Urząd Miasta i Gminy w Łagowie
wpłynęło dnia:
01-04-2020
ilość załączników .....
poz. 3382 podpis .....

Świętokrzyski Urząd Wojewódzki
25-516 Kielce
Aleja IX Wieków Kielc 3 / _

OK.VIII.431.1.2020.MR

Kielce, 2020-04-01

WYSTĄPIENIE POKONTROLNE

Korespondencja wysłana z systemu EZD PUW

W załączeniu przesyłam wystąpienie pokontrolne z kontroli działania systemów teleinformatycznych, używanych do realizacji zadań zleconych z zakresu administracji rządowej, przeprowadzonej w Urzędzie Miasta i Gminy w Łagowie w dniach 12-14 lutego 2020r.

Załączniki:

1. Wystąpienie pokontrolne.pdf

Dokument został podpisany, aby go zweryfikować należy użyć oprogramowania do weryfikacji podpisu
Data złożenia podpisu: 2020-04-01T06:24:02.469Z
Podpis elektroniczny

WOJEWODA ŚWIĘTOKRZYSKI

Kielce, dnia 01-04-2020

Znak: OK.VIII.431.1.2020

Pan Paweł Marwicki
Burmistrz Miasta i Gminy
w Łagowie

Wystąpienie pokontrolne

Kontrolę w Urzędzie Miasta i Gminy w Łagowie, ul. Rynek 62 w dniach 12-14 lutego 2020r. przeprowadził zespół kontrolerów w składzie:

Marek Rak - Informatyk Wojewódzki, na podstawie pisemnego upoważnienia do przeprowadzenia kontroli numer 55/2020 z dnia 10.02.2020 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 56/2020 z dnia 10.02.2020 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 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	Urząd Miasta i Gminy w Łagowie **nie opublikował** na stronie głównej informacji w jaki sposób w UMiG można składać dokumenty w formie elektronicznej, na jakich nośnikach i w jakich formatach. Na stronie głównej www.lagowgmina.pl został umieszczony jedynie skrót do portalu epuap.gov.pl. Na stronie BIP pod zakładką Elektroniczna Skrzynka Podawcza zostały jedynie umieszczone dane adresowe, konta bankowe, kilka kont pocztowych pracowników UMiG brak jest natomiast informacji o skrytce w systemie epuap lub linku do niej, brak informacji o możliwości składania dokumentów w formie elektronicznej. Jedynie na BIP w zakładce „Składanie dokumentów do podatków drogą elektroniczną" opublikowano link do wzorów dokumentów do pobrania, które należy złożyć w UMiG w formacie pdf jedynie za pomocą adresu poczty elektronicznej na adres urzad@lagowgmina.pl oraz za pomocą platformy epuap. Zamieszczono informację o podpisywaniu dokumentów w formacie pdf. Podczas kontroli zespół stwierdził, że link do platformy epuap zamieszczony na tej stronie BIP jest nieaktualny gdyż po wejściu wyświetla się błąd. Dowód: akta kontroli plik : **www-bledny-link.jpg** **Link-skrytka.jpg**
Ustalone uchybienia, nieprawidłowości	Nieprawidłowy link do skrytki na platformie ePUAP na stronie BIP. Brak informacji o możliwości i sposobie składania dokumentów w postaci elektronicznej osobiście w UMiG w Łagowie. Brak informacji na jakich nośnikach takie dokumenty elektroniczne mogą być złożone.
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	W kontrolowanym okresie czyli w latach 2017-2019 UM i G w Łagowie nie przekazywał wzorów dokumentów do CRWDE gdyż nie uruchamiał nowych usług.
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 ramach projektu „Rozwój świętokrzyskiej e-administracji w gminach: Klimontów, Łagów, Obrazów, Ożarów" zostanie wdrożona otwarta platforma e-usług, cyfrowa platforma integrująca referencyjne i dziedzinowe zasoby informacyjne o charakterze opisowym i przestrzennym w celu ich publikacji oraz świadczenia związanych z nimi usług. Zostaną zmodernizowane programy dziedzinowe umożliwiające świadczenie e-usług wraz z migracją danych ze starych systemów; wdrożone zostaną formularze e-usług; zostanie zmodernizowane elektroniczne zarządzanie dokumentacją; wdrożony zostanie moduł informacji przestrzennej we wszystkich gminach.
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	**PUMA /Platforma Uruchomieniowa Modułów Aplikacyjnych/** jest w pełni zintegrowanym systemem informatycznym wspomagającym realizacje zadań jednostek samorządu terytorialnego. System umożliwia podłączenie aplikacji napisanych w różnych technologiach programistycznych, z różnych systemów operacyjnych, a także daje możliwość integracji z systemami obiegu dokumentów oraz z internetowymi systemami obsługi obywatela tzn. zapewnia praktyczną realizację koncepcji e-Urzędu. **ŻRÓDŁO to** program do edycji oraz przetwarzania danych gromadzonych w Systemie Rejestrów Państwowych t.j. rejestr PESEL, dowody osobiste, rejestry stanu cywilnego, Centralny Rejestr Sprzeciwów oraz System Odznaczeń Państwowych.
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 spraw oraz wykonywania czynności kancelaryjnych jest system tradycyjny. W roku 2020 w ramach projektu „Rozwój świętokrzyskiej e-administracji w gminach: Klimontów, Łagów, Obrazów, Ożarów" między innymi zostanie wdrożony elektroniczny system obiegu 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	Wymiana danych systemach PUMA i ŹRÓDŁO z systemami wspomagającymi zapewniona jest przez eksport części danych w formacie XML.
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
Ocena obszaru kontroli nr 1	**Pozytywna z nieprawidłowościami**
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	Zespołowi kontrolującemu przedłożono Zarządzenie nr 96/2018 Burmistrza Miasta i Gminy Łagów z dnia 20 września 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy Łagów. **Wykonanie zarządzenia powierzono Inspektorowi Ochrony Danych Osobowych**. Załącznik nr. 2 do wyżej wymienionego zarządzenia tj. Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych przedłożono zespołowi kontrolującemu po siedmiu godzinach od rozpoczęcia kontroli (podobno pracownicy nie mogli zaleźć załącznika nr 2). Tymczasem oba dokumenty czyli PBPDO oraz załącznik nr.2 do PBPDO powinny być dostępne dla pracowników UMiG w Łagowie tak aby każdej chwili mogli się nim wspierać w codziennej pracy. Wszystkie wyżej wymienione dokumenty tj. Zarządzenie nr 96/2018 Burmistrza Miasta i Gminy w Łagowie, załącznik nr 1 Polityka Bezpieczeństwa Przetwarzania Danych Osobowych oraz załącznik nr 2 Instrukcja Zarządzania systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych **dotyczą jedynie ochrony szczególnych danych jakimi są dane osobowe**, natomiast zbiór danych przetwarzanych, gromadzonych w UMiG w Łagowie jest znacznie szerszy i również powinien podlegać odpowiedniej ochronie, sposób ochrony pozostałych danym powinien być ujęty w wyżej wymienionej dokumentacji. Należałoby również całość dokumentacji wprowadzonej Zarządzeniem 96/2018 Burmistrza Miasta i Gminy w Łagowie z dnia z dnia 20 września 2018 roku dostosować do wymogów KRI tak aby wytworzona dokumentacja posiadała atrybuty autentyczności, rozliczalności, niezaprzeczalności i niezawodności. Przedłożona zespołowi kontrolującemu dokumentacja wprowadzona Zarządzeniem nr 96/2018 z dnia 20 września 2018 roku, tj. załącznik nr 1 i 2 wygląda tak jakby została skopiowana z dokumentacji innej instytucji i nie została dopasowana, dostosowana do wymogów i specyfiki UMiG w Łagowie oraz nie została wdrożona w pełnym zakresie. Przykładem tego może być punkt 4 strona 10, PBDO UMiG w Łagowie, gdzie napisano, że zestaw dokumentacji PBPDO składa się z dziewięciu dokumentów z tego 2 wymienione poniżej nie zostały wytworzone oraz wdrożone: - opis struktury zbiorów danych osobowych - opis przepływu danych pomiędzy poszczególnymi systemami Cytuję „*Wyżej wymienione dokumenty będą prowadzone w formie odrębnej dokumentacji, **przez Inspektora Ochrony Danych Osobowych** na podstawie wzorów stanowiących załączniki do niniejszej PBPDO*". Jeżeli z jakiś powodów wyżej wymienione dokumenty są zbędne lub niepotrzebne w UMiG lub w praktyce nie są wykorzystywane, IODO powinien dokonać przeglądu przynajmniej raz w roku PBPDO do czego jest zobowiązany między innymi umową IPZ.272.1.2020 i dokonać odpowiednich zmian. Zgodnie z wprowadzonym zarządzeniem Burmistrza Miasta i Gminy w Łagowie z dnia 20 września 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy Łagów w punkcie 12 na stronie 17 opisano procedurę dotyczącą uzyskania **upoważnienia do przetwarzania danych osobowych**. Napisano cytuję „upoważnienie wydaje się na wniosek Kierownika Komórki Organizacyjnej" ZAŁĄCZNIK NR 2. Zespół kontrolny ustalił że brakuje wniosków Kierownika Komórki Organizacyjnej do IODO na podstawie których IODO powinien wydać upoważnienie. Świadczy to o tym że powyższe osoby oraz inni pracownicy nie przestrzegają zapisów, procedur określonych w PBPDO, a po drugie nie zostali przeszkoleni w tym zakresie przez

