

**Uchwała Zarządu
Stowarzyszenia Rozwoju Wsi Świętokrzyskiej
Nr 20/2011
z dn. 7 lipca 2011 r.
w sprawie przyjęcia Systemu Realizacji Projektu
„Wsparcie sieci lokalnych grup działania województwa świętokrzyskiego”**

Na podstawie § 23 ust. 2 lit. j Statutu Stowarzyszenia Rozwoju Wsi Świętokrzyskiej uchwała się co następuje:

§ 1.

Przyjmuje się do stosowania System Realizacji Projektu „Wsparcie sieci lokalnych grup działania województwa świętokrzyskiego” składający się z:

- a) Regulaminu Projektu, który stanowi Załącznik nr 1 do niniejszej uchwały,
- b) Zasad współpracy i komunikacji w trakcie realizacji projektu „Wsparcie sieci lokalnych grup działania województwa świętokrzyskiego”, stanowiący Załącznik nr 2 do niniejszej uchwały,
- c) Polityki bezpieczeństwa dla zbioru *Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007* u Beneficjenta PO KL, która stanowi Załącznik nr 3 do niniejszej uchwały.

§ 2

Wykonanie uchwały powierza się Dyrektorowi Biura Stowarzyszenia Rozwoju Wsi Świętokrzyskiej.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Regulamin Projektu „Wsparcie sieci lokalnych grup działania województwa świętokrzyskiego”

§ 1.

Postanowienia ogólne

1. Niniejszy regulamin określa główne warunki przystąpienia i zasady udziału w projekcie pn. „Wsparcie sieci lokalnych grup działania województwa świętokrzyskiego”, realizowanym w ramach Programu Operacyjnego Kapitał Ludzki 2007-2013, Priorytet V „Dobre rządzenie”, Działanie 5.4 „Rozwój potencjału trzeciego sektora”, Poddziałanie 5.4.2 „Rozwój dialogu obywatelskiego”.
2. Realizatorem projektu jest Stowarzyszenie Rozwoju Wsi Świętokrzyskiej, z siedzibą w Łagowie, ul. Słupska 3.
3. Projekt współfinansowany jest przez Unię Europejską (UE) ze środków Europejskiego Funduszu Społecznego (EFS) na podstawie umowy nr UDA-POKL.05.04.02-00-826/10-00 o dofinansowanie realizacji projektu podpisanej z Ministerstwem Pracy i Polityki Społecznej.
4. Czas realizacji projektu: 01 maja 2011 r. – 30 kwietnia 2014 r.
5. Ogólny nadzór oraz rozstrzyganie spraw nieuregulowanych niniejszym regulaminem należy do kompetencji dyrektora Stowarzyszenia Rozwoju Wsi Świętokrzyskiej.

§ 2.

Przedmiot projektu

1. Przedmiotem projektu jest wzmocnienie porozumienia i potencjału Lokalnych Grup Działania (LGD) Województwa Świętokrzyskiego.
2. Wsparcie oferowane w ramach projektu dotyczy:
 - a. utworzenia sekretariatu porozumienia, którego zadaniem będzie zdobywanie oraz przekazywanie wiedzy i informacji istotnych w zakresie działalności LGD;
 - b. opracowania i wdrożenia Elektronicznego Systemu Informacji i Oceny (e-LGD) w celu przyspieszenia obiegu dokumentów w LGD oraz usprawnienia procesu oceny wniosków składanych do LGD;
 - c. organizacji spotkań sieciujących w celu integracji środowiska LGD oraz wypracowania rozwiązań ułatwiających przepływ informacji i podejmowania wspólnych działań;
 - d. organizacji 3 edycji szkoleń Ekspert Zarządzania Strategicznego oraz 3 edycji szkoleń Ekspert Marketingu Regionalnego, służących wzmocnieniu zasobów ludzkich LGD w zakresie metod oraz technik marketingu, promocji, opracowania strategii, dialogu obywatelskiego i współpracy z administracją publiczną.

§ 3.

Grupa docelowa projektu

1. Projekt skierowany jest do 18 Lokalnych Grup Działania Województwa Świętokrzyskiego.
2. Dla 12 Lokalnych Grup Działania objętych *Porozumieniem o współpracy Lokalnych Grup Działania Województwa Świętokrzyskiego* opracowany zostanie i wdrożony Elektroniczny System Informacji i Oceny e-LGD.
3. Grupę docelową szkoleń oraz spotkań sieciujących stanowią osoby fizyczne będące pracownikami lub członkami Lokalnych Grup Działania Województwa Świętokrzyskiego.

§ 4.

