Zarządzenie Nr 17/2010
Burmistrza Miasta Mławy
z dnia 17 lutego 2010 roku

w sprawie polityki bezpieczeństwa dla systemu monitorowania Europejskiego Funduszu Społecznego 2007 w Urzędzie Miasta w Mławie

Postanowienia ogólne

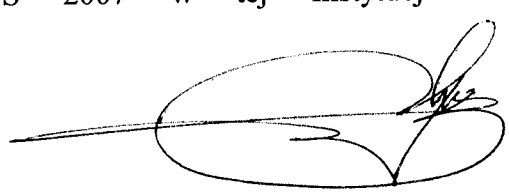
§ 1.

Polityka Bezpieczeństwa dla systemu Podsystemu Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL, zwana dalej „Polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w systemie Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007, zwanym dalej „PEFS 2007" w Urzędzie Miasta w Mławie.

§ 2

Użyte w Polityce określenia oznaczają:

1. **Administrator Danych** Ministra Rozwoju Regionalnego
2. **ustawa** Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);
3. **rozporządzenie** 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. Nr 100, poz. 1024);
4. **użytkownik** Osobę upoważnioną do tego przez Administratora Danych do przetwarzania danych osobowych w PEFS 2007;
5. **Administrator Bezpieczeństwa Informacji** Osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007
6. **Administrator Bezpieczeństwa Informacji w IP/IP2** Osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu właściwej Instytucji Pośredniczącej /Instytucji Pośredniczącej II Stopnia PO KL, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 w tej Instytucji



Pośredniczącej / Instytucji Pośredniczącej II Stopnia PO KL;

7. **Administrator Bezpieczeństwa Informacji u Beneficjenta** Osobę wyznaczona przez Burmistrza Miasta Mławy, odpowiedzialna za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta;
8. **naruszenie zabezpieczenia systemu informatycznego** Jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności PEFS 2007;
9. **dane osobowe** Wszelkie informacje dotyczące zidentyfikowania lub możliwej do zidentyfikowania osoby fizycznej
10. **przetwarzanie danych osobowych** Jakiekolwiek operacje wykonywane na danych osobowych polegające na zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, udostępnianiu lub usuwaniu danych osobowych, a zwłaszcza te, które wykonuje się w PEFS 2007;
11. **usuwanie danych osobowych** Zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
12. **zbiór danych osobowych** Posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
13. **zabezpieczenie danych osobowych** Środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą;
14. **Instrukcja** Instrukcję Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 w IP/IP2;
15. **Pracownik** Osobę zatrudnioną na podstawie stosunku pracy lub innego stosunku prawnego;
16. **Beneficjent** Urząd Miasta w Mławie
17. **Ministerstwo** Ministerstwo Rozwoju Regionalnego.

Zakres oraz zasady zabezpieczenia danych osobowych

§ 3.

Zasady zabezpieczania danych osobowych opisane w Polityce oraz instrukcji dotyczą danych osobowych osób fizycznych.

§ 4.

Zasady, o których mowa w § 3, stosuje się w stosunku do zbioru danych osobowych znajdujących się w PEFS 2007.

§ 5.

1) Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełni Administrator Danych.
2) Kontrolę nad poprawnością realizacji przepisów o ochronie danych osobowych w szczególności zasad opisanych w Polityce oraz Instrukcji, oraz wykonywaniem zadań związanych z ochroną danych osobowych PEFS 2007 w Urzędzie Miasta w Mławie , sprawuje Administrator Bezpieczeństwa Informacji.

§ 6.

Dane osobowe przetwarzane w PEFS 2007 są objęte tajemnicą.

§ 7.

Przetwarzanie danych osobowych w PEFS 2007 jest dopuszczalne wyłącznie w zakresie niezbędnym do udzielenia wsparcia, realizacji projektów, ewaluacji, monitoringu, sprawozdawczości i kontroli, w ramach Programu Operacyjnego Kapitał Ludzki.

§ 8.

Przetwarzanie danych osobowych w PEFS 2007 nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sadowym lub administracyjnym.

§ 9.

W przypadku zbierania jakichkolwiek danych osobowych na potrzeby PEFS 2007 bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana do przekazania tej osobie informacji o:

1) pełnej nazwie Ministerstwa oraz jego adresie;

2) celu zbierania danych osobowych;
3) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
4) dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożliwością wzięcia udziału w projekcie realizowanym w ramach Programu Operacyjnego Kapitał Ludzki.

§ 10.

1) Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w ustawie oraz w pełnej zgodności z przepisami prawa.
2) Wnioski o udostępnienie danych osobowych przetwarzanych w PEFS 2007, po wstępnym rozpatrzeniu przez Administratora Bezpieczeństwa Informacji, są rozpatrywane przez Administratora Danych.

§ 11.

1) Przetwarzanie danych osobowych znajdujących się w PEFS 2007 może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 7, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy ustawy, rozporządzenia oraz umowy o dofinansowanie projektu.
2) Umowy lub porozumienia o powierzeniu przetwarzania danych osobowych w PEFS 2007 powinny zostać przed podpisaniem, w zakresie dotyczącym zasad przetwarzania danych osobowych, zaopiniowane przez Administratora Bezpieczeństwa w Informacji u Beneficjenta.