	IODO. Oświadczenia osób dopuszczonych do przetwarzania danych osobowych a pełniących stanowiska Kierownicze w komórkach organizacyjnych zawierają następujący zapis w punkcie 2: „*zapoznałem/am się i rozumiem zasady dotyczące ochrony danych osobowych opisane w Polityce Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym oraz zobowiązuję się do ich przestrzegania*". Kierownicy Komórek organizacyjnych w tym również IODO oraz inni pracownicy UMiG w Łagowie nie przestrzegają więc zapisów PBPDO ustalonych w zarządzeniu Burmistrza MiG w Łagowie w roku 2018. Zgodnie z Instrukcją alarmową w przypadku wystąpienia zagrożenia lub incydentu naruszającego ochronę danych osobowych (patrz punkt 20 strona 22-24) zdefiniowano typowe zagrożenia bezpieczeństwa danych osobowych. Między innymi do typowych zagrożeń zaliczono „ ***niestosowanie zasad ochrony danych osobowych przez osoby upoważnione***" (patrz punkt 3), czyli w tym przypadku KKO oraz IODO nie przestrzegając zasad opisanych w PBPDO tworzą zagrożenie bezpieczeństwa przetwarzanych, gromadzonych danych osobowych w UMiG w Łagowie. Kolejne pytanie, dlaczego takie postępowanie nie zostało wykryte przez wyznaczone do tego celu osoby między innymi IODO i Audytora wewnętrznego (audyt w roku 2018) i nie została uruchomiona procedura alarmowa wystąpienia zagrożenia i incydentu naruszającego ochronę danych osobowych. Dlaczego o zaistniałej sytuacji nie został poinformowany Burmistrz Miasta i Gminy w Łagowie jako Administrator danych, dlaczego IODO nie podjął żadnych działań mających na celu usunięcia powyższych nieprawidłowości. Kolejnym przykładem niedostosowania dokumentacji wprowadzonej Zarządzeniem nr 96/2018 Burmistrza MiG w Łagowie do specyfiki pracy UMiG w Łagowie lub brakiem nadzoru nad wprowadzoną dokumentacją oraz przestrzeganiem opisanych w niej procedur jest załącznik numer 22 „Środki techniczne i organizacyjne **niezbędne** dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych dla lokalizacji UMiG w Łagowie". Dostarczony zespołowi kontrolującemu dokument zawiera następujący zapis: „*Klucze do poszczególnych pomieszczeń pracownicy pobierają i zdają po zakończeniu pracy* ***do sekretariatu*** ". Zespół kontrolny ustalił że pracownicy po zakończeniu pracy zabierają klucze od pokoi w których pracują w UMiG do domu. Klucze nie są pobierane ani zdawane w sekretariacie, ta procedura albo nie została przystosowana do specyfiki pracy w UMiG w Łagowie albo opisana procedura w PBPDO nie została wdrożona przez IODO. Kolejnym przykładem niedopełnienia obowiązków, nie wdrożenia procedur, nie przestrzegania PBPDO przez Kierowników Komórek Organizacyjnych, ASI a w szczególności IODO który jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury (patrz IZSI strona 13) jest **procedura nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym**. Brak dowodów stosowania załączników PRO_1_1 i PRO_1_2. Brak dokumentacji w tym zakresie, brak atrybutów świadczących o autentyczności, rozliczalności, niezaprzeczalności wyżej wymienionej procedury. Analogiczna sytuacja jak z opisaną wcześniej procedurą dotyczącą uzyskania **upoważnienia do przetwarzania danych osobowych.** Dodatkowo na stronie 3 załącznika PRO_1 jest zapis mówiący o tym że IODO w porozumieniu z ASI ma obowiązek okresowej kontroli i weryfikacji zasadności posiadanych przez użytkowników uprawnień, przynajmniej **raz na 3 miesiące** czyli co najmniej **3 razy w roku**. Brak jakiejkolwiek dokumentacji w tym zakresie. Może to świadczyć o tym, że kontrola okresowa nie jest i nie była wykonywana przez IODO.