Procedury rekrutacji

1. Rekrutację prowadzi się w Biurze Projektu.
2. Rekrutację prowadzi Komisja Rekrutacyjna w składzie: dyrektor biura Stowarzyszenia Rozwoju Wsi Świętokrzyskiej, koordynator projektu, asystent koordynatora projektu.
3. Informacje o rekrutacji zamieszczone są na tablicy ogłoszeń w siedzibie Biura Projektu, na stronie internetowej www.lgd-srws.pl oraz na stronie internetowej projektu.
4. Procedura rekrutacji obejmuje następujące etapy:
 - a. wypełnienie i złożenie formularza zgłoszeniowego;
 - b. weryfikacja kryteriów formalnych, ocena kwalifikowalności;
 - c. zawarcie „Porozumienia Na Rzecz Współpracy” oraz złożenie i podpisanie „Deklaracji uczestnictwa w projekcie”;
5. Zasady przyjmowania zgłoszeń:
 - a. formularze zgłoszeniowe dostępne będą na stronie internetowej projektu, w siedzibie Biura Projektu oraz w siedzibach biur poszczególnych LGD;
 - b. formularz należy wypełnić czytelnie, drukowanymi literami, podpisać oraz osobiście dostarczyć do Biura Projektu wraz z kompletem wymaganych dokumentów przed zakończeniem procesu rekrutacji.
6. Rekrutacja będzie prowadzona w terminie od 1 do 30 czerwca 2011.
7. Oddzielnym kryterium rekrutacyjnym podlegać będą organizacje LGD dla których opracowany zostanie i wdrożony Elektroniczny System Informacji i Oceny e-LGD, oddzielnym zaś osoby fizyczne zakwalifikowane do udziału w szkoleniach.
8. Zasady kwalifikacji do udziału w projekcie:
 - a. kwalifikację do udziału w projekcie prowadzi Komisja Rekrutacyjna;
 - b. Komisja Rekrutacyjna dokonuje oceny kwalifikowalności na bieżąco, w trakcie okresu przyjmowania formularzy zgłoszeniowych ;
 - c. kwalifikacja organizacji LGD nastąpi na podstawie:
 - analizy informacji zawartych w formularzu zgłoszeniowym – o zakwalifikowaniu będzie decydować najwyższa liczba punktów uzyskanych w ramach dwóch kryteriów:
 - 1) liczba gmin wchodzących w skład LGD (1 gmina-1 punkt),
 - 2) liczba kobiet pracujących w LGD (1 kobieta-2 punkty)

W przypadku jednakowej liczby punktów o zakwalifikowaniu do udziału w projekcie zadecyduje wyższa ocena uzyskana w kryterium zatrudnionych kobiet;

 - kolejności zgłoszenia;
 - d. kwalifikacja osób fizycznych będących pracownikami bądź członkami Lokalnych Grup Działania Województwa Świętokrzyskiego, rekrutowanych na szkolenia nastąpi na podstawie następującej punktacji:
 - pracownik lub członek Zarządu LGD – 2 pkt.,
 - kobieta – 3 pkt.,
 - LGD wchodzi w skład *Porozumienia o współpracy Lokalnych Grup Działania Województwa Świętokrzyskiego* – 4 pkt.
9. Na spotkania sieciujące poszczególne LGD zakwalifikowana do projektu będzie zgłaszać 2 osoby priorytetowe oraz 2 osoby rezerwowe według kolejności wskazanej przez każdą LGD.

10. W sytuacji rezygnacji z udziału w spotkaniu sieciującym przedstawiciele dowolnej LGD, na ich miejsca będą kwalifikowane osoby z listy rezerwowej, przy czym w pierwszej kolejności wybierane będą kobiety a decydować będzie kolejność zgłoszeń.
11. Lista osób rezerwowych utworzona zostanie z kandydatów/kandydatek, którzy z powodu wyczerpania limitu miejsc nie zakwalifikują się do udziału w projekcie.
12. Osoby z listy rezerwowej będą kwalifikowane do udziału w projekcie w sytuacji rezygnacji osób wcześniej zakwalifikowanych.
13. Decyzję o włączeniu do uczestnictwa w projekcie kandydata/kandydatki z listy rezerwowej podejmuje koordynator projektu.

§ 5.

Zasady uczestnictwa

1. Każda LGD uczestnicząca w projekcie zobligowana jest do zgłoszenia 2 osób priorytetowych oraz 2 osób rezerwowych, które uczestniczyć będą w spotkaniach sieciujących;
2. 12 Rad LGD dla których opracowany zostanie i wdrożony Elektroniczny System Informacji i Oceny e-LGD (ESIO) uczestniczyć będzie w 12 jednodniowych szkoleniach z zakresu zasad obsługi ESIO.
3. Osoba fizyczna uczestnicząca w projekcie zobowiązana jest do:
 - a. punktualnego i aktywnego uczestnictwa w zajęciach szkoleniowych;
 - b. potwierdzania uczestnictwa każdorazowo na liście obecności;
 - c. wypełnianie ankiet ewaluacyjnych i monitoringowych.
4. W celu uzyskania certyfikatu ukończenia szkolenia uczestnik/uczestniczka projektu zobowiązany/-a jest do uczestnictwa w co najmniej 80% zajęć objętych programem.
5. Organizator dopuszcza usprawiedliwione nieobecności spowodowane chorobą lub ważnymi sytuacjami losowymi. Usprawiedliwienie jest dokonywane na podstawie przedstawionego zwolnienia lekarskiego lub karty leczenia szpitalnego.
6. W przypadku przekroczenia dozwolonego limitu nieobecności uczestnik/uczestniczka projektu jest zobowiązany/-a do uzyskania zgody koordynatora projektu na kontynuację uczestnictwa w projekcie.
7. Uczestnik/uczestniczka projektu zostaje skreślony/-a z listy uczestników w przypadku:
 - przekroczenia dozwolonego limitu nieobecności i nie uzyskania od koordynatora projektu zgody na kontynuację uczestnictwa w projekcie,
 - złożenia pisemnej rezygnacji z uczestnictwa w projekcie.

§ 6.

