**Załącznik do Zarządzenia Nr 54/2017**
**Wójta Gminy Sławatycze**
**z dnia 31 grudnia 2017 r.**

# POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W PROJEKTACH UNIJNYCH

## DLA ZBIORÓW:

„UCZESTNICY PROJEKTÓW DOFINANSOWANYCH Z EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO W RAMACH REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA LUBELSKIEGO 2014-2020" ORAZ CENTRALNY SYSTEM TELEINFORMATYCZNY WSPIERAJĄCY REALIZACJĘ PROGRAMÓW OPERACYJNYCH

## Rozdział 1

## Postanowienia ogólne

### §1.

Polityka Bezpieczeństwa ochrony danych osobowych w Urzędzie Gminy w Sławatyczach dla zbiorów: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020" oraz „Centralny system teleinformatyczny wspierający realizację programów operacyjnych" zwana dalej „Polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorze danych osobowych dla projektu współfinansowanych ze środków Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego na lata 2014-2020 w Urzędzie Gminy w Sławatyczach, zwanym dalej „Beneficjentem".

### §2.

Użyte w Polityce określenia oznaczają:

**Ustawa** - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)

**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. z 2004 r. nr 100. poz. 1024);

**Instytucja Zarządzająca** - należy przez to rozumieć instytucję zaangażowaną w realizację projektu „Środowiskowe i dzienne wsparcie dzieci i młodzieży w Gminie Sławatycze" z którą Beneficjent zawarł umowę o dofinansowanie projektu - Zarząd Województwa Lubelskiego;

**System SL2014** - należy przez to rozumieć aplikację główną centralnego systemu teleinformatycznego, wykorzystywany w procesie rozliczania Projektu oraz komunikowania się z Instytucją Zarządzającą, o którym mowa w Wytycznych Ministra Infrastruktury i Rozwoju w zakresie warunków gromadzenia i przechowywania danych w postaci elektronicznej na lata 2014-2020;

**SZT** - System zarządzania tożsamością — aplikacja wspierająca zarządzanie procesami logowania w ramach centralnego systemu teleinformatycznego. Umożliwia zalogowanie się do systemu SL2014;

**Operator** - należy przez to rozumieć urząd obsługujący ministra właściwego do spraw rozwoju regionalnego;

**Beneficjent** - Gmina Sławatycze;

**Użytkownik** - należy przez to rozumieć osobę mającą dostęp do Systemu SL2014, wyznaczoną przez Beneficjenta do wykonywania w jego imieniu czynności związanych z realizacją projektu;

**Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej dane osobowe, w rozumieniu ustawy, dotyczące:
a) pracowników Beneficjenta.

b) uczestników projektów realizowanych ze środków EFS w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020,
c) osób, których dane są przetwarzane w związku z badaniem kwalifikowalności wydatków w projekcie, w tym w szczególności personelu projektu, a także oferentów, uczestników komisji przetargowych i wykonawców przetwarzanie przez Beneficjenta w celu realizacji projektu;

**Administrator danych osobowych** - Zarząd Województwa Lubelskiego - Instytucja Zarządzająca (IZ) dla zbiorów „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020" Minister Rozwoju dla zbioru Centralny system teleinformatyczny wspierający realizację programów operacyjnych;

**Przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, przechowywaniu, opracowywaniu, zmienianiu, udostępnianiu i usuwaniu danych osobowych, zwłaszcza te, które wykonuje się w systemie informatycznym;

**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 w systemie informatycznym** - 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;

**Naruszenie zabezpieczenia** - jakiekolwiek zdarzenie lub działanie, które może stanowić przyczynę utraty zasobów, niezawodności, integralności lub poufności;

**Administrator Bezpieczeństwa Informacji** - ABI - osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w instytucji zarządzającej;

**Administrator Danych u Beneficjenta** - Wójt Gminy Sławatycze;

**Administrator Systemu Informatycznego u Beneficjenta** - ASI - osoba odpowiedzialna za sprawność, konserwację, oraz wdrażanie technicznych zabezpieczeń systemu informatycznego u Beneficjenta.