	W przedłożonych Zespołowi kontrolującemu upoważnieniach do przetwarzania danych osobowych nie została wypełniona informacja **o nadanym identyfikatorze w systemie informatycznym.** Upoważnienie numer 220.385.4.2018 do przetwarzania danych osobowych jest niezgodne ze wzorem zamieszczonym w PBPDO a więc w dokumentacji wprowadzonej Zarządzeniem nr 96/2018 Burmistrza MiG w Łagowie w 2018 roku. Nie podano przyczyn tego stanu rzeczy. W IZSI (załącznik nr 2 do PBPDO) stosowany jest termin **Administrator Bezpieczeństwa Informacji,** który po wejściu w życie RODO został zastąpiony przez Inspektora Ochrony Danych Osobowych. Sytuacja ta świadczy o tym że IZSI już na wstępie czyli podczas tworzenia jej na potrzeby Zarządzenia nr 99/2018 Burmistrza Miasta i Gminy w Łagowie nie została odpowiednio przejrzana i poprawiona zgodnie ze specyfiką pracy UMiG w Łagowie również pod kątem obowiązującej terminologii. Zespół Kontrolny zwrócił też uwagę na tzw. hasła administratorów i ich przechowywanie. Kilkakrotnie bo i w załączniku PRO_2 w punkcie l) i w załączniku PRO_3 w punkcie 2 jest opisana procedura w tym zakresie. W załączniku PRO_3 w punkcie 2 jest zapis cytuje *„ASI jest zobowiązany do prowadzenia metryk haseł administratora i przechowywania ich w zamkniętych kopertach, odrębnych dla każdego systemu/aplikacji, w sejfie lub w szafie pancernej, do których dostęp ma wyłącznie ASI,ADO i Administrator Bezpieczeństwa Informacji*". Załącznik PRO_2 w punkcie l) jest zapis cytuje *„wyjątkiem jest zdeponowanie haseł użytkowników lub administratorów systemu w bezpiecznym miejscu (np. sejf, szafa pancerna), w zamkniętej kopercie opisanej nazwiskiem osoby upoważnionej do jej otwarcia*". W rzeczywistości wygląda to tak że ASI przechowuje hasła w jednej nieopisanej kopercie w pokoju numer 44 w zwykłej szafie zamykanej na zwykły klucz. Stan zastany przez zespół kontrolujący nie odpowiada zdefiniowanym procedurom i wymaganiom opisanym w obu załącznikach z IZSI, co po raz kolejny świadczy o tym że dokumentacja wprowadzona ww. zarządzeniem nie została poprawnie wdrożona oraz nie jest stosowana i przestrzegana przez osoby które zobowiązały się do jej przestrzegania poprzez złożenie własnoręcznie podpisu pod „Oświadczeniem". W szczególności dotyczy to IODO który jest odpowiedzialny za przygotowanie, wdrożenie oraz nadzór nad procesami, procedurami opisanymi w PBPOD i IZSI. Należy jeszcze zwrócić uwagę że oba zapisy w obu załącznikach nie są spójne. Zespół kontrolny ustalił, że Oświadczenia i Upoważnienia pracowników nie posiadają cech rozliczalności, autentyczności i niezaprzeczalności ponieważ nie zawierają bardzo istotnej informacji kiedy i z jaką datą oświadczenia, upoważnienia zostały wydane i podpisane przez oświadczającego. Brak na nich daty wystawienia. Takich cech nie nosi również pozostała część przedłożonych załączników z PBPDO. Zespołowi kontrolującemu została również przedłożona dokumentacja dotycząca likwidacji sprzętu znajdującego się na wyposażeniu UMiG w Łagowie z 12 lutego 2019 roku (40 pozycji, prośba o likwidację poprzez utylizację). W Załączniku nr 2 do PBPDO znajduje się opisana (patrz załącznik PRO_10) „Procedura niszczenia uszkodzonych/przestarzałych technologicznie nośników danych", do procedury dołączony jest wzór protokołu niszczenia uszkodzonych nośników danych. W wyżej wymienionym zestawieniu znajduje się klika notebooków i kilka zestawów komputerowych, ale nie ma tam mowy o nośnikach danych. Najwyraźniej nie zostały sporządzone protokoły zniszczenia nośników danych ze sprzętu który jest wymieniony na liście z dnia 12 lutego 2019 roku. Jest to kolejna procedura, która jest opisana na papierze ale w rzeczywistości nie jest należycie wykonywana.

	Dowód: akta kontroli plik : OK.VIII.432.1.2020 EZD : polityka bezpieczeństwa .pdf zarządzenie.pdf wykaz sprzętu 2020.doc Pobrane-dokumenty-UMiG-Łagów.pdf : IZSI strony 104-150 Załącznik nr.22 strony 53-59 Oświadczenia strony 13-16 Upoważnienia strony 8-12 2020-02-13-09-03-26-01-umowa-IODO.pdf
Ustalone uchybienia, nieprawidłowości	Brak w procedurach zapisów mających na celu ochronę wszystkich danych przetwarzanych, gromadzonych w UMiG w Łagowie, a nie jedynie danych osobowych. Podjęte przez Burmistrza Miasta i Gminy Łagów działania chronią jedynie **dane osobowe**. Dlatego dokumentacja nie jest zgodna z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Rozporządzenie to dotyczy wszelkich danych przetwarzanych w podmiocie publicznym. Dokumentacja PBPDO nie jest dostosowana do specyfiki pracy w UMiG w Łagowie, wdrożona jest jedynie częściowo, a jej postanowienia na co dzień i tak nie są przestrzegane przez pracowników urzędu a w szczególności przez IODO, Kierowników Komórek Organizacyjnych i przez ASI. Inspektor Ochrony Danych nie realizuje należycie swoich obowiązków określonych w umowie oraz dokumentacji. Brakuje kontroli ze strony Administratora Danych nad jego działaniami.
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 został przedłożony dokument pt.: „Analiza poufności, integralności i rozliczalności systemów informatycznych pod katem zagrożeń i ryzyka" zwany dalej „Analizą zagrożeń i ryzyka przy przetwarzaniu danych osobowych" z dnia 20.12.2018 roku. W załączniku numer 3 „Podatność systemu na zagrożenia" do wyżej wymienionego dokumentu w § 3 w punkcie 1 wymieniono czynności wykonane mające na celu ograniczenie podatności systemu na zagrożenia. Wymieniono między innymi: - przeglądy okresowe nośników - kontrolę konfiguracji - testowanie oprogramowania - audyt - zabezpieczenie haseł w punkcie 2 wymieniono prowadzenie odpowiedniej dokumentacji Zespołowi kontrolującemu nie została przedstawiona, przedłożona żadna dokumentacja świadcząca o tym że wyżej wymienione czynności są wykonywane, która posiadałaby zgodnie z KRI atrybuty autentyczności, rozliczalności i niezaprzeczalności. W załączniku nr 5 „Wnioski i działania naprawcze w związku z przeprowadzoną

