych wzorów dokumentów elektronicznych do centralnego repozytorium. Wzory dokumentów są publikowane w BIP Urzędu.
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	Urząd Miasta i Gminy Małogoszcz nie posiada własnej platformy usługowej. Jest tylko wykupiona usługa „Platformy zakupowej" u firmy zewnętrznej platformazakupowa.pl/pn/Malogoszcz służąca do komunikowania się z wykonawcami w trakcie postępowania przetargowego.
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	Program Źródło przeznaczony do przetwarzania danych zgromadzonych w Systemie Rejestrów Państwowych powiązany jest z rejestrem mieszkańców w systemie RESPONS. W UMiG wdrożony jest system RESPONS dawna PUMA (moduły: Ewidencja Ludności, Wyborcy, Kadry, Płace, Koncesje Alkoholowe, Paliwa). W oparciu o umowę z firmą ZETO nr 21/0028/JU opieką autorską zostało objętych 26 modułów systemu. Moduł Wyborcy powiązany jest z rejestrem mieszkańców (moduł Ewidencja ludności) Moduł Paliwa powiązany jest z modułem Kontrahenci. W urzędzie gminy funkcjonuje także zintegrowane oprogramowanie autorstwa firmy Sygnity do obsługi świadczeń wychowawczych, świadczeń rodzinnych, funduszu alimentacyjnego, dodatku osłonowego, programu Czyste Powietrze i zadań własnych gminy. Wszystkie moduły ww. oprogramowania są wzajemnie powiązane i wymieniają ze sobą dane.
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	Podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie Miasta i Gminy w Małogoszczu jest system tradycyjny. Funkcjonujący w urzędzie elektroniczny system obiegu dokumentów jest systemem wspomagającym system tradycyjny. W systemie tym odbywa się odbieranie i dekretowanie korespondencji na poszczególnych pracowników. System elektronicznego obiegu dokumentów Edicta został wprowadzony zarządzeniem burmistrza nr 9/2017 z dnia 25 stycznia 2017 r. Dowód: BIP UMiG Małogoszcz, zakładka „Elektroniczny obieg dokumentów".
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	Informacja o formatach danych w jakich przyjmowane i przekazywane są dokumenty elektroniczne znajduje się na stronie BIP Urzędu w zakładce „Elektroniczna Skrzynka Podawcza – Informacje". Akceptowalne formaty plików to: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.
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	Całość dokumentacji SZBI składa się z dwóch zasadniczych dokumentów wprowadzonych zarządzeniem nr 144/2015 Burmistrza Miasta i Gminy Małogoszcz z dnia 17 grudnia 2015r.: 1. „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych" – załącznik 1 do Zarządzenia 144/2015 2. „Instrukcji Zarządzania Systemem Informatycznym" – załącznik 2 do Zarządzenia 144/2015 Z przeprowadzonej rozmowy z ASI wynika iż od dnia wdrożenia wyżej wymienionej dokumentacji Zarządzeniem 144/2015 roku dokumentacja czyli PBPDO jak również IZSI nie były aktualizowane praktycznie do dnia kontroli. PBPDO została opracowana na podstawie ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2014 poz. 1182) w 2015 roku. Przy jej opracowaniu nie uwzględniono Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie KRI, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. W między czasie została opublikowana nowa Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych. W UMiG nie podjęto żadnych działań na przestrzeni 7 lat mających na celu zaktualizowanie procedur, procesów, instrukcji związanych z nową ustawą o ochronie danych osobowych oraz rozporządzeniem w sprawie KRI. Nie dokonano przeglądu dokumentacji pod kątem jej aktualizacji. 1 lutego 2022 roku podpisano umowę „o wykonanie zadań Inspektora Ochrony Danych oraz świadczenia usług w zakresie doradztwa informatycznego". W ramach umowy Zleceniobiorca zobowiązuje się w terminie nie dłuższym niż 3 miesiące od dnia podpisania umowy do wytworzenia i przekazania Zleceniodawcy dokumentów z załącznika nr 1 do umowy. Termin przekazania dokumentacji minął 1 kwietnia 2022 (na dzień rozpoczęcia kontroli mamy 17 dni po terminie). Zleceniodawca zobowiązuje się w późniejszym terminie wykonać „Analizę ryzyka systemu informatycznego oraz danych osobowych".

