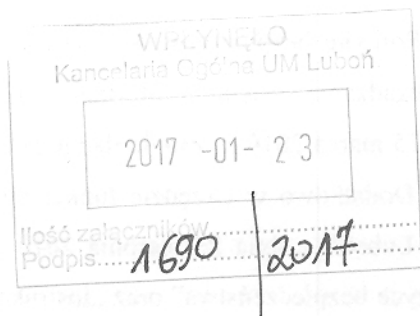




WOJEWODA WIELKOPOLSKI

OI-VII.1610.1.2016.5

Poznań, ..... 2017 01. 18



**Pani**

**Małgorzata Machalska**

**Burmistrz Miasta Luboń**

Plac Edmunda Bojanowskiego 2  
62-030 Luboń

### WYSTĄPIENIE POKONTROLNE

Na podstawie art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2011 r. Nr 185, poz. 1092) oraz art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114, z późn. zm.) w dniu 15 grudnia 2016 r. w Urzędzie Miasta Luboń (Plac Edmunda Bojanowskiego 2, 62-030 Luboń) została przeprowadzona kontrola systemów informatycznych i rejestrów publicznych, używanych do realizacji zadań zleconych z zakresu administracji rządowej, związanych z prowadzeniem ewidencji ludności i danych USC.

Czynności kontrolne przeprowadził, na podstawie upoważnienia Wojewody Wielkopolskiego Nr 587/16 z dnia 8 grudnia 2016 r., zespół kontrolny w składzie: Monika Piotrowska – starszy specjalista w Biurze Organizacyjno-Administracyjnym i Daniel Janik – starszy informatyk w Biurze Obsługi i Informatyki Wielkopolskiego Urzędu Wojewódzkiego w Poznaniu.

Jednostka kontrolowana została poinformowana o przedmiotowej kontroli pismem nr OI-VII.1610.1.2016.5 z dnia 9 grudnia 2016 r.

Zakres kontroli obejmował ocenę funkcjonowania jednostki kontrolowanej w aspekcie prawidłowości postępowania związanego z bezpieczeństwem informacji zawartych w rejestrach publicznych – ewidencji ludności i aktach stanu cywilnego.

**Wojewoda Wielkopolski pozytywnie ocenia działalność kontrolowanej jednostki w zakresie objętym kontrolą.**

Sformułowana ocena została oparta na podstawie poniższych ustaleń kontroli.

We wstępnej fazie prowadzonej kontroli zespół kontrolny poprosił o przedłożenie polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, do których posiadania zobowiązuje jednostki rozporządzenie Ministra Spraw

Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

Jednostka kontrolowana przedstawiła zespołowi kontrolnemu „Politykę bezpieczeństwa w Urzędzie Miasta Luboń” z dnia 1 października 2008 r. oraz „Instrukcję zarządzania systemem informatycznym Ochrony Danych Osobowych w Urzędzie Miasta Luboń” z dnia 15 marca 2010 r., zatwierdzone przez Pana Dariusza Szmyta, ówczesnego Burmistrza Miasta Luboń. Dodatkowo w Urzędzie funkcjonuje „Regulamin Ochrony Danych Osobowych w Urzędzie Miasta Luboń” z dnia 23 sierpnia 2010 r., stanowiący wyciąg najistotniejszych zapisów zawartych w „Polityce bezpieczeństwa” oraz „Instrukcji zarządzania”.

Administrator danych osobowych w kontrolowanej jednostce nie powołał administratora bezpieczeństwa informacji, a przypisane mu zadania są realizowane przez Sekretarza, Pana Janusza Piaseckiego oraz Administratora Systemów Informatycznych, Pana Marcina Wicińskiego. W toku kontroli otrzymano informację, iż w Urzędzie przygotowywane jest zarządzenie Burmistrza powołującego administratora bezpieczeństwa informacji.

Osoby mające dostęp do przetwarzania danych osobowych posiadają wymagane ustawowo upoważnienia. W pierwszej kolejności zespół kontrolny otrzymał do wglądu upoważnienie Ministra Spraw Wewnętrznych z dnia 28 listopada 2014 r. dla Pani Małgorzaty Machalskiej, Burmistrza Miasta Luboń do przetwarzania danych osobowych zgromadzonych w rejestrze PESEL, Rejestrze Dowodów Osobistych i Rejestrze Stanu Cywilnego, a także do udzielania dalszych imiennych upoważnień pracownikom. I tak, w tym zakresie sprawdzono upoważnienia dla:

- Pana Cezarego Bidermana, kierownika USC, z dnia 30 stycznia 2015 r. (l.dz. WAG.142.22.2015),
- Pani Jagody Wawrzyniak, zastępcy kierownika USC, z dnia 27 lutego 2015 r. (l.dz. WAG.142.23.2015),
- Pani Jolanty Pawłety, specjalisty WSO, z dnia 2 stycznia 2015 r. (l.dz. WAG.142.11.2015),
- Pani Kamili Wrzyszczyńskiej, specjalisty WSO, z dnia 2 stycznia 2015 r. (l.dz. WAG.142.12.2015),
- Pani Marty Marczyńskiej, podinspektora WSO, z dnia 2 stycznia 2015 r. (l.dz. WAG.142.14.2015).