## Rozdział 2

## Zakres oraz zasady zabezpieczania danych osobowych

### §3.

Niniejszą politykę stosuje się do zbiorów danych osobowych dla projektów współfinansowanych ze środków Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego na lata 2014-2020 znajdujących się u Beneficjenta.

## §4.

1. Instytucja Zarządzająca powierza Beneficjentowi przetwarzanie danych osobowych.
2. Zakres danych osobowych przetwarzanych przez Użytkownika w Systemie nie może być większy niż powierzony do przetwarzania przez Instytucję Zarządzającą.
3. Dane osobowe są przetwarzane wyłącznie w celu realizacji umowy na realizację projektu współfinansowanego z Unii Europejskiej w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego na lata 2014-2020
4. Użytkownik odpowiada za zgodność z dokumentami źródłowymi, danych osobowych wprowadzonych przez siebie do Systemu SL2014.
5. Obszar, w którym przetwarzane są dane osobowe, zabezpieczone są przed dostępem osób nieuprawnionych.
6. Przetwarzanie danych osobowych w formie elektronicznej odbywa się wyłącznie na komputerach służbowych i obsługiwanych przez uprawnione osoby na podstawie upoważnienia wydanego przez Administratora Danych.
7. Administratorem danych dla zbioru:
   a) „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020" jest Województwo Lubelskie z siedzibą przy ul. Grottgera 4, 20-029 Lublin
   b) Centralny system teleinformatyczny wspierający realizację programów operacyjnych" jest Minister Rozwoju
8. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby upoważnione przez Beneficjenta, posiadające imienne upoważnienie do przetwarzania danych osobowych.
9. Instytucja Zarządzająca umocowuje Beneficjenta do wydawania i odwoływania imiennych upoważnień do przetwarzania danych osobowych w zbiorach: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020". Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych stanowią załącznik do umowy o dofinansowanie. Upoważnienia są przechowywane w siedzibie Beneficjenta.
10. Upoważnienia do przetwarzania danych osobowych w zbiorze „Centralny system teleinformatyczny wspierający realizację programów operacyjnych" wydaje Minister Rozwoju.
11. Imienne upoważnienia są ważne do dnia odwołania. Upoważnienie wygasa z chwilą ustania stosunku prawnego łączącego Beneficjenta z osobą, której wydano upoważnienie. Beneficjent powinien posiadać przynajmniej jedną osobę legitymującą się imiennym upoważnieniem do przetwarzania danych osobowych odpowiedzialną za nadzór nad zarchiwizowaną dokumentacją.
12. Beneficjent prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w związku z wykonywaniem umowy o dofinansowanie. - Załącznik nr 1 do Polityki bezpieczeństwa
13. Beneficjent niezwłocznie informuje Instytucję Zarządzającą o:
    1) wszelkich przypadkach naruszenia tajemnicy danych osobowych lub o ich niewłaściwym użyciu;
    2) wszystkich czynnościach z własnym udziałem w sprawach dotyczących ochrony danych osobowych prowadzonych w szczególności przed Generalnym Inspektoratem Ochrony Danych Osobowych, urzędami państwowymi, policją lub przed sądem;
    3) wynikach kontroli prowadzonych przez podmioty uprawnione w zakresie przewarzania danych osobowych wraz z informacją na temat zastosowania się do wydanych zaleceń.

§5.

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

§6.

Dane osobowe przetwarzane w zbiorze podlegają ochronie zgodnie z przepisami ustawy.

§7.

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą wyrazi na to zgodę, a w przypadku osób niepełnoletnich taką zgodę musi wyrazić opiekun prawny.
2. Powierzone dane osobowe mogą być przetwarzane przez Beneficjenta wyłącznie w celu:

    1) udzielania wsparcia uczestnikom Projektu, z uwzględnieniem rekrutacji, działań informacyjnych, monitorowania, sprawozdawczości, ewaluacji, kontroli i audytu prowadzonych w zakresie projektu dotyczy zbioru „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020"
    2) zarządzania, kontroli, audytu, ewaluacji, sprawozdawczości i raportowania w ramach Programu oraz zapewnienia realizacji obowiązku informacyjnego dotyczącego przekazywania do publicznej wiadomości informacji o podmiotach uzyskujących wsparcie z funduszy polityki spójności w ramach Programu dotyczy zbioru „Centralny system teleinformatyczny wspierający realizację programów operacyjnych".