Zasady monitoringu uczestników/uczestniczek szkoleń

1. Uczestnicy/uczestniczki projektu zobowiązani są podać dane niezbędne organizatorom do wypełnienia kwestionariusza PEFS którego celem jest gromadzenie informacji na temat osób i instytucji korzystających ze wsparcia w ramach EFS, oraz określenie efektywności realizowanych zadań w procesie badań ewaluacyjnych po zakończeniu realizacji projektu.
2. Uczestnicy/uczestniczki projektu mają prawo dostępu do treści swoich danych osobowych oraz ich modyfikowania.
3. Administratorem zebranych danych osobowych jest Instytucja Zarządzająca dla Programu Operacyjnego Kapitał Ludzki - Minister Rozwoju Regionalnego ul. Wspólna 2/4, 00-926 Warszawa;
4. Dane osobowe będą przetwarzane wyłącznie w celu udzielenia wsparcia i obsługi Projektu;

5. Dane osobowe mogą zostać udostępnione innym podmiotom w celu ewaluacji, jak również w celu realizacji zadań związanych z monitoringiem i sprawozdawczością w ramach Programu Operacyjnego Kapitał Ludzki
6. Podanie danych jest dobrowolne, aczkolwiek odmowa ich podania jest równoznaczna z brakiem możliwości udzielenia wsparcia w ramach Projektu;
7. Uczestnicy/uczestniczki projektu zobowiązani są do udziału we wszelkich badaniach ankietowych, ewaluacyjnych przeprowadzanych w trakcie i w przeciągu 12 miesięcy po zakończeniu realizacji projektu.
8. Uczestnicy/uczestniczki projektu już w trakcie rekrutacji akceptują zasady ewaluacji projektu, co poświadczają własnoręcznym podpisem na formularzu zgłoszeniowym.

§ 7.

Zasady rezygnacji z uczestniczenia w projekcie

1. W przypadku rezygnacji z uczestnictwa w projekcie należy niezwłocznie poinformować o tym fakcie osobiście, telefonicznie bądź za pośrednictwem poczty elektronicznej koordynatora projektu.
2. W przypadku rezygnacji z zajęć projektu w trakcie ich trwania uczestnik/uczestniczka projektu zobowiązany/-a jest do złożenia pisemnego oświadczenia dotyczącego przyczyn rezygnacji.
3. Organizator zastrzega sobie prawo skreślenia danej osoby z listy uczestników projektu w przypadku naruszenia postanowień niniejszego regulaminu oraz zasad współżycia społecznego.

§ 8.

Postanowienia końcowe

1. Regulamin wchodzi w życie z dniem 04.05.2011 r.
2. Organizator zastrzega sobie zmianę regulaminu w każdym czasie.
3. Regulamin jest dostępny na stronie internetowej projektu.

Zasady Współpracy i Komunikacji w Trakcie Realizacji Projektu

Zapewnienie sprawnej realizacji zadań w ramach projektu „Wsparcie sieci lokalnych grup działania województwa świętokrzyskiego” oraz utrzymanie wysokiej jakości wypracowywanych produktów wymaga określenia jasnych zasad współpracy oraz opracowania procedur komunikacji pomiędzy uczestnikami projektu.

W celu zapewnienia sprawnej komunikacji pomiędzy uczestnikami projektu konieczne jest określenie:

1. zasad obiegu informacji pomiędzy poziomami organizacyjnymi projektu oraz
2. zasad tworzenia, obiegu i archiwizowania dokumentów projektowych, w tym przekazywanych produktów prac.

1. Zasady obiegu informacji:

Za zapewnienie sprawnej komunikacji podczas projektu odpowiedzialne będą w różnym zakresie wszystkie poziomy organizacyjne projektu.

Koordynator projektu będzie odpowiedzialny za informowanie o postępie prac projektowych, potrzebach modyfikacji w projekcie oraz istotnych ryzykach projektu (np. zagrożenia wykonania harmonogramu). Koordynator będzie też odpowiedzialny za:

- a. przygotowanie listy zadań do realizacji w ramach projektu;
- b. opis wykonanych prac, pełną sprawozdawczość z realizacji poszczególnych zadań projektowych;
- c. szacunkową ocenę stopnia zaawansowania prac;
- d. ocenę ryzyka zagrażającego terminowej realizacji poszczególnych zadań;
- e. propozycje zmian projektowych – zmiany do harmonogramu lub zakresu prac.

Asystent koordynatora projektu odpowiedzialny będzie za pełną sprawozdawczość z zakresu realizacji poszczególnych zadań projektowych, w tym głównie:

- a. postępów w rekrutacji organizacji oraz indywidualnych uczestników do projektu;
- b. kwalifikowalności bądź niekwalifikowalności osób zainteresowanych udziałem w projekcie,
- c. zmianie danych osobowych uczestników/uczestniczek projektu (w tym głównie danych teleadresowych).

Pracownicy Sekretariatu Porozumienia – odpowiedzialni będą za pełną sprawozdawczość z zakresu pracy Sekretariatu, oraz:

- a. zbieranie wszelkich informacji od Lokalnych Grup Działania z województwa świętokrzyskiego;
- b. monitorowanie stron internetowych, w szczególności dotyczących organizacji pozarządowych i ogłoszonych konkursów dla ngo;
- c. zbieranie informacji na temat zmian w prawie dotyczącym działania Lokalnych Grup Działania;
- d. przygotowywanie cotygodniowego newslettera dla LGD.

Księgowa zobligowana jest do przekazywania koordynatorowi projektu, na 10 dni roboczych przed przygotowaniem poszczególnego wniosku o płatność, kserokopii dokumentów księgowych, tj.:

- wyciągów bankowych,
- faktur, rachunków,
- list płac,

Forma przekazania: osobiście lub pocztą.

Dokumenty księgowo, prócz faktur, winny zawierać: kolejny numer dowodu zgodny z ewidencją księgową.