W upoważnieniach zawarto zobowiązanie do zachowania tajemnicy przetwarzanych danych i sposobów ich zabezpieczania.

Ponadto wyrywkowo sprawdzono upoważnienia do przetwarzania danych w systemach ELUD i e-SOS (elektroniczny obieg spraw) dla:

- Pani Jagody Wawrzyniak, młodszego referenta ds. ewidencji ludności w WSO, z dnia 6 lipca 2012 r., nr 10/2012,

- Pani Jolanty Pawłęty, specjalisty ds. ewidencji ludności i dowodów osobistych w WSO, z dnia 6 kwietnia 1999 r.,
- Pani Kamili Waškowiak, młodszego referenta ds. ewidencji ludności i dowodów osobistych w WSO, z dnia 1 lutego 2008 r.

Niniejsze upoważnienia zostały podpisane przez Sekretarza Miasta z upoważnienia Burmistrza.

Kontrolujący otrzymali do wglądu listy obecności pracowników Urzędu, którzy wzięli udział w szkoleniu dotyczącym ochrony danych osobowych, które odbyło się w listopadzie 2015 r., a po szkoleniu pracownicy wypełnili testy z tematyki ochrony danych.

Zgodnie z otrzymanymi informacjami nowi pracownicy przechodzą indywidualne szkolenia, (korzystają z wewnętrznego portalu, otrzymują materiał drukowany oraz płytę CD), czego potwierdzeniem były wypełniane przez nich testy z zagadnień ochrony danych osobowych (marzec-kwiecień 2016 r.).

Ponadto w ramach podnoszenia świadomości, w Urzędzie funkcjonuje wewnętrzny portal, na którym w zakładce „Baza wiedzy” zamieszczane są materiały dla pracowników, newslettery. Z kolei drogą mailową przekazywane są informacje do wiadomości i stosowania przez pracowników, np. „Ile strat generują ataki hakerskie na świecie” z 17 października 2016 r., „Bezpieczeństwo systemów informatycznych” z 31 maja 2016 r., „Instrukcja dla pracowników na wypadek infekcji ransomware” z 10 października 2016 r.

W powyższym zakresie nie stwierdzono nieprawidłowości.

Następnie zespół kontrolny zapoznał się z metodami pracy w systemach informatycznych i rejestrach publicznych, związanych z prowadzeniem ewidencji ludności i danych USC pod kątem bezpieczeństwa informacji (tj. centralny System Rejestrów Państwowych „Źródło” oraz lokalny: ELUD, autorstwa firmy Radix) i skonfrontował je z wymogami zawartymi w przepisach prawa. Kontrola wykazała co następuje.

1. W zakresie organizacyjno-technicznym:

- a) pomieszczenia, gdzie odbywa się przetwarzanie danych osobowych są zabezpieczone przed dostępem osób nieupoważnionych, monitory ustawione prawidłowo (uniemożliwiają podgląd danych na ekranie przez osoby postronne);
- b) kontrola dostępu do pomieszczeń – pracownicy pobierają i zdają klucze w Punkcie Obsługi Klienta, funkcjonuje elektroniczna rejestracja czasu pracy;
- c) zespół kontrolny przeprowadził oględziny pomieszczenia serwerowni obsługującej kontrolowane rejestry publiczne:
  - serwerownia została zlokalizowana na I piętrze po pokoju biurowym, stąd wejście przez zwykłe drzwi drewniane, zabezpieczone zamkiem,