	W dniu kontroli to jest 26 kwietnia Zespołowi Kontrolnemu został przedłożony dokument wytworzony tego samego dnia przez IODO (Pana RŁ) informujący, że na podstawie ustalonego harmonogramu (przypomnę, iż harmonogram został ustalony już wcześniej patrz załącznik nr.1 do umowy o wykonywaniu zadań IOD, terminy nie zostały dotrzymane) wdrożenia dokumentacji wykona następujące czynności w terminach: Do 30 kwietnia 2022 przekaże „Rejestr Czynności Przetwarzania Danych Osobowych, Politykę Ochrony Danych Osobowych" Do 9 maja 2022 przekaże „Analizę ryzyka" Do 9 maja 2022 przeszkoli pracowników UMiG przetwarzających dane osobowe. Zespołowi kontrolnemu nie został przedłożony załącznik numer 1 do IZSI. Z przeprowadzonej rozmowy z ASI wynika iż załącznik nie był używany przez pracowników UMiG. Przypomnę iż załączniki numer 1 do IZSI służy do nadawania, modyfikacji, odbierania uprawnień w systemach informatycznych. Na załączniku numer 1 jest miejsce na podpis bezpośredniego przełożonego użytkownika systemu wraz z datą wystawienia załącznika, miejsce na podpis Kierownika. Wynika z tego, że osoby które zapoznały się z PBPDO (jest stosowne oświadczenie pracowników) nie stosowały się do PBPDO mając świadomość odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów (taki zapis jest na oświadczeniu) oraz patrz (IZSI patrz Rozdział II, paragraf 4 IZSI, punkt 4). Procedura odbierania uprawnień w systemach informatycznych według IZSI powinna rozpocząć się pismem ABI zawierającym informacje o dacie i przyczynie odebrania, modyfikacji uprawnień. Również i ten zapis z IZSI nie jest i nie był stosowany w praktyce. Ta sama sytuacja dotyczy załącznika numer 2 do IZSI „Ewidencji uprawnień w zakresie dostępu do systemu informatycznego". Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf
Ustalone nieprawidłowości	Do dnia kontroli to jest 26 kwietnia 2022 roku dokumentacja wdrożona Zarządzeniem 144/2015 nie była aktualizowana, przeglądana. W roku 2018 została opublikowana nowa ustawa o ochronie danych osobowych, ale Administrator nie podjął żadnych czynności zmierzających do aktualizacji dokumentacji, procedur i procesów zgodnie z nową ustawą. Trzeba również zwrócić uwagę na fakt, że wszelkie działania podjęte przez UMiG dotyczyły tylko i wyłącznie szczególnych danych jakimi są dane osobowe a nie danych w szerszym znaczeniu gromadzonych i przetwarzanych w UMiG (patrz KRI). W momencie wydania Zarządzenia 144/2015 wprowadzona PBPDO nie uwzględniała Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie KRI.

	Przez 7 lat Administrator praktycznie nie podjął żadnego wysiłku w celu aktualizacji dokumentacji, procedur, procesów wdrożonych Zarządzeniem 144/2015. Podpisana umowa z firmą zewnętrzną na świadczenie usług IODO zobowiązywała Zleceniobiorcę do wykonania określonych czynności (patrz załącznik numer 1 do umowy) w określonych terminach. Terminy te zostały znacznie przekroczone a stan na dzień kontroli wygląda tak iż UMiG nie posiada PBI która uwzględniałaby KRI. Umowa z firmą zewnętrzną dotyczy znów tylko i wyłącznie ochrony szczególnych danych jakimi są dane osobowe a nie danych w szerszym znaczeniu.