Opis wszystkich dokumentów księgowych winien być zgodny z zasadami finansowania PO KL i należy na nim zamieścić:

- a. Numer umowy o dofinansowanie projektu;
- b. Informację o współfinansowaniu projektu ze środków Europejskiego Funduszu Społecznego;
- c. Nazwę zadania zgodnie z zatwierdzonym wnioskiem o dofinansowanie, w ramach którego wydatek jest poniesiony (dodatkowo adnotację, jeśli wydatek dotyczy kosztów pośrednich);
- d. Kwotę kwalifikowaną lub w przypadku, gdy dokument księgowy dotyczy kilku zadań, kilka kwot w odniesieniu do każdego zadania;
- e. Każdy dokument powinien być opatrzony informacją o poprawności merytorycznej oraz formalno-rachunkowej oraz w przypadku gdy dokument dotyczy zamówień publicznych odniesienie do ustawy z dnia 29 stycznia 2004. Prawo zamówień publicznych.

Wyciąg z ewidencji księgowej (raport) powinien umożliwić uzyskanie informacji dotyczących:

- a. Numeru faktury VAT lub innego dokument związanego z wydatkiem,
- b. Wewnętrzny numer dokumentu księgowego,
- c. Datę wystawienia dokumentu księgowego oraz datę zapłaty,
- d. Określenie zakupionego towaru/usługi (rodzaj wydatku kwalifikowanego),
- e. Kwotę wydatków kwalifikowanych (wydatki brutto kwalifikowalne i VAT kwalifikowalny),
- f. Informacje na temat poniesienia wydatków w ramach cross-financingu.

2. Zasady tworzenia, obiegu i archiwizowania dokumentów projektowych, w tym przekazywanych produktów prac

Za bieżące administrowanie procesem obiegu i archiwizacji dokumentów projektowych odpowiada Koordynator projektu. Komunikacja wewnętrzna pomiędzy Koordynatorem projektu a poszczególnymi osobami zaangażowanymi w realizację projektu będzie oparta o dwa podstawowe typy dokumentów projektowych:

- sprawozdania,
- notatki ze spotkań,

W celu usprawnienia i przyspieszenia obiegu dokumentacji projektowej wszelkie produkty prac, raporty oraz notatki ze spotkań mogą być przekazywane drogą elektroniczną (z opcją potwierdzenia). W przypadku wybranych dokumentów oraz ostatecznych wersji produktów prac wymagana będzie oprócz wersji elektronicznej również wersja papierowa dokumentów podpisana przez wykonawcę zadania. Zespoły Zadaniowe zobowiązane będą do przygotowania produktów prac w terminach i w zakresie określonym w harmonogramie.

Zasady archiwizacji dokumentacji związanej z projektem

1. Niniejsze zasady archiwizacji dokumentacji dotyczą projektu „wsparcie sieci lokalnych grup działania województwa świętokrzyskiego”.
2. Wszystkie dokumenty związane z realizacją Projektu będą przechowywane co najmniej do

3. 31 grudnia 2020 r. zgodnie z § 12, pkt. 1 umowy ramowej w sposób zapewniający dostępność, poufność i bezpieczeństwo. Realizator projektu poinformuje Instytucję Pośredniczącą o miejscu archiwizacji dokumentów związanych z realizowanym Projektem.
4. Miejsca archiwizacji dokumentacji:
 - w trakcie realizacji Projektu dokumenty będą archiwizowane w Burze Projektu, ul. Rakowska 5, Łągów; pokój nr
 - po zakończeniu realizacji Projektu dokumenty będą archiwizowane w:
.....
5. Realizator Projektu obowiązkowo będzie przechowywał dokumenty:
 - a. oryginał złożonego wniosku o dofinansowanie projektu,
 - b. pisma informujące o akceptacji wniosku i przyznaniu dofinansowania,
 - c. umowę o dofinansowaniu projektu,
 - d. faktury i inne dokumenty potwierdzające poniesienie wydatków,
 - e. wyciągi z konta bankowego projektu,
 - f. sprawozdania i dokumenty potwierdzające zawarte w nich informacje,
 - g. wnioski płatnicze,
 - h. istotną korespondencję, w tym zwłaszcza dotyczącą zmian w projekcie,
 - i. umowy z wykonawcami wraz z dokumentacją dotyczącą sposobu wyłonienia wykonawcy,
 - j. wykaz beneficjentów ostatecznych projektu oraz zestawienie danych ich dotyczących,
 - k. listy obecności uczestników szkoleń i trenerów,
 - l. programy zajęć szkoleniowych,
 - m. dokumenty potwierdzające osiągnięcie przez beneficjentów ostatecznych określonych rezultatów,
 - n. ankiety oceny projektu przez beneficjentów ostatecznych.
6. Dopuszcza się w uzasadnionych przypadkach archiwizację dokumentów na nośnikach CD, jednak preferowane są wersje wydrukowane dokumentacji.



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI



MINISTERSTWO PRACY
I POLITYKI SPOŁECZNEJ

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



**POLITYKA BEZPIECZEŃSTWA
DLA ZBIORU *PODSYSTEM MONITOROWANIA*
EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007
U BENEFICJENTA PO KL**

§ 1.

Postanowienia ogólne

Polityka Bezpieczeństwa dla zbioru *Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007* u Beneficjenta PO KL, zwana dalej „Polityką”, określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorze *Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007*, zwanym dalej „PEFS 2007”, w Stowarzyszeniu Rozwoju Wsi Świętokrzyskiej z siedzibą w Łagowie, zwanym dalej „Beneficjentem”.