	analizą ryzyka i zagrożeń przy przetwarzaniu danych osobowych" w § 4 jest zapis cytuję *„ADO w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy podejmuje działania naprawcze, polegające w szczególności na :"* w pozycji trzeciej zapisano cytuję ***„cykliczna weryfikacja zakresu przyznanych upoważnień"***. Zespół kontrolny ustalił że są to jedynie zapisy w dokumentacji. Brak dowodów, które jednoznacznie potwierdziłyby wykonywanie opisanych czynności przez upoważnione do tego celu osoby. Po raz kolejny tym razem w załączniku numer 8 twórca dokumentu powołuje się na to że została wdrożona PB i IZSI, a jak wynika z niniejszej kontroli PBPDO i IZSI została wdrożona częściowo i nie jest przestrzegana przez pracowników UMiG w Łagowie, a procedury, procesy w niej opisane funkcjonują w UMiG w Łagowie w szczątkowej formie. Została natomiast udostępniona dokumentacja w zakresie Audytu w roku 2018 wykonana przez Audytora wewnętrznego. Do tematu rzetelności i wiarygodności przeprowadzonego audytu w roku 2018 przez Audytora wewnętrznego zespół kontrolny odniósł się w punkcie 2.9 niniejszego dokumentu. Dowód: akta kontroli plik : Wersja papierowa dokumentu „Analiza poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka" zwana dalej „Analizą zagrożeń i ryzyka przy przetwarzania danych osobowych"
Ustalone uchybienia, nieprawidłowości	Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowy została wykonana, tzn. stworzono odpowiedni dokument. Natomiast opierając się o stworzony dokument dotyczący analizy ryzyka zespół kontrolny ustalił, że nie zostały podjęte odpowiednie czynności które są wymienione w na stronie numer 13 i 14 analizy ryzyka. **Nie podjęto również działań naprawczych** określonych na stronie 19 analizy ryzyka. Czyli teoretycznie przeprowadzono analizę ryzyka ale w praktyce nie podjęto działań wynikających z tej analizy. Zespołowi kontrolującemu nie przedłożono żadnej dokumentacji w tym zakresie.
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 kontrolującemu została przedłożona dokumentacja dotycząca inwentaryzacji sprzętu i oprogramowania, stan na dzień 21.01.2020. Dostarczono wykaz sprzętu w formie tabelki zawierającej jedynie nazwę sprzętu np. Komputer przenośny Toshiba czy Tablety 18 szt. Dowód: akta kontroli plik : OK.VIII.432.1.2020 EZD : wykaz sprzętu 2020.doc
Ustalone uchybienia, nieprawidłowości	Dostarczono wykaz sprzętu w formie tabelki zawierającej jedynie nazwę sprzętu. Wykaz ten nie spełnia wymogów określonych w KRI czyli nie posiada informacji obejmującej rodzaj i konfigurację sprzętu i oprogramowania używanego w UMiG w Łagowie na dzień kontroli.
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	Zasady nadawania, modyfikowania, odbierania uprawnień w systemach informatycznych w praktyce według PBPDO UMiG w Łagowie powinny być oparte na procedurze i dokumentacji zdefiniowanej w IZSI (patrz załącznik PRO_1 i PRO_2). Zespół kontrolny ustalił że żaden z tych formularzy praktycznie nie jest używany a tym samym procedura, proces z PBPDO UMiG w Łagowie nie jest przestrzegany co jest równoznaczne z tym że pracownicy UMiG w Łagowie nie stosują Zarządzenia nr 96/2018 Burmistrza MiG w Łagowie z roku 2018 oraz mimo podpisanego Oświadczenia nie przestrzegają PBPDO w UMiG w Łagowie. W IZSI w załączniku PRO_1 strona 7 zapisano, że *„IOD w porozumieniu z ASI ma obowiązek okresowej kontroli i weryfikacji zasadności posiadanych przez użytkowników uprawnień przynajmniej raz na 3 miesiące*". Brak jakiejkolwiek dokumentacji, która potwierdziłaby wykonanie kontroli i weryfikacji w tym zakresie. Analogiczna sytuacja związana jest z procedurą dotyczącą uzyskania **upoważnienia do przetwarzania danych osobowych**. Napisano cytuję „upoważnienie wydaje się na wniosek Kierownika Komórki Organizacyjnej" ZAŁĄCZNIK NR 2. Zespół kontrolny ustalił że brakuje wniosków Kierowników Komórek Organizacyjnych do IODO na podstawie których IODO powinien wydać upoważnienie. Ponownie procedury zdefiniowane w PBPDO w UMiG w Łagowie nie są przestrzegane przez pracowników UMiG. W załączniku nr 5 „Wnioski i działania naprawcze w związku z przeprowadzoną analizą ryzyka i zagrożeń przy przetwarzaniu danych osobowych" w § 4 cytuję *„ADO w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy podejmuje działania naprawcze, polegające w szczególności na :*" w pozycji trzeciej zapisano cytuję *„**cykliczna weryfikacja zakresu przyznanych upoważnień**".* Dowód: akta kontroli plik : OK.VIII.432.1.2020 EZD : polityka bezpieczeństwa .pdf zarządzenie.pdf Pobrane-dokumenty-UMiG-Łagów.pdf : IZSI strony 104-150 Oświadczenia strony 13-16 Upoważnienia strony 8-12
Ustalone uchybienia, nieprawidłowości	28 września 2018 roku Burmistrz Miasta i Gminy w Łagowie wydając Zarządzenie nr 96/2018 zobowiązał wszystkich pracowników Urzędu do zapoznania się z treścią PBPDO oraz powierzył wykonanie zarządzenia IOD. Zespół kontrolny ustalił, że procedury związane z zarządzaniem uprawnieniami do pracy w systemach informatycznych określone w PBPDO MiG w Łagowie do dnia kontroli tj. luty 2020 nie zostały wdrożone przez IOD oraz nie są przez niego monitorowane zgodnie z zapisami PBPDO UMiG w Łagowie. Pomimo tego że każdy z pracowników UMiG w Łagowie podpisał własnoręcznie Oświadczenie o zobowiązaniu się do przestrzegania zasad, dokumentacji, procedur zawartych w PBPDO tych zasad nie przestrzega się. W tym przypadku dotyczy to bezpośrednio Kierowników Komórek Organizacyjnych, IOD i ADO.