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 kontrolującemu została przedłożona dokumentacja z lat 2015-2021. Dokumentacja „Rejestr Ryzyk" zawiera zidentyfikowane ryzyka ich istotność, przyczyny, ewentualne skutki oraz proponowane mechanizmy kontrolne dla określonych zadań na konkretnych stanowiskach np. przyznawanie i wypłata świadczenia wychowawczego. Podobnie dokumentacja zatytułowana „Analiza Ryzyk" praktycznie zawiera te same informacje co „Rejestr Ryzyk". Informacje dotyczą konkretnego zadania na konkretnym stanowisku np. przyznawanie i wypłata świadczenia wychowawczego. Analiza ryzyk odbywa się na podstawie Zarządzenia Burmistrza Miasta i Gminy Małogoszcz nr 0050.(10 i 12).1023 z dnia 7 litego 2013 roku o kontroli zarządczej. Wyżej wymienione dokumenty nie mają nic wspólnego z analizą ryzyka w rozumieniu KRI czyli ryzyka utraty integralności, dostępności, poufności informacji oraz podejmowania działań minimalizujących ryzyko stosownie do przeprowadzonej analizy ryzyka. (Patrz KRI paragraf 20, punkt 2, podpunkt 3). Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf
Ustalone nieprawidłowości	Brak przeprowadzania analizy ryzyka w rozumieniu KRI w latach 2015-2022 (Patrz KRI paragraf 20, punkt 2, podpunkt 3).
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	ASI przedłożył prowadzony przez siebie „Wykaz sprzętu komputerowego w UMiG". Zestawienie zawiera informacje typu: pokój w którym znajduje się obecnie sprzęt, imię i nazwisko pracownika, nazwa zestawu, monitor, oprogramowanie (wersja systemu plus wersja pakietu office), inne oprogramowanie (RESPONS, Źródło, Edicta itp), wyposażenie w UPS, urządzenia peryferyjne (drukarki, czytniki, skanery itp.) Dowód - akta kontroli plik: pobrane-dokumenty-Małogoszcz.pdf
Ustalone uchybienia	Inwentaryzacja sprzętu i oprogramowania oparta jest o rejestr prowadzony przez ASI w formie elektronicznej. Brak w wykazie urządzenia UTM, routera, switchy i innych urządzeń zamontowanych w pomieszczeniu serwerowni. Dokument nie posiada atrybutów takich jak podpis osoby prowadzącej wykaz oraz daty wytworzenia dokumentu.
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	Zespołowi kontrolnemu nie zostały przedłożony załącznik numer 1 do IZSI służący do nadawania, modyfikacji odbierania uprawnień w systemach informatycznych. Z przeprowadzonej rozmowy z ASI wynika, że załącznik nie był używane przez pracowników UMiG. Na załączniku numer 1 jest miejsce na podpis bezpośredniego przełożonego użytkownika systemu wraz z datą wystawienia załącznika oraz miejsce na podpis kierownika. Wynika z tego, że osoby, które zapoznały się z PBPDO (jest stosowne oświadczenie pracownika) nie stosowały się do PBPDO mając świadomość odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów (taki zapis jest na oświadczeniu oraz w IZSI patrz Rozdział II, paragraf 4 IZSI, punkt 4). Zespół Kontrolny przeanalizował upoważnienia kilku pracowników wraz z ich uprawnieniami w systemie RESPONS. W przypadku pracownika JŁ (brak oświadczenia), którego upoważnienie jest z dnia 1.09.2020 roku, upoważnienie odnosi się jedynie do zbioru KONTRAHENTÓW w systemie RESPONS pracownik ma dostęp do modułów: Kontrahenci, FK, Faktury, Budżet, Administracja. Być może jest tak, że upoważnienie do „zbioru" Kontrahentów wymaga dostępu do wyżej wymienionych modułów i uprawnień do modułów ale nie wynika to na pewno z upoważnienia.

