ZARZĄDZENIE NR 81/2013
Starosty Łódzkiego Wschodniego
z dnia 23 października 2013 r.

w sprawie wykonania zaleceń pokontrolnych
w Starostwie Powiatowym w Łodzi

W związku z kontrolą zadań realizowanych przez Administratora Bezpieczeństwa Informacji oraz zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji w Starostwie Powiatowym w Łodzi realizowanej na podstawie zarządzenia nr 22/2013 Starosty Łódzkiego Wschodniego z dnia 6 marca 2013 r. w sprawie ustalenia planu kontroli instytucjonalnej w Starostwie Powiatowym w Łodzi na rok 2013 oraz zarządzenia nr 35/2013 Starosty Łódzkiego Wschodniego z dnia 17 kwietnia 2013 r. w sprawie kontroli planowanej zadań realizowanych przez Administratora Bezpieczeństwa Informacji oraz zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji w Starostwie Powiatowym w Łodzi zarządzam, co następuje:.

§ 1.1 Należy opracować harmonogram związany z dostosowaniem polityki bezpieczeństwa do postanowień prawnych zawartych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.), rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji i 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) oraz jej wdrożenia.

2. Należy przeprowadzić analizę zagrożeń dla bezpieczeństwa informacji, a w szczególności danych osobowych.

3. W celu zapewnienia adekwatnej, skutecznej, efektywnej kontroli zarządczej należy m.in.:

1) rozpocząć prace mające na celu zmianę unormowań zawartych w polityce bezpieczeństwa, instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych poprzez m.in.:
   a) aktualizację zbiorów zawierających dane osobowe,
   b) aktualizację ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych,
   c) aktualizację ewidencji oprogramowania przetwarzającego dane osobowe,
   d) aktualizację ewidencji pomieszczeń, w których przetwarza się dane osobowe,
   e) przygotowanie projektu zarządzenia Starosty w sprawie ustalenia Polityki bezpieczeństwa i Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,
2) wyodrębnić z projektu zarządzenia w sprawie ustalenia Polityki bezpieczeństwa i Instrukcji zarządzania ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, ewidencji

oprogramowania przetwarzającego dane osobowe, ewidencji pomieszczeń, w których przetwarza się dane osobowe. Ujęcie wskazań w zakresie zobligowania do ich bieżącego prowadzenia Administratora Bezpieczeństwa Informacji,

3) uwzględnić w polityce bezpieczeństwa, w tym instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych:
   a) używane przez pracowników loginy, służące do uwierzytelniania się w poszczególnych systemach operacyjnych (aplikacjach internetowych), a w szczególności służących do przetwarzania danych osobowych,
   b) wskazania dotyczące realizacji zadań związanych z funkcjonowaniem archiwum zakładowego, a dotyczących ochrony danych osobowych, bezpieczeństwa informacji,
   c) wskazania dotyczące realizacji zadań realizowanych przez pracowników zatrudnionych na pozamiejscowych stanowiskach pracy w obszarze ochrony danych osobowych, bezpieczeństwa informacji,
   d) wskazania dotyczące korzystania z mobilnych urządzeń (służbowych telefonów komórkowych, służbowych i prywatnych komputerów przenośnych, na których przetwarza się dane osobowe, nośników pamięci np.: pendrive),
   e) wskazania dotyczące realizacji projektu pn. „Budowa Zintegrowanego Systemu e-Usług Publicznych Województwa Łódzkiego (Wrota Regionu Łódzkiego)" i zawartą umowę partnerską,
4) przygotować projekt zmiany unormowań zawartych w zarządzeniu nr 23/2009 Starosty Łódzkiego Wschodniego z dnia 26 lutego 2009 r. w sprawie wyznaczenia administratora bezpieczeństwa informacji w Starostwie Powiatowym w Łodzi oraz określenia jego obowiązków i uprawnień, poprzez wyznaczenie kierownikom komórek organizacyjnych, samodzielnym stanowiskom pracy obowiązku współpracy z Administratorem Bezpieczeństwa Informacji w zakresie określonym w protokole z kontroli (m.in. wskazanie częstotliwości, formy udokumentowania ustaleń związanych z realizacją zadań prowadzenia okresowych kontroli w zakresie stosowanych zabezpieczeń systemu informatycznego, szkoleń osób upoważnionych do przetwarzania danych osobowych, dokonywania okresowej analizy zagrożeń dla bezpieczeństwa danych osobowych),
5) prawidłowo powierzyć obowiązki pracownikom (pisemne potwierdzenie przyjęcia obowiązków) w zakresie realizacji polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,
6) przeprowadzić szkolenia dla pracowników Starostwa w zakresie realizacji polityki bezpieczeństwa, w tym instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,
7) wprowadzić zasady posługiwania się podpisem elektronicznym, które obejmowałyby m.in. obowiązek prowadzenia ewidencji oraz wydawania upoważnień,
8) zapewnić prowadzenie w Wydziale Organizacyjnym ewidencji pozwalającej na wyodrębnienie informacji o rodzaju zakupionego, używanego oprogramowania, a w szczególności w zakresie posiadanych licencji (m.in. legalności posługiwania się nim),