§ 2.

Użyte w Polityce określenia oznaczają:

Administrator Danych	- Instytucję Zarządzającą PO KL;
ustawa	- ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);
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);
użytkownik	- osobę upoważnioną do przetwarzania danych osobowych w PEFS 2007;
Administrator Bezpieczeństwa Informacji	- osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007;
Administrator Bezpieczeństwa Informacji PEFS 2007 w IP/IP2	- osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 w IP/IP2;

Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta	- osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w PEFS 2007 u Beneficjenta;
Administrator Systemu u Beneficjenta	- osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych w PEFS 2007 u Beneficjenta, o ile zadania te zostały wyłączone z zakresu kompetencji Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta i powierzone przez osobę upoważnioną do podejmowania decyzji u Beneficjenta innemu pracownikowi;
naruszenie zabezpieczenia PEFS 2007	- jakiegokolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności PEFS 2007;
dane osobowe	- wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
przetwarzanie danych osobowych	- jakiegokolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;
usuwanie danych osobowych	- zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
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;

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;
Instrukcja	- Instrukcję Zarządzania Systemem Informatycznym dla systemu <i>Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007</i> u Beneficjenta;
Pracownik	- osobę zatrudnioną u Beneficjenta na podstawie stosunku pracy lub innego stosunku prawnego;
Ministerstwo	- Ministerstwo Rozwoju Regionalnego.

§ 3.

Niniejszą politykę stosuje się do zbioru danych osobowych PEFS 2007 znajdujących się u Beneficjenta.

§ 4.

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

§ 5.

Dane osobowe przetwarzane w PEFS 2007 podlegają ochronie zgodnie z przepisami ustawy.

§ 6.

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.

§ 7.

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 sądowym lub administracyjnym.

§ 8.

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:

- a. pełnej nazwie Ministerstwa oraz jego adresie;
- b. celu zbierania danych osobowych;
- c. prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
- d. dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością wzięcia udziału w projekcie realizowanym w ramach Programu Operacyjnego Kapitał Ludzki.

§ 9.

Jakiegokolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w ustawie oraz w pełnej zgodności z przepisami prawa.

Wnioski o udostępnienie danych osobowych przetwarzanych w PEFS 2007, po wstępnym rozpatrzeniu przez Administratora Bezpieczeństwa Informacji, są rozpatrywane przez Administratora Danych.

§ 10.

Przetwarzanie danych osobowych znajdujących się w PEFS 2007 może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 6, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy ustawy, rozporządzenia oraz umowy o dofinansowanie projektu.

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 Informacji PEFS 2007 u Beneficjenta.

§ 11.

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

- uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
- uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
- uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;

- uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
- uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
- 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.

§ 12.

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

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

§ 13.

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.

§ 14.

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

§ 15.

Do zadań Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta należy w szczególności:

- współdziałanie z Administratorem Bezpieczeństwa Informacji PEFS 2007 w IP/IP2 w zakresie zapewniającym wypełnianie przez Beneficjenta obowiązków wynikających z ustawy i rozporządzenia;
- prowadzenie i aktualizacja rejestru, o którym mowa w § 20, który stanowi załącznik nr 1 do Polityki;

- prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w PEFS 2007 u Beneficjenta, który stanowi załącznik nr 2 do Polityki;
- analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych w ramach PEFS 2007 u Beneficjenta oraz pisemne informowanie o wynikach analizy osoby upoważnione do podejmowania decyzji w imieniu Beneficjenta;
- opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych w PEFS 2007 podmiotowi zewnętrznemu wobec Beneficjenta;
- inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych w PEFS 2007 u Beneficjenta.

§ 16.

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

§ 17.

Obowiązki Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta wykonywane są przez wyznaczonego przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta Pracownika.

Nadzór nad wykonywaniem obowiązków Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta i, o ile został powołany, Administratora Systemu u Beneficjenta pełni osoba upoważniona do podejmowania decyzji w imieniu Beneficjenta.

§ 18.

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

§ 19.

Do przetwarzania danych osobowych w PEFS 2007 mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienie wydane przez upoważnioną do tego osobę. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach do umowy o dofinansowanie projektu.

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.

Pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją przez złożenie podpisu na liście prowadzonej przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta, której wzór jest określony w załączniku nr 3 do Polityki.

§ 20.

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 PEFS 2007 u Beneficjenta.

Rejestr, o którym mowa w ust. 1, zawiera:

- imię i nazwisko pracownika;
- jego identyfikator w systemie informatycznym służącym przetwarzaniu danych w PEFS 2007;
- zakres przydzielonego uprawnienia;
- datę przyznania uprawnień;
- podpis Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta potwierdzający przyznanie uprawnień;
- datę odebrania uprawnień
- podpis Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta potwierdzający odebranie uprawnień.

§ 21.

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 PEFS 2007 u Beneficjenta oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych. W takim przypadku § 19 i 20 stosuje się odpowiednio.

Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 22.

Wszyscy pracownicy oraz osoby, o których mowa w § 21 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.

§ 23.

Użytkownicy są w szczególności zobowiązani do:

- bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w PEFS 2007, określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania PEFS 2007 oraz jego obsługi;

- przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
- 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;
- niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
- 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;
- bezzwłocznego zawiadomiania Administratora Bezpieczeństwa Informacji PEFS 2007 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.

§ 24.

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

§ 25.

Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

- stwierdzono naruszenie zabezpieczenia PEFS 2007;
- stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych;
- inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych w PEFS 2007.

§ 26.