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 kontrolującemu została przedłożona dokumentacja dotycząca szkoleń przeprowadzonych przez IODO w latach 2017-2018. Przedłożono jedynie listy obecności wraz z podpisami uczestników szkolenia. Szkolenie zatytułowano „Szkolenie z ochrony danych osobowych". Nie przedstawiono konspektów do szkoleń, które jednoznacznie określałyby ich zakres. Zespół kontrolny ustalił że po 20 września 2018 roku czyli po wprowadzeniu przez Burmistrza Miasta i Gminy w Łagowie Zarządzenia nr 96/2018, IODO nie przeprowadził szkolenia wszystkich pracowników UMiG w Łagowie w zakresie stosowania Polityki Bezpieczeństwa Przetwarzania Danych Osobowych. Przeszkolonych zostało jedynie dwóch pracowników w tym zakresie. Z listy dostarczonej z działu Kadr urzędników zatrudnionych w okresie 2017-2020 w UMiG w Łagowie wynika że przynajmniej trzech osób z tej listy nie ma na listach obecności ze szkoleń. IODO tłumaczył to tym że zrezygnował z prowadzenia dokumentacji dotyczącej przeprowadzonych szkoleń i twierdzi że te osoby zostały przeszkolone. Zespół kontrolny zwraca uwagę na to że dokumentacja ze szkoleń lub dokumentacja dotycząca szkoleń zgodnie z wytycznymi KRI powinna nosić atrybuty autentyczności, rozliczalności i niezaprzeczalności oraz powinna dotyczyć następujących zagadnień: a) zagrożeń bezpieczeństwa informacji b) skutki naruszenia bezpieczeństwa informacji, w tym odpowiedzialność prawna c) stosowanie środków zapewniających bezpieczeństwo informacji Brak jest natomiast konspektów do przeprowadzonych szkoleń a z samych list nie wynika z jakiego zakresu byli szkoleni pracownicy UMiG przez IODO. Dowód - akta kontroli plik: Pobrane-dokumenty-UMiG-Łagów.pdf : Szkolenia z zakresu ochrony danych osobowych strony 2-7 IZSI strony 104-150 Oświadczenia strony 13-16 Upoważnienia strony 8-12 Wykaz urzędników zatrudnionych w UMiG w Łagowie w okresie 01.10.2017 do 12.02.2020 i aktualnie pracujących, strona 1
Ustalone uchybienia, nieprawidłowości	Dokumentacja dotycząca szkoleń powinna zawierać atrybuty autentyczności, rozliczalności, niezaprzeczalności. Osoba szkoląca powinna opracować konspekt do każdego szkolenia z którego jednoznacznie by wynikało jakie tematy i zagadnienia poruszało szkolenie. Nie może być tak że IODO decyduje się na nie prowadzenie dokumentacji związanej ze szkoleniami i uważa, że jeżeli osoba dostała upoważnienie jest to równoznaczne z tym że odbyła odpowiednie szkolenie. To co ustalił zespół kontrolny sugeruje, że IODO nie przeprowadził szkoleń z PBPDO wdrożonej zarządzeniem nr 96/2018 Burmistrza MiG w Łagowie lub szkolenie były na tak niskim poziomie co w konsekwencji doprowadziło do tego, że PBPDO

	w UMiG w Łagowie nie jest przestrzegana. Taki stan rzeczy trwa od roku 2018.
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	Zgodnie z Rozporządzeniem z dnia 12 kwietnia 2012 roku w sprawie KRI minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych § 20 ust.2 punkt 8 UMiG w Łagowie powinien ustanowić zasady określające bezpieczną pracę na odległość. Zasady te powinny być ustalone, ponieważ z umowy serwisowej systemu dziedzinowego PUMA z dnia 22.12.2017 roku pomiędzy Gminą Łagów a firmą ZETO SOFTWARE (patrz § 1, punkt 25) wynika że po stronie zamawiającego jest zapewnienie zdalnego dostępu do systemu. W PBPDO UMiG w Łagowie zespół kontrolny nie znalazł opisanej procedury mającej na celu zdefiniowanie i opisanie procesu służącego do realizacji połączeń zdalnych. Dowód: akta kontroli plik : OK.VIII.432.1.2020 EZD : polityka bezpieczeństwa .pdf Pobrane-dokumenty-UMiG-Łagów.pdf : Umowy ZETO SOFTWARE strony 60-86 IZSI strony 104-150
Ustalone uchybienia, nieprawidłowości	W dokumentacji wprowadzonej Zarządzeniem nr 96/2018 Burmistrza Miasta i Gminy w Łagowie z dnia 20 września 2018 nie zdefiniowano podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość z uwzględnieniem atrybutów autentyczności, rozliczalności, niezaprzeczalności i niezawodności.
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	Zespół kontrolny zapoznał się z umowa opieki autorskiej Systemu PUMA nr 17/1455/JU zawarta z ZETO SOFTWARE w dniu 22.12.2017 r. z okresem obowiązywania od 25.12.2017r. do 31.12.2020r. Druga wersja tej umowy o tym samym numerze z okresem obowiązywania od 1.03.2018 do 31.12.2018r. Do tej drugiej wersji umowy serwisowej przedłożono również umowę powierzenia przetwarzania danych nr 17/1593/JU zawartą z ZETO SOFTWARE w dniu 3.01.2018r z okresem obowiązywania od 01.01.2018 do 31.12.2018r. Umowy powierzenia przetwarzania danych osobowych dla ZETO odnoszącej się do tej umowy z okresem obowiązywania od 25.12.2017r. do 31.12.2020r. nie przedłożono. Zespołowi kontrolującemu nie przełożono też żadnych umów dotyczących serwisu sprzętu komputerowego. ASI utrzymuje ze wszelkie naprawy sprzętu wykonywane są własnymi siłami. Przedłożono dokument „Prośba o likwidację sprzętu z dnia 12.02.2019", oraz o powołaniu komisji w tej sprawie. Nie przedłożono jednak żadnych zapisów dotyczących tej sprawy. Stary sprzęt komputerowy w tym nośniki danych zostały zlikwidowane, tzn. zdjęte ze stanu posiadania lecz nie zostały zutylizowane i nie opuściły budynku urzędu.