9) opracować zasady korzystania ze służbowej poczty elektronicznej pracowników (mając na względzie postanowienia instrukcji kancelaryjnej). Niezbędne jest opracowanie narzędzi gwarantujących brak dostępu do korzystania z poczty służbowej osób, których zatrudnienie w Starostwie ustało. Podobne rozwiązania należy zastosować w przypadku aplikacji internetowych,
10) ograniczyć możliwość logowania się do systemów operacyjnych przez osoby nieupoważnione (np. poprzez udostępnianie haseł innym pracownikom, stażystom),
11) uwzględnić przy opracowywaniu zakresów obowiązków, uprawnień i odpowiedzialności pracowników oraz upoważnień do przetwarzania danych osobowych, zakresów zastępstw w przypadku nieobecności pracowników,
12) należy dokonać przeglądu stosowanych zabezpieczeń w zakresie dokumentów pozostawionych w punkcie ksero oraz szafach zlokalizowanych na korytarzach Starostwa, a także pozostawionych przez pracowników po zakończeniu pracy w pomieszczeniach służbowych,
13) monitorować sprawność urządzeń do klimatyzacji w serwerowni oraz urządzeń UPS,
14) przekazać informację kierownikom komórek organizacyjnych, iż zakresy obowiązków, uprawnień i odpowiedzialności pracowników powinny gwarantować bezpieczeństwo informacji, m.in. poprzez zawarcie w nich:
    a) zakresu delegowanych uprawnień, m.in. powiązanych z: polityką bezpieczeństwa i instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych np.: wszelkich uprawnień do logowania się w aplikacjach komputerowych lokalnych i internetowych (ze wskazaniem loginu); dostępem do służbowej poczty elektronicznej; posługiwaniem się elektronicznym podpisem. Lista uprawnień powinna zawierać informacje do jakiej aplikacji, czy też poczty elektronicznej pracownik ma dostęp oraz identyfikator, login poprzez, który pracownik dokonuje uwierzytelnienia,
    b) zakresu odpowiedzialności m.in. dotyczących: odpowiedzialności materialnej za powierzone mienie; zachowania tajemnicy (państwowej, służbowej, zawodowej, skarbowej), której ujawnienie mogłoby narazić pracodawcę na szkodę; ochrony danych osobowych,
    c) wszystkich okoliczności, które pozwolą rozliczyć się pracownikom z zakładem pracy w przypadku ustania zatrudnienia,
    d) zakresu zastępstw w przypadku nieobecności pracowników,
    e) obowiązku bieżącego archiwizowania dokumentów,
    f) obowiązku zapoznawania się z wydawanymi aktami prawnymi dotyczącymi realizowanych obowiązków (m.in. bieżące zapoznawanie się z zarządzeniami wydawanymi przez Starostę Łódzkiego Wschodniego),
    ł) obowiązku bieżącego zapoznawania się z informacjami zawartymi w Intranecie oraz na tablicach ogłoszeń w Starostwie,
    g) w ramach zarządzania ryzykiem obowiązku informowania bezpośrednich przełożonych o występowaniu wszelkich zidentyfikowanych ryzyk, prawdopodobieństwa jego

wystąpienia i ewentualnych skutkach, proponowania mechanizmów kontrolnych mających sprowadzić ryzyko do akceptowalnego poziomu.

15) należy respektować postanowienia zawarte w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych przy wymianie informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526).

4. Powyższe czynności należy przeprowadzić przy współudziale kierowników komórek organizacyjnych, pracowników zatrudnionych na samodzielnych stanowiskach pracy w Starostwie Powiatowym w Łodzi.

5. Harmonogram uwzględniający przynajmniej zakres określony w ust. 3 należy opracować w terminie do dnia 30 listopada 2013 r. oraz przekazać Sekretarzowi Powiatu.

§ 2. Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 3. Zobowiązuję kierowników komórek organizacyjnych oraz pracowników zatrudnionych na samodzielnych stanowiskach pracy w Starostwie Powiatowym w Łodzi do ścisłej współpracy z Administratorem Bezpieczeństwa Informacji na rzecz wykonania zaleceń pokontrolnych określonych w zarządzeniu.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
mgr inż. Piotr Busiakiewicz