§8.

Przetwarzanie danych osobowych 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 wskazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§9.

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

3) adresie swojej siedziby i pełnej nazwie
4) celu zbierania danych osobowych:
5) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
6) dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością wzięcia udziału w Projekcie.

§ 10

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

§ 11

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

§ 12

Każdej osobie, której dane osobowe są przetwarzane w zbiorze przysługuje prawo do kontroli przetwarzania jej 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, a 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 maksymalnie 30 dni od dnia wpłynięcia wniosku do Beneficjenta, wskazać w powszechnie zrozumiałej formie:
1) jakie dane osobowe dotyczące zapytującej osoby są przetwarzane przez Beneficjenta;
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 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.

## Rozdział 4

## Obowiązki Administratora Danych, Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego u Beneficjenta

### §15.

Administrator Danych u Beneficjenta jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym. Administrator Danych poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych u Beneficjenta.
Administrator Danych u Beneficjenta wyznacza Administratora Systemu Informatycznego u Beneficjenta.

### §17.

Do zadań Administratora Systemu Informatycznego u Beneficjenta należy w szczególności:
1) odpowiedzialność za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych dla projektów współfinansowanych ze środków EFS w ramach RPO WL na lata 2014-2020
2) zapewnienie bezpieczeństwa systemu informatycznego
3) nadzór nad siecią komputerową
4) wykonywanie czynności związanych z naprawami i modernizacją sprzętu komputerowego
5) wykonywanie czynności związanych z usuwaniem awarii sprzętu komputerowego
6) wykonywanie innych zadań zleconych przez Administratora Danych

### § 18.

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

## Rozdział 5

## Przetwarzanie danych osobowych

### §19.

1. Do przetwarzania danych osobowych w zbiorach: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020" 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 Załączniku do umowy o dofinansowanie projektu.
2. Każdy pracownik, przed dopuszczeniem go do przetwarzania danych osobowych w zbiorach: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020", 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 Danych u Beneficjenta, której wzór jest określony w Załączniku nr 2 do Polityki.

**§ 20.**

Każdy pracownik mający dostęp do danych osobowych w zbiorach: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020" jest wpisywany do rejestru - ewidencji osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Administratora Danych u Beneficjenta.
Rejestr ewidencji , o którym mowa w ust. 1, zawiera:
1) imię i nazwisko pracownika;
2) jego identyfikator w systemie informatycznym służącym przetwarzaniu danych w SL2014;
3) zakres przydzielonego uprawnienia;
4) datę przyznania uprawnień;
5) datę odebrania uprawnień
6) podpis Administratora Danych u Beneficjenta.

**§ 20.**

1. Dopuszczenie do przetwarzania danych osobowych znajdujących się w zbiorach: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020" przez osoby niebędące pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii Administratora Danych u Beneficjenta oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych. W takim przypadku § 19 i 20 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.

**§ 22.**

Wszyscy pracownicy oraz osoby, o których mowa w § 21 ust. 1. mają obowiązek zachowania tajemnicy o przetwarzanych w zbiorach: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020", 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:
1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w zbiorze danych osobowych określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania SL2014 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 oraz jego obsługi;
4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;

5) nieudzielania informacji o danych osobowych przetwarzanych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
6) bezzwłocznego zawiadamiania Administratora Danych u Beneficjenta o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

## Rozdział 6

## Postępowanie w przypadku naruszenia ochrony danych osobowych

### § 24.

Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:
1) stwierdzono naruszenie zabezpieczenia w zbiorze przetwarzanych danych osobowych
2) 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;
3) inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych w zbiorze danych osobowych.

### §25.

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych w zbiorze danych, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Administratora Danych u Beneficjenta.
2. Administrator Danych u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:
   1) poinformować pisemnie o zaistniałym zdarzeniu Administratora Danych w IZ i stosować się do jego zaleceń;
   2) 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.
3. Administrator Systemu Informatycznego u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych jest zobowiązany niezwłocznie:
   1) wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i podpisać;
   2) 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:
   3) 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:
      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:
   4) szczegółowo analizować stan systemu informatycznego służącego przetwarzaniu danych osobowych w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;

5) przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych.