	Dowód - akta kontroli pliki: Pobrane-dokumenty-UMiG-Łagów.pdf : Prośba o likwidację sprzętu z 12.02.2018 strona 29-30 Umowa Powierzenia Przetwarzania Danych Osobowych nr 17/1593/JU §1 ust. 1
Ustalone uchybienia, nieprawidłowości	Brak dokumentacji dotyczącej likwidacji wycofanego sprzętu komputerowego, w tym brak dokumentacji dotyczącej niszczenia trwałego nośników z danymi np. dysków z wycofanego sprzętu komputerowego. Brak aktualnie obowiązującej umowy powierzenia przetwarzania danych osobowych dla ZETO związanej z przetwarzaniem danych osobowych w systemie PUMA.
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 dokumentacji wprowadzonej Zarządzeniem nr 96/2018 Burmistrza MiG w Łagowie zdefiniowano procesy związane z postępowaniem w sytuacjach naruszenia ochrony danych osobowych (patrz załącznik nr 16, punkt 3). Procedura zgłaszania naruszenia bezpieczeństwa informacji raz mówi o tym że zgłoszenie naruszenia należy zgłosić do swojego bezpośredniego przełożonego, a w innym miejscu jest napisane że osobą odpowiedzialną za przyjęcie zgłoszenia jest ASI. W punkcie 20 PBPDO (strona 23) znajduje się następujący zapis: „*W przypadku stwierdzenia zagrożenia lub incydentu naruszenia ochrony danych osobowych, należy niezwłocznie poinformować o tym fakcie IODO. W przypadku braku możliwości zawiadomienia IODO należy powiadomić ???????*” to już trzecia osoba do której według przedłożonej zespołowi kontrolującemu dokumentacji pracownik ma obowiązek zgłosić naruszenie. W razie niemożliwości zawiadomienia IODO ma zawiadomić kogo ?(pytajniki). Wygląda to tak jakby procedura nie była ukończona. Dalej napisano że informację należy składać osobiście lub telefonicznie. biorąc pod uwagę fakt że IODO nie ma na miejscu w budynku UMiG w Łagowie nie podano konkretnego numeru telefonu na który należy dzwonić do IODO. W dalszej części PBPDO podano jakie informacje ma przekazać osoba zgłaszająca : 1.imię i nazwisko 2.miejsce i czas wystąpienia zagrożenia lub incydentu 3.opis sytuacji Ma się to nijak do wymienianego już wcześniej załącznika 16 do PBPDO (patrz strona 2 tego załącznika). Dowód: akta kontroli plik : OK.VIII.432.1.2020 EZD : polityka bezpieczeństwa .pdf Pobrane-dokumenty-UMiG-Łagów.pdf : IZSI strony 104-150
Ustalone uchybienia, nieprawidłowości	Procedura zgłaszania naruszenia ochrony danych osobowych (patrz załącznik nr 16 do PBPDO) w innym miejscu zwana również Instrukcją alarmową w przypadku wystąpienia zagrożenia lub incydentu naruszającego ochronę danych osobowych (patrz PBPDO strona 22 i 23) nie zawiera kluczowych informacji. Nic z tych dokumentów nie wynika. Nadal nie wiemy do kogo pracownik ma zgłosić incydent, nadal nie wiemy kto zastępuje IODO w momencie kiedy nie można się z nim skontaktować, i czy IODO jest właściwą osobą której pracownik ma zgłosić incydent. Nie wspomnę o merytorycznym chaosie dotyczącym informacji jakie ma zebrać a następnie przekazać pracownik który zgłasza incydent, w jakiej formie i komu bezpośrednio.

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 kontrolującemu została udostępniona dokumentacja tzw. Plan audytu wewnętrznego na rok 2018 który obejmować miał: 1.Audyt bezpieczeństwa teleinformatycznego (wykonywany co roku) 2.Ocenę systemu zarządzania bezpieczeństwem informacji na przykładzie wybranych zagadnień realizowanych w UMiG w Łagowie oraz dokumentację z samego audytu. Przedłożono również Sprawozdanie z audytu z roku 2018. Jednym w celów audytu było cytuję „*Weryfikacja wymagań w zakresie zarzadzania bezpieczeństwem informacji wynikających z § Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*". Powyższe sprawozdanie z audytu potwierdza zgodność systemu zarządzania bezpieczeństwem informacji z powyższymi wymaganiami. To co ustalił zespół kontrolny w czasie kontroli w dniach 12-13 lutego 2020 r. rozmija się kompletnie z opinią audytora wewnętrznego zawartą w sprawozdaniu. Proszę zwrócić uwagę, że zakres, cel i obszar przeprowadzonego audytu przez audytora wewnętrznego w roku 2018 jest identyczny jak zakres, cel i obszar kontroli prowadzonej przez zespół kontrolny w roku 2020 w ramach tej kontroli. Nasze ustalenia są jednak inne i zostały opisane w niniejszym dokumencie. Zespół kontrolny nie zgadza się z audytorem wewnętrznym w kwestiach określonych w KRI w § 20 od punktu 2-14. Dowód: akta kontroli plik : OK.VIII.432.1.2020 EZD : polityka bezpieczeństwa .pdf Pobrane-dokumenty-UMiG-Łagów.pdf : IZSI strony 104-150 Plan audytu wewnętrznego 2018 strony 31-33 Plan audytu wewnętrznego 2019 strony 34-36 Sprawozdanie z przeprowadzonego audytu wewnętrznego 2018 strony 37-52
Ustalone uchybienia, nieprawidłowości	Audyt przeprowadzony przez audytora wewnętrznego zdaniem zespołu kontrolnego rozmija się z ustaleniami Zespołu Kontrolnego w każdym kontrolowanym przez audytora wewnętrznego obszarze. Audyt zaplanowany na rok 2019 nie został przeprowadzony.
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	Zespołowi kontrolującemu została przedłożona dokumentacja świadcząca o wykonywaniu przez ASI kopii zapasowych danych. Zostały przedłożone zrzuty ekranów z konsoli Cobian Backup Gravity 11 świadczące o tym że kopie są zaplanowane na każdy dzień tygodnia na godzinę 20.00 z wyjątkiem sobót i niedziel. Natomiast w dokumentacji dotyczącej PBPDO wprowadzonej Zarządzeniem nr 96/2018 Burmistrza MiG w Łagowie w roku 2018 nie ma zdefiniowanych procedur które w jednoznaczny sposób wskazują kiedy, kto wykonuje, na jakie nośniki i gdzie