	Dla pracownika KBK (brak oświadczenia) konto w systemie RESPONS zostało założone 3.09.2019 roku, pracownik ma uprawnienia w modułach Administracja, Gospodarka odpadami, grunty, kontrahenci, podatek od osób prawnych, windykacja. Zespół Kontrolny w teczce z upoważnieniami nie znalazł upoważnienia dla pracownika KBK. Podobnie jest z kontami pracowników KS (brak oświadczenia), MK konto w systemie RESPONS utworzone 31.12.2021 roku natomiast w teczce z upoważnieniami nie ma upoważnienia pracownika KS. Pracownik KR konto w systemie RESPONS utworzone 22.01.2021 roku, natomiast upoważnienie zostało podpisane dnia 24.02.2021 roku. Podobnie jak w przypadku poprzednich pracowników upoważnienie jest wystawione do zbiorów: podatki, ewidencja gruntów, zwrot podatku akcyzowego. Natomiast w systemie RESPONS pracownik ma uprawnienia do szeregu modułów być może uprawnienia są nadane właściwie ale nie wynika to z upoważnienia. Pracownik MZ ma upoważnienie wystawione 25.05.2018 roku, wymienionych jest kilka zbiorów do których jest uprawniony. Konto w systemie RESPONS zostało utworzone 13.02.2021 roku. uprawnienia nadane w systemie RESOPNS są do innych zbiorów niż to wynika z upoważnienia, Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf
ustalone nieprawidłowości	Brak jasnej jednoznacznej mającej atrybuty autentyczności, rozliczalności, niezaprzeczalności i niezawodności procedury służącej do nadawania, modyfikacji, odbierania uprawnień w systemach informatycznych. Brak przestrzegania przez pracowników UMiG obowiązującej PBPDO. Brak dokumentów świadczących o okresowych audytach uprawnień w systemach informatycznych.
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 podstawę do oceny	Zespołowi kontrolnemu zostały przedłożone listy szkoleń z lat 2017-2021 wraz z odręcznymi podpisami uczestników szkolenia. Szkolenia wewnętrzne z zakresu cytuję „Polityki Bezpieczeństwa Informacji w urzędzie Miasta i Gminy w Małogoszczu, Cyberbezpieczeństwem oraz Instrukcją Zarzadzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy". Dowód - akta kontroli plik

	pobrane-dokumenty-Małogoszcz.pdf
Ustalone uchybienia	Zespół Kontrolny ustalił szereg zaniedbań, związanych z procedurami, procesami, instrukcjami opisanymi w PBPDO i IZSI polegających na nie przestrzeganiu PBPDO (patrz punkty 2.4) co rzutuje na efekty przeprowadzonych szkoleń z tego zakresu.
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	PBPDO i IZSI nie zawierają opisanych, zdefiniowanych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Z rozmowy z ASI wynika iż połącznie zdalne zazwyczaj z podmiotami trzecimi (ZETO, Sygnity) są wykonywane, ale każde połączenie jest przez niego monitorowane. Dowód - akta kontroli plik: pobrane-dokumenty-Małogoszcz.pdf
Ustalone nieprawidłowości	Brak w PBPDO i IZSI zdefiniowanych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość
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 Kontrolnemu zostały przedłożone umowy z firmami ZETO (umowa opieki autorskiej, umowa powierzenia przetwarzania danych osobowych 2020) oraz SIGNITY (umowa licencyjna 2020-2021). Posiadają one zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf
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	W PBPDO i IZSI nie ma zdania na temat procedury zgłaszania incydentów. Praktycznie na dzień kontroli pracownicy UMiG nie wiedzą w jaki sposób zgłaszać incydenty, nie wiedza komu zgłaszać incydenty. Zespołowi Kontrolnemu został przedłożony załącznik 6 do PBPDO ale

	w obowiązującej PBPDO UMiG nie ma zdefiniowanego załącznika numer 6. Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf
Ustalone nieprawidłowości	Brak procedury lub instrukcji, brak szkoleń z zakresu zgłaszania incydentów w UMiG.