§ 12.

Każdej osobie, której dane osobowe są przetwarzane w PEFS 2007 przysługuje prawo do kontroli przetwarzania jej danych osobowych zawartych w zbiorach danych osobowych, a w szczególności prawo do:

1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
5) uzyskania informacji o sposobie udostępniania danych osobowych, z w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§ 13.

Na wniosek osoby, której dane osobowe dotyczą, Beneficjent jest zobowiązany, w terminie 30 dni od dnia wpłynięcia wniosku do Beneficjenta, wskazać na piśmie, w formie powszechnie zrozumiałej:

1) jakie dane osobowe dotyczące zapytującej osoby są przetwarzane przez Beneficjenta w PEFS 2007;
2) w jaki sposób zebrano te dane osobowe;
3) w jakim celu i zakresie te dane osobowe są przetwarzane;
4) od kiedy są przetwarzane te dane osobowe;
5) w jakim zakresie oraz komu te dane osobowe zostały udostępnione.

§ 14.

W razie wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe przetwarzane przez Beneficjenta w PEFS 2007 są niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, w jakim zostały zebrane, Beneficjent jest zobowiązany do uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych osobowych lub ich usunięcia zgodnie z żądaniem osoby, której dane osobowe dotyczą.

Obowiązki Administratora Bezpieczeństwa Informacji IP/IP2

§ 15.

Administrator Bezpieczeństwa Informacji u Beneficjenta poza realizacją zadań wynikających z polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych w PEFS 2007 u Beneficjenta.

§ 16.

Do zadań Administratora Bezpieczeństwa Informacji u Beneficjenta należy w szczególności:

1) współdziałanie z Administratorem Bezpieczeństwa Informacji w IP/IP2 w zakresie zapewniającym wypełnianie przez Beneficjenta obowiązków wynikających z ustawy i rozporządzenia;
2) prowadzenie i aktualizacja rejestru, o którym mowa w § 21, którego wzór jest określony w załączniku nr 1 do Polityki;
3) prowadzenie i aktualizacja wykazu budynków, pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w PEFS 2007 u Beneficjenta, którego wzór jest określony w załączniku nr 2 do Polityki;
4) analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych w ramach PEFS 2007 u Beneficjenta;
5) opiniowanie umów i porozumień, których przedmiotem jest powierzanie przetwarzania danych osobowych zawartych w PEFS 2007 podmiotowi zewnętrznemu wobec Beneficjenta;
6) inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych w PEFS 2007 u Beneficjenta;

7) zapoznawanie każdego pracownika mającego dostęp do danych osobowych w PEFS 2007, z obowiązującymi u Beneficjenta zasadami ochrony danych osobowych;

§ 17.

W doborze i stosowaniu środków ochrony danych osobowych w PEFS 2007 Administrator Bezpieczeństwa Informacji u Beneficjenta zwraca szczególna uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub modyfikacją.

§ 18.

1. Obowiązki Administratora Bezpieczeństwa Informacji u Beneficjenta wykonywane są przez wyznaczonego przez Burmistrza Miasta Mława Pracownika.
2. Nadzór nad wykonaniem obowiązków Administratora Bezpieczeństwa Informacji u Beneficjenta pełni Burmistrz Miasta Mławy

§ 19.

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych w PEFS 2007, Administrator Bezpieczeństwa Informacji u Beneficjenta konsultuje się i współpracuje z Administratorem Bezpieczeństwa Informacji w IP/IP2.

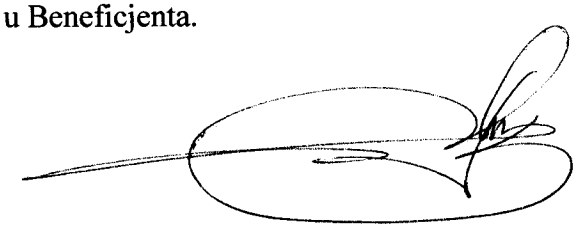
Przetwarzanie danych osobowych

§ 20.

1) Do przetwarzania danych osobowych w PEFS 2007 mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienia wydane przez Administratora Danych lub osobę przez niego upoważnioną. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określane są w załącznikach do porozumienia w sprawie powierzenia przetwarzania danych osobowych.
2) Każdy pracownik przed dopuszczeniem go do przetwarzania danych osobowych w PEFS 2007, musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją.
3) Pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją przez złożenie podpisu na liście prowadzonej przez Administratora Bezpieczeństwa Informacji u Beneficjent, której wzór jest określony w załączniku nr 3 do Polityki.

§ 21.

1. Każdy pracownik mający dostęp do danych osobowych w PEFS 2007 jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Administratora Bezpieczeństwa Informacji u Beneficjenta.
2. Rejestr, o którym mowa w ust. 1, zawiera:



1) imię i nazwisko pracownika;
2) jego identyfikator w PEFS 2007;
3) zakres przydzielonego uprawnienia;
4) datę przyznania uprawnień;
5) datę odebrania uprawnień.

§ 22.