	są przechowywane kopie danych, zbiorów danych, systemów. Brak jest również dokumentacji mówiącej o tym że prowadzone są w jakimś odstępnie czasu testy odtwarzania danych z kopii zapasowych przez ASI. ASI poinformował zespół kontrolny że takie testy wykonuje, ale nie prowadzi żadnej dokumentacji w tym zakresie. Dowód - akta kontroli plik : OK.VIII.432.1.2020 EZD : polityka bezpieczeństwa .pdf Pobrane-dokumenty-UMiG-Łagów.pdf : Zrzuty ekranu Cobian Backup 11 Gravity strony 89-91
Ustalone uchybienia, nieprawidłowości	W dokumentacji wprowadzonej Zarządzeniem nr 96/2018 Burmistrza Miasta i Gminy w Łagowie z dnia 20 września 2018 roku brak opisanych procedur, procesów, schematów, harmonogramów wykonywania kopii zapasowych danych, kopii zapasowych systemów pracujących w Urzędzie Miasta i Gminy w Łagowie. Brak dokumentacji prowadzonej przez ASI dotyczącej odtwarzania danych z kopii zapasowych.
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 PUMA (platforma uruchomieniowa modułów aplikacyjnych) to system wspomagający działalność urzędów administracji publicznej i ich jednostek organizacyjnych został wdrożony w ramach projektu e-świętokrzyskie. ŹRÓDŁO to bezpłatna aplikacja ogólnopolska służąca do obsługi Systemu Rejestrów Państwowych
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	Zespół kontrolny sprawdził zabezpieczenia fizyczne (monitoring, wejścia do budynku, pomieszczenie serwerowni) w czasie przeprowadzonych oględzin (patrz protokół oględzin). Dowód - akta kontroli plik : Protokol_ogledzin_pomieszczen.doc
Ustalone	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**

uchybienia, nieprawidłowości	
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 systemami PUMA, ŹRÓDŁO pod kątem zabezpieczenia antywirusowego, przeciwprzepięciowego, zostały sprawdzone ustawienia wygaszaczy ekranów. W dwóch przypadkach parametry wygaszaczy nie były ustawione. Sprawdzono konfiguracje urządzenia FortiGate (dostarczono zrzut ekranu z konsoli) z którego wynika że przynajmniej od roku 2017 (urządzenie trafiło do UMiG w Łagowie w roku 2016 z wykupionymi rocznymi licencjami) nie wykupiono licencji i w tym momencie urządzenie działa jako zwykły router, niczego nie filtruje i przed niczym nie zabezpiecza. Antywirus, IPS, antyspam i filtrowanie stron nie działa. Zespół kontrolny ustalił również że Serwer plików pracuje na systemie operacyjnym **Windows 2003 R2** którego wsparcie przez producenta zakończyło się w lipcu 2015 roku a więc 5 lat temu. ASI twierdzi że jest planowana wymiana tego systemu w roku 2020. Pozostałe urządzenia tj. Serwer Bazy Danych i Serwer Druku, Serwer na którym zainstalowany jest system PUMA posiadają zainstalowane aktualizacje oraz systemy pod którymi pracują mają wsparcie producenta. Wymienione urządzenia są zainstalowane w szafie dystrybucyjnej, są podpięte do urządzenia podtrzymującego napięcie Cyberpower. Czas podtrzymania zasilania przez urządzenie Cyberpower przy pełnym obciążeniu szacowany jest na 40 minut. ASI utrzymuje że przeprowadził odpowiednie testy w tym zakresie. Brak jest natomiast dokumentacji potwierdzającej przeprowadzone testy przez ASI. Na stacjach roboczych (w części) zainstalowany jest system Windows 7 który w tym roku (styczeń) stracił wsparcie producenta. ASI utrzymuje że w jednym z projektów w których bierze udział UMiG w Łagowie jest zaplanowana wymiana tych urządzeń. Kontrolowany wyjaśnił, że licencje do urządzenia Fortigate zostaną zakupione z projektu pn. „Rozwój świętokrzyskiej e-administracji w gminach: Klimontów, Łagów, Obrazów, Ożarów". Nowe oprogramowanie systemowe, które zastąpi Windows 7 ma być dostarczone po wyłonieniu dostawcy w przetargu w marcu bieżącego roku. Dowód: akta kontroli plik : Protokol_ogledzin_pomieszczen.doc