- klucze do serwerowni są w posiadaniu informatyka, a komplet zapasowy został zdeponowany w Punkcie Obsługi Klienta i jest do dyspozycji wyłącznie dla Sekretarza Miasta oraz pracownika zastępującego informatyka,
  - w pomieszczeniu pracuje klimatyzator, serwisowany corocznie przez firmę zewnętrzną,
  - zasilanie awaryjne realizowane w oparciu o lokalne zasilacze UPS zabezpieczające urządzenia aktywne i serwery,
  - wszystkie urządzenia zamontowane w szafie teleinformatycznej,
  - wydzielony blat na czynności serwisowe,
  - dodatkowa ochrona obiektu z wykorzystaniem monitoringu wizyjnego na zewnątrz, wewnątrz budynku dwie kamery,
  - wydzielone sieci rządowe (m.in. dostęp do Źródła) odseparowane od lokalnych sieci urzędowych LAN,
  - zastosowano dodatkową separację sieci WiFi i wewnętrznej sieci LAN,
  - zastosowano ochronę brzegową sieci w oparciu o rozwiązanie UTM Fortigate,
  - w celu podniesienia bezpieczeństwa zastosowano konfigurację macierzy RAID na serwerach oraz dyskach sieciowych,
  - wdrożono usługi katalogowe Active Directory, w oparciu o darmowe rozwiązania SAMBA 4,
  - zmieniono technologię dostępu do sieci Internet na łącze światłowodowe u nowego operatora;
- d) utrzymywana i aktualizowana jest inwentaryzacja sprzętu komputerowego oraz oprogramowania, z czego inwentaryzacja oprogramowania przeprowadzana jest przez informatyka on-line za pomocą narzędzia Uplook przy każdej większej zmianie zasobów (ostatnia wg stanu na 15 listopada 2016 r.);
- e) w jednostce kontrolowanej zarządzeniem Nr 83/2014 Burmistrza Miasta Luboń z 31 grudnia 2014 r. został ustanowiony i wdrożony System Zarządzania Bezpieczeństwem Informacji, zgodnie z normą ISO/IEC 27001 (zarządzenie zatwierdzone przez Burmistrza, Panią Małgorzatę Machalską). Zgodnie z uzyskaną informacją, Urząd nie poddał się jeszcze certyfikacji przez jednostkę zewnętrzną, jednakże opracowana dokumentacja oraz wdrożone rozwiązania systemowe świadczą o rzetelności w stopniowym wdrażaniu SZBI;
- f) przeprowadzane są okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji – Raport z analizy ryzyka utraty bezpieczeństwa informacji z 31 października 2016 r., l.dz. RPO-23321/2016, WAG.0135.4.2016 (w tym: pkt 3 – wyniki analizy ryzyka z utraty bezpieczeństwa informacji systemów i rejestrów służących do

prowadzenia ewidencji oraz danych USC). W konsekwencji ww. powstał Raport okresowy, wskazujący na postępy prac nad podniesieniem poziomu bezpieczeństwa stacji roboczych, stan na 31 października 2016 r., l.dz. RPO-23322/2016, WAG.0135.05.2016.

W powyższym zakresie nie stwierdzono nieprawidłowości.

2. W zakresie bezpieczeństwa systemów informatycznych:

- a) przydzielanie, zmiana uprawnień do pracy w systemach przetwarzających dane osobowe odbywa się na wniosek kierownika przekazany do Sekretarza Miasta; wzór wniosku do pobrania na portalu wewnętrznym;
- b) w systemie informatycznym służącym do przetwarzania danych ewidencji ludności stosowana jest dwustopniowa kontrola dostępu: karta kryptograficzna oraz hasła dla każdego użytkownika (certyfikat na karcie kryptograficznej wgrywany przez MSWiA);
- c) komputery pracujące w ww. systemach posiadają zabezpieczenie antywirusowe w postaci oprogramowania Eset Endpoint Antivirus (zarządzane centralnie, sygnatury odnawiane corocznie); wyrywkowo sprawdzono stan aktualizacji bazy wirusów;
- d) użytkownicy pracują na kontach bez praw administratorskich; wdrożono system domenowy, który zapewnia zmianę hasła co 30 dni oraz złożoność hasła: 12 znaków, cyfry i znaki specjalne;
- e) przed utratą danych, bazy danych zabezpieczone zostały poprzez automatyczne wykonywanie kopii zapasowych za pomocą systemu backupowego WD Arkeia; praktykuje się również zabezpieczanie danych użytkowników, którzy aby zapewnić sobie kopie dokumentów przechowują je w określonych zasobach zamapowanych na stacjach roboczych;
- f) naprawy realizowane są głównie we własnym zakresie Urzędu; w przypadku napraw gwarancyjnych lub napraw przez firmy zewnętrzne, sprzęt jest pozbawiany dysków; ewentualny serwis sprzętowy lub aplikacyjny odbywa się na miejscu;
- g) dane dotyczące dowodów osobistych przenoszone są z systemu Źródło do ELUD przy użyciu szyfrowanego pendriv'a, z kontrolą dostępu. W Urzędzie zapewniono 22 szt. służbowych szyfrowanych sprzętowo pendriv'ów oraz 10 szt. pendriv'ów nieszyfrowanych, które udostępnia się na wniosek wypełniony przez użytkownika.

W powyższym zakresie nie stwierdzono nieprawidłowości.

Ze względu na brak zastrzeżeń do projektu wystąpienia pokontrolnego z dnia 21 grudnia 2016 r., przekazanego za pismem OI-VII.1610.1.2016.5 z 21 grudnia 2016 r., niniejsze wystąpienie pokontrolne obejmuje treść ww. projektu. Mając na uwadze, iż w trakcie czynności kontrolnych nie stwierdzono nieprawidłowości ani uchybień, wystąpienia pokontrolnego nie uzupełnia się o zalecenia pokontrolne. Jednakże poddają pod rozważenie doposażenie pomieszczenia pełniącego rolę serwerowni

w dodatkowe elementy: specjalistyczne drzwi, czujki ppoż., monitoring warunków środowiskowych pomieszczenia z elementami powiadamiania wyznaczonych osób.



Wojewoda Wielkopolski  
*Zbigniew Hoffmann*