1) Dopuszczenie do przetwarzania danych osobowych znajdujących się w PEFS 2007 przez osoby niebędące pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii Administratora Bezpieczeństwa Informacji u Beneficjenta oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych. W takim przypadku § 20 i 21 stosuje się odpowiednio.
2) Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

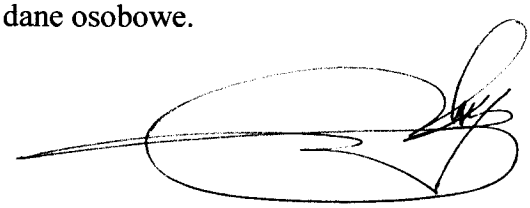
§ 23.

Wszyscy pracownicy oraz osoby, o których mowa § 22 ust.1, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych w PEFS 2007 danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

§ 24.

Użytkownicy są szczególności zobowiązani do:

1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w PEFS 2007, określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania PEFS 2007 oraz jego obsługi;
2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
3) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcji i innych procedurach dotyczących zarządzania PEFS 2007 oraz jego obsługi;
4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
5) nieudzielania informacji o danych osobowych przetwarzanych w PEFS 2007 innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
6) bezwzględnego zawiadamiania w formie pisemnej Administratora Bezpieczeństwa Informacji u Beneficjenta o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych w PEFS 2007, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.



§ 25.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych są określone w załączniku nr 4 do Polityki.

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 26.

Za naruszenie danych osobowych uznaje się przypadki, gdy:

1) stwierdzono naruszenie zabezpieczenia PEFS 2007;
2) stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu mogą wskazywać na naruszenie zabezpieczeń tych danych;
3) inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych w PEFS 2007.

§ 27.

1) Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych w PEFS 2007, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji u Beneficjenta.
2) Administrator Bezpieczeństwa Informacji u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:
    1. poinformować o zaistniałym zdarzeniu Administratora Bezpieczeństwa Informacji w IP/IP2 i stosować się do jego zaleceń;
    2. zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu;
    3. wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je data i podpisać;
    4. przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby niepowołanej do danych osobowych;
    5. podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody zabezpieczyć przed usunięciem ślady naruszania ochrony danych osobowych, w szczególności przez:
        a. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej,

b. wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
c. zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu;

6. szczegółowo analizować stan PEFS 2007 w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;
7. przywrócić normalne działania PEFS 2007 z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, ta samą drogą.

§ 28.

1) Po przywróceniu normalnego stanu zbioru danych osobowych w PEFS 2007 należy przeprowadzać szczegółową analizę, w celu określenia naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
2) Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych w PEFS 2007.
3) Jeżeli przyczyną zdarzenia była infekcja wirusem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
4) Jeżeli przyczyna zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań Beneficjenta, a w przypadku gdy użytkownik nie jest pracownikiem, konsekwencje wynikające z umowy, o której mowa w § 22 ust. 1.

§ 29.

Administrator Bezpieczeństwa Informacji u Beneficjenta przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia PEFS 2007 i w terminie 14 dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia PEFS 2007 przekazuje go Administratorowi Bezpieczeństwa Informacji w IP/IP2.

Kontrola nad przestrzeganiem ochrony danych osobowych

§ 30.

1) Bieżąca kontrola nad przetwarzaniem danych osobowych w PEFS 2007 u Beneficjenta jest dokonywana przez Burmistrza Miasta Mławy.
2) W ramach kontroli, o której mowa w ust. 1, Burmistrz Miasta Mławy nadzoruje z Administratorem Bezpieczeństwa Informacji u beneficjenta, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§ 31.

1) Administrator Bezpieczeństwa Informacji u Beneficjenta przeprowadza raz w roku kalendarzowym kontrolę w zakresie przestrzegania przez użytkowników Polityki, Instrukcji oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport, który przekazuje do 31 stycznia każdego roku Administratorowi Bezpieczeństwa Informacji w IP/IP2.
2) Przygotowując raport, o którym mowa w ust. 1, Administrator Bezpieczeństwa Informacji u Beneficjenta uwzględnia informacje zawarte w raportach, o których mowa w § 29.

§ 32.

Kontrola, o której mowa w § 31, polega w szczególności na sprawdzeniu:

1) którzy pracownicy maja dostęp do danych osobowych;
2) czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom lub osobom;
3) czy pracownicy i inne osoby mające dostęp do danych osobowych przetwarzanych w PEFS 2007 posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez osobę upoważnioną do tego przez Administratora Danych.

Postanowienia końcowe

§ 33.

Polityka jest dokumentem wewnętrznym Beneficjenta i jest objęta obowiązkiem zachowania w tajemnicy przez wszystkie osoby, którym zostanie ujawniona.

§ 34.

Do spraw nieuregulowanych w Polityce stosuje się przepisy o ochronie danych osobowych.

§ 35.

Polityka nie wyłączna stosowania innych instrukcji dotyczących zabezpieczenia PEFS 2007.

§ 36.

Wykazy i rejestry, których wzory są określone w załącznikach do Polityki, prowadzi Administrator Bezpieczeństwa Informacji u Beneficjenta.

§ 37.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ MIASTA
mgr Sławomir Kowalewski