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 PEFS 2007 u Beneficjenta.

Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:

- poinformować pisemnie o zaistniałym zdarzeniu Administratora Bezpieczeństwa Informacji PEFS 2007 w IP/IP2 i stosować się do jego zaleceń;
- zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu.

Administrator Bezpieczeństwa Informacji u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych w PEFS 2007 jest zobowiązany niezwłocznie:

- wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i podpisać;
- przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby niepowołanej do danych osobowych w systemie informatycznym służącym przetwarzaniu danych osobowych w PEFS 2007;
- podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych, w szczególności przez:
 - fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej,
 - wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
 - zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu;
- szczegółowo analizować stan systemu informatycznego służącego przetwarzaniu danych osobowych w PEFS 2007 w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;
- przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych w PEFS 2007.

Czynności opisane w ust. 3 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 27.

Po przywróceniu normalnego stanu PEFS 2007 należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych w PEFS 2007.

Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

Jeżeli przyczyną 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 § 21 ust. 1.

§ 28.

Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia PEFS 2007 i w terminie 21

dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia PEFS 2007 przekazuje go Administratorowi Bezpieczeństwa Informacji w IP/IP2.

Jeżeli naruszenie zabezpieczenia PEFS 2007 nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych w PEFS 2007 Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta przygotowując raport, o którym mowa w ust. 1 współpracuje z Administratorem Systemu u Beneficjenta, o ile został powołany.

§ 29.

Bieżąca kontrola nad przetwarzaniem danych osobowych w PEFS 2007 u Beneficjenta jest dokonywana przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

W ramach kontroli, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§ 30.

Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta przeprowadza w pierwszym kwartale roku kalendarzowym kontrolę w zakresie przestrzegania przez użytkowników Polityki, Instrukcji oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport.

Przygotowując raport, o którym mowa w ust. 1, Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta uwzględnia informacje zawarte w raportach, o których mowa w § 28.

§ 31.

Kontrola, o której mowa w § 30, polega w szczególności na sprawdzeniu:

- którzy pracownicy mają dostęp do danych osobowych;
- czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom lub osobom;
- czy pracownicy i inne osoby mające dostęp do danych osobowych przetwarzanych w PEFS 2007 posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę .

§ 32.

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

§ 33.

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

§ 34.

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia PEFS 2007.

§ 35.

Wykazy i rejestry znajdujące się w załącznikach nr 1-3 do Polityki, prowadzi Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

Wykaz znajdujący się w załączniku nr 4 do Polityki prowadzi w zakresie środków organizacyjnych Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta, zaś w zakresie środków technicznych Administrator Systemu u Beneficjenta, o ile został powołany.

§ 36.

Integralną część niniejszej Polityki stanowią następujące załączniki:

Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych w PEFS 2007 u Beneficjenta PO KL;

Załącznik nr 2 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe w PEFS 2007;

Załącznik nr 3 – Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;

Załącznik nr 4 – Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych

w ramach PEFS 2007;

Załącznik nr 5 – Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

Załącznik nr 6 – Instrukcja zarządzania systemem informatycznym dla systemu *Podsystem monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL*.

Załącznik nr 1
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
u Beneficjenta PO KL

Rejestr osób upoważnionych do przetwarzania danych osobowych w PEFS 2007 u Beneficjenta PO KL

Lp.	Imię i nazwisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Podpis ABI PEFS 2007 u Beneficjenta	Data odebrania uprawnień	Podpis ABI PEFS 2007 u Beneficjenta
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Załącznik nr 3
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
u Beneficjenta PO KL

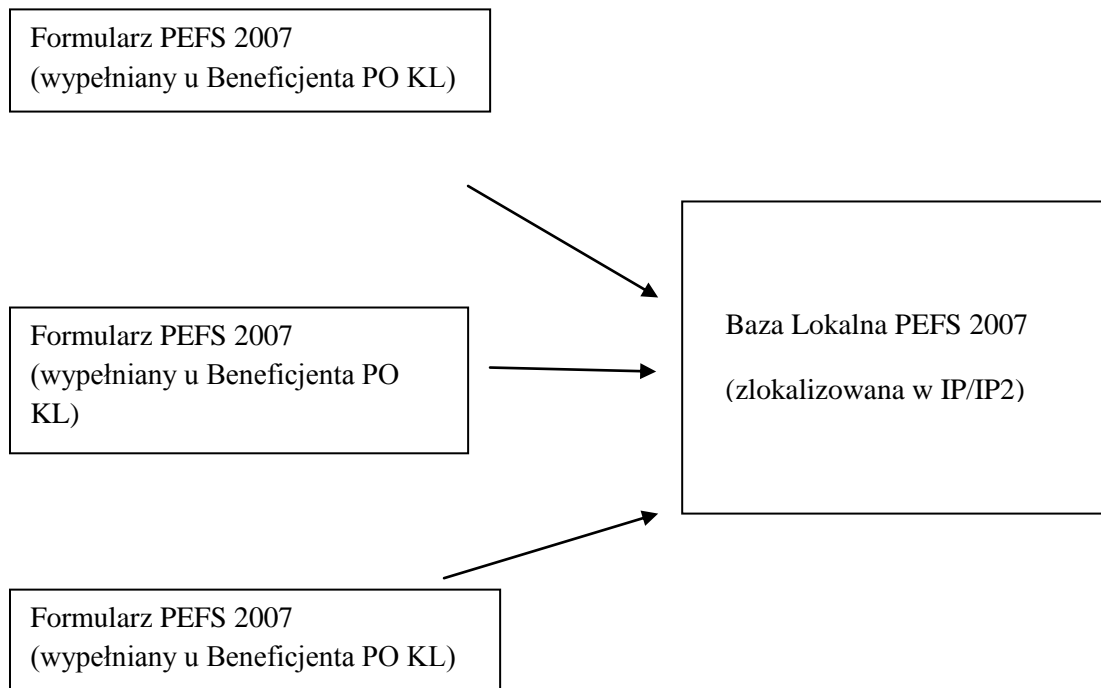
Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

Oświadczam, iż zapoznałem/am się z:
przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz
z przepisami wykonawczymi do niniejszej ustawy,
Polityką Bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta PO KL oraz
Instrukcją Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
u Beneficjenta PO KL.