	Pobrane-dokumenty-UMiG-Łagów.pdf : Konsola urządzenia FortiGate strona 17 Schemat sieci UMiG strona 18
Ustalone uchybienia, nieprawidłowości	W sieci urzędu działają urządzenia zabezpieczające nie posiadające już ważnych licencji i w związku z tym nie realizujące w pełni swoich funkcji. Występują też komputery z systemami operacyjnymi, które nie mają już wsparcia producenta. Wymóg dbałości o aktualizację oprogramowania nie jest spełniony.
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 PUMA, ŹRÓDŁO posiadają mechanizmy do zarządzania kontami, uprawnieniami, hasłami do tych systemów. Posiadają funkcję umożliwiającą odnotowanie wykonywanych czynności na koncie administratora jak również na kontach użytkowników. Taka sama sytuacja dotyczy stacji roboczych, serwerów oraz urządzenia FortiGate. Dowód - akta kontroli plik : Pobrane-dokumenty-UMiG-Łagów.pdf : Użytkownicy systemu PUMA i ich uprawnienia 2020-02-13 strony 151-155
Ustalone uchybienia, nieprawidłowości	**BRAK UCHYBIEŃ, NIEPRAWIDŁOWOŚCI**
Ocena obszaru kontroli nr 2	**Pozytywna z nieprawidłowościami**
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	Strona www.lagowgmina.pl została przetestowana za pomocą oprogramowania NVDA (czytnik ekranu). Swobodnie za pomocą klawisza TAB można poruszać się po poszczególnych pozycjach strony, menu, podmenu strony to samo tyczy się strony BIP. Strona www.lagowgmina.pl posiada możliwość powiększania czcionki, oraz posiada funkcjonalność zmiany kontrastu, która **nie działa.** Strona BIP nie posiada żadnej funkcjonalności w zakresie dostępności dla osób niepełnosprawnych. Na stronie BIP zostały umieszczone pliki graficzne (zdjęcia) bez zdefiniowanego parametru ALT który wykorzystują czytniki ekranów. Przykład www.lagowgmina.biuletyn.net zdjęcie skarbnika gminy Łagów. Zostały przetestowane zamieszczone na stronie BIP pliki w formacie PDF pod kątem zgodności z WCAG 2.0 (odczyt zawartości treści plików przez czytnik ekranu). Część dokumentów jak np. Wniosek o udostępnienie informacji publicznej spełnia wymagania WCAG 2.0. Na stronie znajdują się pliki w formacie PDF które nie spełniają wymagań WCAG 2.0 np. Statut Miasta i Gminy Łagów (plik **U_357.pdf)** który został zamieszczony na stronie w formacie pdf (skan) jego zawartość nie jest dostępna dla czytników ekranu. Plików takich jest więcej między innymi w podstronach: - Plany polowań kół łowieckich - Informacja o terminie i czasie odpalania ładunków wybuchowych w zakładach górniczych na terenie gminy - Wspólnoty gruntowe - Gospodarka odpadami W opublikowanych sesjach Rady Miejskiej w Łagowie brak napisów lub tłumaczenia migowego. Dowód – strony internetowe: https://www.youtube.com/channel/UC8O_TdulJFUSfaVYRA-su-w/featured http://www.lagowgmina.pl/asp/pliki/11_listopad_2015_r/wniosek_p._wojtasinska.pdf
Ustalone uchybienia, nieprawidłowości	Nie działa funkcjonalność zmiany kontrastu na stronie głównej i na stronie BIP. Pliki zamieszczone na stronach www.lagowgmina.pl i www.lagowgmina.biuletyn.net w formacie PDF są w formie skanów, które nie mogą być czytane przez czytniki ekranów. Na stronie BIP zostały umieszczone pliki graficzne (zdjęcia) bez zdefiniowanego parametru ALT, który wykorzystują czytniki ekranów. Pliki multimedialne np. Sesje Rady Miasta w Łagowie nie są dostosowane do potrzeb osób niesłyszących (brak napisów lub tłumaczeń migowych).
Ocena obszaru kontroli nr 3	**Pozytywna z nieprawidłowościami**
ZALECENIA	1. Rozliczać IODO z wykonania zadań opisanych w dokumentacji. 2. Podpisać z ZETO SOFTWARE umowę powierzenia przetwarzania danych osobowych znajdujących się w systemie PUMA. 3. Zaktualizować i przystosować do specyfiki pracy UMiG dokumentację dotyczącą Polityki Bezpieczeństwa Informacji (PBI) tak aby procedury, procesy i instrukcje w niej opisane były jednoznaczne, zgodne z wymogami KRI oraz chroniły nie tylko szczególne dane jakimi są dane osobowe ale wszelkie dane gromadzone, przetwarzane w UMiG w Łagowie. 4. Wdrożyć w życie zaktualizowaną, poprawioną dokumentację PBI (w tym również IZSI) i bezwzględnie jej przestrzegać. 5. Przeszkolić lub szkolić do skutku z zastosowania procedur, procesów instrukcji opisanych w PBI wszystkich pracowników UMiG w Łagowie zwłaszcza kierowników komórek organizacyjnych. Szkolenie przynajmniej raz w roku z całej wdrożonej PBI . 6. Przeprowadzać okresowo analizę ryzyka. 7. Przeprowadzić raz w roku audyt wewnętrzy z przestrzegania procedur, procesów,

	instrukcji z PBI. 8. Przeprowadzić inwentaryzację sprzętu i oprogramowania tak aby była zgodna z wytycznymi KRI oraz utrzymywać inwentaryzację tak aby jej stan odpowiadał rzeczywistości. 9. Opracować procedury i instrukcje związane z tworzeniem, przechowywaniem, testowaniem kopii zapasowych tak aby całość posiadała atrybuty autentyczności, rozliczalności, niezaprzeczalności. 10. Ustanowić, opisać i przestrzegać zapisów w PBI dotyczących połączeń zdalnych, wyznaczyć osobę odpowiedzialną za uruchomienie połączenia zdalnego zgodnie z opracowaną procedurą. 11. Dopracować procedury przechowywania haseł administracyjnych do systemów, urządzeń i wdrożyć. 12. Napisać od nowa instrukcję dotyczącą incydentów, jednoznacznie w niej określić osoby które należy powiadomić, telefony których należy używać w przypadku wystąpienia incydentu. Określić jednoznacznie osoby odpowiedzialne. 13. Zakupić aktualizację do urządzenia FortiGate, 14. W miarę możliwości po konsultacji z ASI zaktualizować lub wymienić system obsługujący serwer plików. 15. W miarę możliwości wymienić na nowe systemy operacyjne na stacjach roboczych z zainstalowanym systemem Windows 7. 16. Wyprowadzić z serwerowni wszystkie stare urządzenia które obecnie znajdują się poza szafami dystrybucyjnymi. 17. Sprawdzić zgodność z PBPDO konfiguracji stacji roboczych, w szczególności zwrócić uwagę na konfigurację systemu antywirusowego oraz konfiguracje wygaszaczy ekranu. Przeprowadzić testy UPSów do których podłączone są stacje robocze. 18. Wdrożyć Active Directory lub równoważną usługę katalogową. 19. Dokonać przeglądu stacji roboczych pod kątem zgodności z PBI. 20. Dostosować materiały publikowane z serii Rady Miasta na stronach internetowych Starostwa do potrzeb osób niesłyszących (napisy lub tłumaczenie migowe). 21. Zamienić pliki umieszczone na stronach www.lagowgmina.pl i www.lagowgmina.biuletyn,net w formacie PDF (skany) na pliki w formacie PDF lub innym które będą czytelne dla czytników ekranu. 22. Poprawić funkcjonalność zmiany kontrastu na stronie głównej i na stronie BIP.

Na podstawie art. 49 ustawy o kontroli w administracji rządowej, proszę o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości, 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.

z up. Wojewody Świętokrzyskiego
Anna Król
Dyrektor
Wydział Organizacji i Kadr