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	Zespołowi Kontrolnemu przedłożono dokumentację z dwóch audytów zewnętrznych przeprowadzonych w latach 2019-2020. Audytowi z roku 2019 poddano nie wiedzieć czemu PBI i IZSI wprowadzoną zarządzeniem 316/06 z dnia 31 lipca 2006 roku. W tym czasie obowiązywała już „nowa" PBI wprowadzona zarządzeniem 144/2015 roku. Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf
Ustalone uchybienia	Zastrzeżenia są do audytu z roku 2019 audytowano wówczas już nie obowiązującą PBI i IZSI.
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	ASI przedłożył zrzut ekranu z konsoli z systemu Iperius Backup, na którym widać zaplanowane tworzenie kopii zapasowych czterech zbiorów, podany jest dokładny czas wykonania ostatniej kopii oraz jej wynik (pomyślnie utworzono kopię zapasową). Podobnie ma się sprawa z systemem „Świadczenia Rodzinne" , został udostępniony zrzut z ekranu konsoli Firebird Backup Manager, gdzie zdefiniowano harmonogram wykonywania kopii zapasowych dla systemu „Świadczenia rodzinne", podano ścieżkę gdzie kopie mają być zapisywane. ASI przedłożył także dokument Art.23 „Zasady wykonywania kopii bezpieczeństwa" gdzie rozpisał systemy dla których wykonywane są kopie bezpieczeństwa, z jaką częstotliwością, i na których urządzeniach docelowo zapisywana jest kopia bezpieczeństwa i gdzie jest przechowywana. Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf Protokol_ogledzin_pomieszczen.pdf
Ustalone uchybienia	Brak przedłożonego Art. 23 w PBPDO oraz IZSI. Nie wiadomo

	z jakiego dokumentu pochodzi ww. artykuł.
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	System RESPONS (dawna PUMA) to specjalistyczny system obsługi jednostek samorządu terytorialnego. W ramach systemu funkcjonują między innymi moduły: Wyborcy – do wykonywania zadań z zakresu prowadzenia stałego rejestru wyborców oraz przeprowadzania wyborów i referendów oraz moduł Paliwa – do wykonywania zadań z zakresu zwrotu podatku akcyzowego zawartego w cenie oleju napędowego. ŹRÓDŁO to bezpłatna aplikacja ogólnopolska służąca do obsługi Systemu Rejestrów Państwowych. Jej główne funkcje to rejestracja aktów stanu cywilnego, wydawanie i unieważnianie dowodów osobistych, wykonywanie meldunków oraz wprowadzanie danych kontaktowych. CEIDG czyli Centralna Ewidencja i Informacja o Działalności Gospodarczej jest spisem przedsiębiorców, będących osobami fizycznymi, działających na terenie Polski. Spis prowadzony jest od 1 lipca 2011 r. w systemie teleinformatycznym przez ministra właściwego do spraw gospodarki na podstawie przepisów ustawy o swobodzie działalności gospodarczej. Oprogramowanie autorstwa firmy Sygnity służy do realizacji ustawowych zadań z zakresu: świadczeń rodzinnych, świadczeń wychowawczych, funduszu alimentacyjnego, dodatku osłonowego, programu „Czyste Powietrze" oraz zadań własnych gminy.