**§26.**

1. Po przywróceniu normalnego stanu 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.
2. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych.
3. 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.
4. 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.

**§ 27.**

1. Administrator Danych u Beneficjenta przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia w zbiorze danych i w terminie 21 dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia przekazuje go Administratorowi Danych w IZ.
2. Jeżeli naruszenie zabezpieczenia w zbiorze danych nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych Administrator Danych u Beneficjenta przygotowując raport, o którym mowa w ust. 1 współpracuje z Administratorem Systemu Informacji u Beneficjenta.

## Rozdział 7
## Kontrola nad przestrzeganiem ochrony danych osobowych

**§28.**

1. Bieżąca kontrola nad przetwarzaniem danych osobowych u Beneficjenta jest dokonywana przez Administratora Danych u Beneficjenta.
2. W ramach kontroli, o której mowa w ust. 1 Administrator Danych u Beneficjenta jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

**§ 29.**

Kontrola, o której mowa w § 29. polega w szczególności na sprawdzeniu:
1) którzy pracownicy mają 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 zbiorze danych posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

## Rozdział 8

## Postanowienia końcowe

### §30.

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

### §31.

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

### § 32.

Administrator Danych u Beneficjenta jest odpowiedzialny za zapoznanie każdego nowego użytkownika z Instrukcją oraz Polityką Bezpieczeństwa u Beneficjenta, a także z przepisami dotyczącymi ochrony danych osobowych, co użytkownik potwierdza swoim podpisem na liście, stanowiącej Załącznik nr 4 do Polityki Bezpieczeństwa.

### §33.

Wykazy i rejestry znajdujące się w załącznikach nr 1,4,5 do Polityki, prowadzi Administrator Danych u Beneficjenta.

### § 34.

Integralną część niniejszej Polityki stanowią następujące załączniki:

1) Załącznik nr 1 - Rejestr, ewidencja osób upoważnionych do przetwarzania danych osobowych:
2) Załącznik nr 2 – Wzór Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
3) Załącznik nr 3 - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe dla projektów współfinansowanych ze środków EFS w ramach RPO WL 2014-2020";
4) Załącznik nr 4 - Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

WÓJT
Grzegorz Kiec

# EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH
## w Urzędzie Gminy w Sławatyczach

| Lp. | Imię i nazwisko osoby upoważnionej | Upoważnienie nr | Zakres upoważnienia do przetwarzania danych osobowych | Data nadania uprawnień | Data ustania uprawnień | Identyfikator[1] |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

[1] identyfikator nadaje się wyłącznie pracownikowi przetwarzającemu dane osobowe w systemie informatycznym

## 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 2016 r. poz. 922) oraz przepisami wykonawczymi do niniejszej ustawy.
- Polityką Bezpieczeństwa ochrony danych osobowych oraz z Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Sławatyczach dla projektów współfinansowanych ze środków EFS w ramach RPO WL na lata 2014 - 2020

| Lp. | Imię i nazwisko | Data | Podpis potwierdzający zapoznanie się z ww. dokumentami |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |

# Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe dla projektów współfinansowanych ze środków EFS w ramach RPO WL 2014-2020"

| Lp. | Budynek - dane adresowe | Pomieszczenie | |
|---|---|---|---|
| | | Piętro | Numer pomieszczenia |
| 1. | Budynek Urzędu Gminy w Sławatyczach<br>ul. Rynek 14, 21-515 Sławatycze tel. 83 378 33 58 | I piętro | Pok. nr 2 – pierwsze pomieszczenie po prawej stronie<br><br>Pok. nr 6 - czwarte pomieszczenie po prawej stronie<br><br>Pok. nr 11 - pierwsze pomieszczenie po lewej stronie |

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

Zbiór danych osobowych:
- Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
- Centralny system teleinformatyczny wspierający realizację programów operacyjnych

Programy zastosowane do przetwarzania danych osobowych:
- SL2014 Centralny System Teleinformatyczny