Lp.	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z ww. dokumentami
1			
2			
3			

Załącznik nr 4
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego
Funduszu Społecznego 2007 u Beneficjenta PO KL

Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w ramach PEFS 2007



Procedura przekazywania IP/IP2 Formularza PEFS 2007 przez Beneficjentów*

Formularz PEFS 2007 powinien zostać dostarczony na płycie CD lub innym nośniku danych do właściwej instytucji, do której składany jest wniosek beneficjenta o płatność, osobiście lub przesłany pocztą tradycyjną za potwierdzeniem odbioru.

Przekazywane dane powinny zostać uprzednio skompresowane do jednego z formatów: ZIP, TAR, GZ lub RAR oraz zabezpieczone hasłem z wykorzystaniem programu 7-Zip lub WinRAR. Użycie innego programu kompresującego jest dopuszczalne pod warunkiem, że instytucja do której składany jest wniosek o płatność wraz z Formularzem PEFS 2007 dysponuje adekwatnym narzędziem dekompresującym.

Hasło, przy użyciu którego zostaną zabezpieczone dane, powinno zostać przekazane do instytucji, do której dane będą kierowane w odrębnej niż zabezpieczony Formularz przesyłce. Niedopuszczalne jest przesyłanie Formularza PEFS 2007 z danymi pocztą elektroniczną.

Niestosowanie się do w/w procedury będzie uznawane przez IZ za rażące naruszenie przepisów o ochronie danych osobowych.

**Załącznik nr 5
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego
Funduszu Społecznego 2007 u Beneficjenta PO KL**

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Zbiór danych osobowych:

- Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007

Programy zastosowane do przetwarzania danych osobowych:

- Formularz PEFS 2007

Załącznik nr 6
do Polityki Bezpieczeństwa dla systemu Podsystem Monitorowania Europejskiego
Funduszu Społecznego 2007 u Beneficjenta PO KL

Rozdział 1
Przydział haseł i identyfikatorów

§ 1.

1. Dla każdego użytkownika jest ustalany odrębny identyfikator i hasło dostępu do PEFS 2007.
2. Identyfikator użytkownika:
 - a) jest niepowtarzalny, a po wyrejestrowaniu użytkownika z PEFS 2007 nie jest przydzielany innej osobie;
 - b) jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, wraz z imieniem i nazwiskiem użytkownika.
3. Hasło użytkownika:
 - a) jest przydzielane indywidualnie dla każdego z użytkowników;
 - b) nie jest zapisane w systemie komputerowym w postaci jawnej.

§ 2.

1. Osobą odpowiedzialną za przydział identyfikatorów i pierwszych haseł dla użytkowników u Beneficjenta jest Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Przydziału i zmiany haseł dokonuje się w następujący sposób:
 - a) hasła powinny mieć co najmniej 5 znaków
 - b) hasła nie powinny składać się z kombinacji znaków mogących ułatwić ich odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika);
 - c) hasło powinno zostać zmienione niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że mogły się z nim zapoznać osoby trzecie.

§ 3.

1. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora, który został mu przyznany.
2. Użytkownik jest zobowiązany utrzymywać hasło, którym się posługuje lub posługiwał, w ścisłej tajemnicy, w szczególności dołożyć wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem, nawet po ustaniu jego ważności.

Rozdział 2
Rejestrowanie i wyrejestrowywanie użytkowników

§ 4.

1. Rejestracji i wyrejestrowywania użytkowników dokonuje Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta prowadzi rejestr użytkowników, który stanowi załącznik nr 1 do Polityki Bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta.
3. Jakakolwiek zmiana informacji ujawnionych w rejestrze podlega natychmiastowemu odnotowaniu i uaktualnieniu.
4. W PEFS 2007 może zostać zarejestrowany jedynie użytkownik, któremu osoba upoważniona

do tego osoba wydała upoważnienie do przetwarzania danych osobowych w PEFS 2007

§ 5.

1. Po zarejestrowaniu w PEFS 2007 użytkownik jest informowany przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta o ustalonym dla niego identyfikatorze i konieczności posługiwania się hasłami.
2. Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta jest odpowiedzialny za zapoznanie każdego nowego użytkownika z Instrukcją oraz Polityką Bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta, a także z przepisami dotyczącymi ochrony danych osobowych, co użytkownik potwierdza swoim podpisem na liście, stanowiącej załącznik nr 3 do Polityki Bezpieczeństwa dla zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta.

§ 6.

Użytkownik jest wyrejestrowywany z PEFS 2007 w każdym przypadku utraty przez niego uprawnień do przetwarzania danych osobowych w PEFS 2007, co ma miejsce szczególnie w przypadku:

- 1) ustania zatrudnienia tego użytkownika u Beneficjenta lub zakończeniu przez tego użytkownika współpracy z Beneficjentem na podstawie umowy cywilno-prawnej;
- 2) zmiany zakresu obowiązków użytkownika powodujących utratę uprawnień do przetwarzania danych osobowych w PEFS 2007.