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	Budynek posiada 3 wejścia do budynku, w samym budynku mieszczą

faktycznego, stanowiące podstawę do oceny	się jeszcze następujące instytucje: Biblioteka Miejska, Miejsko-Gminny Ośrodek Pomocy Społecznej, Samorządowe Centrum Oświaty. Główne wejście zabezpieczone szklanymi podwójnymi drzwiami z zamkiem. Klucze do pomieszczeń zdawane i pobierane są w „boksie obsługi", gdzie przechowywane są w specjalnej szafie zamykanej na klucz. Brak kontroli wejść do serwerowni, tzn. kontrola jest ponieważ do serwerowni można jedynie wejść poprzez pokój ASI, natomiast brak jest ewidencji osób przebywających czasowo w serwerowni (sprzątający, serwis i inne osoby). Patrz Protokół oględzin pomieszczeń. Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf protokół_ogledzin_pomieszczen.docx
Ustalone uchybienia	Brak w pomieszczeniu serwerowni urządzeń monitorujących temperaturę oraz zadymienie. Brak rejestracji wejść do serwerowni.
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	Zespół kontrolujący sprawdził wybrane stacje robocze z systemem ŹRÓDŁO, Rejestr Wyborców, RESPONS (moduł dopłaty do paliw) i CEIDG pod kątem zabezpieczenia antywirusowego, zabezpieczenia podtrzymania napięcia, polityk wdrożonych na w systemie operacyjnym. Sprawdzono ustawienia polityki haseł. Na czas przeprowadzenia kontroli UMiG miał odpięte urządzenie UTM (ASI wyjaśnił że jest odpięty ze względów technicznych, nie spełnia określonych wymogów). UTMa czasowo zastąpiono routerem tplink ER7206. System (CentOS 6.10 wsparcie skończyło się w roku 2017, łaty w zakresie bezpieczeństwa wychodziły do roku 2020) na którym funkcjonuje oprogramowanie RESPONS jest mocno nieaktualny.

	Podobnie ma się z serwerem windows 2008 R2 (wsparcie dla systemu skończyło się w roku 2020). Polityka haseł (brak zarządzania domenowego) praktycznie nie opracowana i nie wdrożona na kontrolowanych stacjach roboczych (patrz Protokół oględzin z dnia 27 kwietnia 2022 roku). Jest to niezgodne z IZSI (patrz IZSI paragraf 6 punkty 3-7). Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf Protokol_ogledzin_pomieszczen.docx
Ustalone nieprawidłowości	Mocno nieaktualne oprogramowanie serwerów. Konfiguracja polityki haseł na sprawdzanych zestawach komputerowych nie jest zgodna z opisami zawartymi w PBPDO i IZSI. Brak przestrzegania zasad z PBPDO i IZSI.
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	Systemy ŹRÓDŁO, RESPONS posiadają mechanizmy do zarządzania kontami, uprawnieniami, hasłami do tych systemów. Posiadają funkcje umożliwiające odnotowywanie wykonywanych czynności na koncie administratora jak również na kontach użytkowników. Taka sama sytuacja dotyczy stacji roboczych, serwerów oraz urządzeń UTM. Dowód - akta kontroli plik : pobrane-dokumenty-Małogoszcz.pdf
Ustalone uchybienia	Logi z serwerów przechowywane są na tych serwerach. Brak kopii logów systemowych w innym miejscu, brak procedur przeglądania logów systemowych.
Ocena obszaru kontroli nr	Negatywna

2	
Obszar kontroli : 3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych	
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://malogoszcz.pl i www.malogoszcz.eobip.pl zostały przetestowane za pomocą oprogramowania NVDA (czytnik ekranu), zostały również wyświetlone w przeglądarce FireFox i EDGE. Strona https://malogoszcz.pl, ma problem z rozwijanym menu górnym (patrz aktualności, Miasto i Gmina, Urząd itd.). W przeglądarce Firefox, pozycja z menu górnego rozwija się poprzez naciśnięcie (stałe) klawisza ENTER w części przypadków jest to problematyczne, nieskuteczne rozwiązanie. Problematyczne jest też poruszanie się po rozwiniętym menu klawiszem TAB. Opisana funkcjonalność lepiej działa w przeglądarce EDGE. Strony startowe posiadają zdefiniowane skróty klawiaturowe (ATL+ 0 początek strony, ATL+1 przejdź do wyszukiwarki, ALT + 3 przejdź do danych kontaktowych, ALT +4 przejdź do menu górnego, ALT +6 przejdź do menu prawego, ALT+7 przejdź menu dolnego, ALT+8 przejdź do menu bocznego, ALT +9 przejdź do mapy serwisu). W stopce strony znajduje się opublikowana deklaracja dostępności, mapa serwisu do tych funkcjonalności dostęp za pomocą klawiatury jest utrudniony (strona nie podąża za klawiszem TAB). Nie działa lub działa w sposób niewłaściwy przycisk do zmiany kontrastu. Przycisk zmiany wielkości czcionki działa właściwie. Strona www.malogoszcz.eobip.pl, posiada jedynie przycisk do zmiany kontrastu. Wybranie pozycji rozwijanej z menu prawego (np. Władze gminy, Organy gminy) powoduje rozwinięcie tego menu ale przejście na pozycje rozwiniętej jest problematyczne ponieważ kursor ustawia się za każdym razem na pozycji początkowej na stronie i należy porządnie się naklikać klawiszem TAB aby przejść do pozycji rozwiniętej. Tak jest z każdym rozwijaną pozycją z menu prawego. Zamieszczona wyszukiwarka (górny lewy róg strony) działa niewłaściwie np. wpisano adres skrytki epuap „/otig124o8w/skrytka", wpisano RODO za każdym razem otrzymano komunikat „Nie znaleziono artykułów".
Ustalone uchybienia	Niewielkie niedociągnięcia jeżeli chodzi o funkcjonalność strony: górne menu, rozwijanie, poruszanie się, dostępność deklaracji dostępności i mapy strony (przeglądarka nie podąża za klawiszem TAB). Strona BIP - źle działająca wyszukiwarka, brak funkcjonalności dla osób słabo widzących (tylko zmiana kontrastu), problematyczne poruszanie się po stronie.
Ocena obszaru kontroli nr	Pozytywna z uchybieniami

3	
Zalecenia	1. Dokonywać regularnych przeglądów dokumentacji dotyczącej bezpieczeństwa informacji. 2. Dokumentacja dotycząca bezpieczeństwa informacji powinna obejmować wszystkie dane przetwarzane w jednostce, a nie tylko dane osobowe. 3. Przeprowadzać regularnie analizę ryzyka utraty integralności, dostępności lub poufności informacji zgodnie z KRI. 4. Zapewnić rozliczalność rejestru sprzętu i oprogramowania, uwzględnić w rejestrze także urządzenia UTM, routera, switchy i innych urządzeń zamontowanych w pomieszczeniu serwerowni. 5. Wprowadzić procedurę nadawania, modyfikacji, odbierania uprawnień w systemach informatycznych posiadającą atrybuty autentyczności, rozliczalności, niezaprzeczalności i niezawodności. 6. Przeprowadzać okresowe audyty uprawnień w systemach informatycznych. 7. Zdefiniować w dokumentacji podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. 8. Opracować i wdrożyć procedurę w zakresie zgłaszania incydentów naruszenia bezpieczeństwa informacji. 9. W miarę możliwości wprowadzić w serwerowni monitorowanie temperatury i zadymienia. 10. Wdrożyć rejestr wejść do serwerowni. 11. W miarę możliwości zapewnić aktualizację oprogramowania serwerów do wersji wspieranych przez producentów. 12. Wdrożyć politykę haseł na stacjach roboczych. 13. Wykonywać kopie logów systemowych na serwerach i przechowywać je w innym miejscu niż macierzyste serwery. 14. W miarę możliwości poprawić funkcjonowanie wyszukiwarki na stronie BIP oraz funkcjonalności dla osób słabo widzących.

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