Rozdział 3

Rozpoczęcie, zawieszenie i zakończenie pracy w PEFS 2007

§ 7.

1. Użytkownik rozpoczynając pracę jest zobowiązany zalogować się do PEFS 2007 posługując się swoim identyfikatorem i hasłem.
2. W przypadku, gdy użytkownik planuje przerwać pracę, jest zobowiązany do zabezpieczenia dostępu do komputera za pomocą wygaszacza ekranu z aktywnym hasłem.
3. W przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres, a także kończąc pracę, jest zobowiązany wylogować się z PEFS 2007 oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki zawierające dane osobowe.

§ 8.

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczenia PEFS 2007 lub zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w PEFS 2007, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych w PEFS 2007, użytkownik jest zobowiązany niezwłocznie poinformować o tym Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. O każdym przypadku naruszenia zabezpieczenia PEFS 2007 Administrator Bezpieczeństwa Informacji u Beneficjenta jest zobowiązany poinformować w formie pisemnej Administratora Bezpieczeństwa Informacji w IP/IP2.
3. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w ust. 1.

Rozdział 4

Tworzenie oraz przechowywanie kopii awaryjnych

§ 9.

1. Za tworzenie i przechowywanie u Beneficjenta kopii awaryjnych danych osobowych przetwarzanych w PEFS 2007 w sposób zgodny z przepisami prawa oraz poniższymi procedurami jest odpowiedzialny Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Kopie awaryjne danych osobowych przetwarzanych w PEFS 2007 są tworzone nie rzadziej niż raz na kwartał i zawierają pełny obraz danych osobowych w PEFS 2007 u Beneficjenta.
3. Kopie o których mowa w ust. 1 przechowuje się odpowiednio zabezpieczone przed dostępem osób nieuprawnionych w różnych miejscach, w tym w lokalizacjach innych niż zbiór danych osobowych eksploatowany na bieżąco.
4. Kopie awaryjne danych osobowych przetwarzanych w PEFS 2007 po ustaniu ich użyteczności są bezzwłocznie usuwane.
5. Kopie awaryjne danych osobowych przetwarzanych w PEFS 2007, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.

Rozdział 5

Ochrona PEFS 2007 przed wrogim oprogramowaniem

§10.

1. Bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego i kradnącego hasła odbywa się przy zastosowaniu zainstalowanego na każdej stacji roboczej aktualizowanego na bieżąco programu antywirusowego automatycznie monitorującego występowanie wirusów, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego, oprogramowania kradnącego hasła podczas operacji na plikach;
2. Nadzór nad instalowaniem oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

§ 11.

1. O każdorazowym wykryciu wirusa lub konia trojańskiego przez oprogramowanie monitorujące użytkownik jest zobowiązany niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Po usunięciu wirusa lub innego niebezpiecznego oprogramowania Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta, sprawdza PEFS 2007 oraz przywraca go do pełnej funkcjonalności i sprawności.

§ 12.

1. Dyski lub inne informatyczne nośniki zawierające dane osobowe przetwarzane w PEFS 2007 są przechowywane w sposób uniemożliwiający dostęp do nich osobom innym niż użytkownicy.
2. Żadne nośniki informacji zawierające dane osobowe nie są udostępniane poza obszar, w którym są przetwarzane dane osobowe.
3. Zapis w ust. 1 nie dotyczy sytuacji, o której mowa w § 29 pkt. 1 ustawy o ochronie danych osobowych, tzn. udostępnia posiadanych w zbiorze danych osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, w szczególności przekazania przez Beneficjenta danych z PEFS 2007 właściwej Instytucji Pośredniczącej/Instytucji

Pośredniczącej II Stopnia.

Rozdział 6

Przeglądy i konserwacja PEFS 2007, sprzętu komputerowego oraz zbioru danych osobowych

§ 13.

1. Przeglądy i konserwacje sprzętu komputerowego wynikające ze zużycia sprzętu oraz warunków zewnętrznych i eksploatacji, z uwzględnieniem ważności sprzętu dla funkcjonowania PEFS 2007, są dokonywane przez Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.
2. Dyski lub inne informatyczne nośniki informacji umieszczone w urządzeniach przeznaczonych do napraw, gdzie jest wymagane zaangażowanie zewnętrznych firm serwisowych, usuwa się z tych urządzeń lub pozbawia się przed naprawą zapisu danych osobowych przetwarzanych w PEFS 2007.
3. W przypadku niemożliwości usunięcia nośnika lub pozbawienia go zapisu tych danych osobowych naprawy dokonuje się pod nadzorem Administratora Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

Rozdział 7

Wymagania sprzętowo-organizacyjne

§ 14.

1. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.
2. Komputery powinny zostać ustawione w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną użytkowników.
3. Osoby nieuprawnione do dostępu do danych osobowych w PEFS 2007 mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe w PEFS 2007 wyłącznie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 15.

Decyzję o instalacji na stacji roboczej obsługującej przetwarzanie danych osobowych w PEFS 2007 jakiegokolwiek oprogramowania systemowego lub użytkowego podejmuje Administrator Bezpieczeństwa Informacji PEFS 2007 u Beneficjenta.

Rozdział 8

Postanowienia końcowe

§ 16.

1. Do spraw nieuregulowanych w Instrukcji stosuje się przepisy o ochronie danych osobowych.
2. Instrukcja nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia PEFS 2007.