Legnickie Stowarzyszenie
Inicjatyw Obywatelskich

ANEKS NR 3

z dnia 12.09.2024 r.

do Zarządzenia nr 1/ LSIO/2009 z dnia 1 lipca 2009 r.

Na podstawie niniejszego Aneksu wprowadza się zmiany w Polityce bezpieczeństwa przetwarzania danych osobowych z uwzględnieniem wytycznych programu Fundusze Europejskie dla Dolnego Śląska 2021 - 2027:

I.
Zmianie ulega treść dokumentu „Polityka bezpieczeństwa przetwarzania danych osobowych" oraz „Rejestr Czynności Przetwarzania na podstawie art. 30 ust. 1 RODO"

II.
Aneks wchodzi w życie z dniem podpisania z mocą obowiązującą od dnia 12.09.2024 roku.

POLITYKA BEZPIECZEŃSTWA
W LEGNICKIM STOWARZYSZENIU INICJATYW OBYWATELSKICH

1 - WSTĘP

Polityka bezpieczeństwa jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Legnickie Stowarzyszenie Inicjatyw Obywatelskich w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO). Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO — rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowaną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego określenia tożsamość osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, utrwalanie, rejestrowanie, organizowanie, porządkowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, pobieranie, przeglądanie, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, dopasowywanie lub łączenie, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażające zgodę na przetwarzanie danych osobowych z nim związanych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (procesor) to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu

zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie — jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

LSIO – Legnickie Stowarzyszenie Inicjatyw Obywatelskich

1 - OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

1.1 OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć.
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
   a. nazwę zbioru (opis kategorii osób),
   b. opis celów przetwarzania,
   c. charakter, zakres, kontekst danych osobowych,
   d. odbiorcy danych,
   e. funkcjonalny opis operacji przetwarzania,
   f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing),
   g. informacja o konieczności wpisu do rejestru czynności przetwarzania,
   h. informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

1.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka). Legnickie Stowarzyszenie Inicjatyw Obywatelskich zobowiązuje się do spełnienia obowiązków prawnych wobec danych w zbiorach. Należy przede wszystkim zapewnić, że:

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas (zasada ograniczonego czasu),
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
5. opracowano klauzule informacyjne dla powyższych osób,

6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28)

1.3 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania

Definicje

1. Aktywa — środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
2. Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent).
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

2.3.1 Wyznaczenie zagrożeń

1. Legnickie Stowarzyszenie Inicjatyw Obywatelskich jest odpowiedzialne za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.

2.3.2 Wyliczenie ryzyka dla zagrożeń

1. Legnickie Stowarzyszenie Inicjatyw Obywatelskich określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Legnickie Stowarzyszenie Inicjatyw Obywatelskich określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną Skalę skutków prezentuje Tabela B.
5. Legnickie Stowarzyszenie Inicjatyw Obywatelskich wylicza Ryzyka (R) dla wszystkich zagrożeń formuły: R - P*S

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)	OPIS
zagrożenie niskie	1	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest znikoma (bliska zeru).
zagrożenie średnie	2	Wystąpienie zagrożenia jest realne, lecz nie przekracza 50% prawdopodobieństwa.
zagrożenie wysoki	3	Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje, istnieje więcej niż 50 % szans na wystąpienie.

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.3.3 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Legnickie Stowarzyszenie Inicjatyw Obywatelskich porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Proponowaną skalę ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	SKALA (WAGA)	OPIS
Niskie ryzyko	1-2	Ryzyko pomijalne i akceptowalne (akceptujemy)
Średnie ryzyko	3-6	Ryzyko jest opcjonalne (akceptujemy albo obniżamy)
Wysokie ryzyko	9	Ryzyko jest nieakceptowane (musimy obniżyć)

2.3.4 Reakcja na wartość ryzyka

1. Akceptacja ryzyka - zabezpieczenia są właściwe - brak potrzeby stosowania dodatkowych zabezpieczeń.
2. Działania obniżające ryzyko, które może stosować Legnickie Stowarzyszenie Inicjatyw Obywatelskich:

- przeniesienie - przerzucenie ryzyka (outsourcing, ubezpieczenie)
- unikanie - eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)
- redukcja - zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. szyfrowanie pendrive'ów z danymi wynoszonymi poza firmę).

2.3.5 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).

2.4 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Legnickie Stowarzyszenie Inicjatyw Obywatelskich decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.

2. Legnickie Stowarzyszenie Inicjatyw Obywatelskich zobowiązane jest do monitorowania wdrożenia zabezpieczeń

3. UPOWAŻNIENIA

1. Legnickie Stowarzyszenie Inicjatyw Obywatelskich odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej i w systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Legnickiego Stowarzyszenia Inicjatyw Obywatelskich lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie. Upoważnienia są nadawane w formie udokumentowanego zakresu obowiązków.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli,

audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia

5. Legnickie Stowarzyszenie Inicjatyw Obywatelskich prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO.

4. INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów.
   b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych.
   c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności).
   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych).
   c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu, Legnickie Stowarzyszenie Inicjatyw Obywatelskich prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
   b. inicjuje ewentualne działania dyscyplinarne
   c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
   d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Legnickie Stowarzyszenie Inicjatyw Obywatelskich dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Legnickie Stowarzyszenie Inicjatyw Obywatelskich bez zbędnej zwłoki — w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia — Legnickie Stowarzyszenie Inicjatyw Obywatelskich zgłasza je organowi nadzorczemu.
8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

5. SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Legnickie Stowarzyszenie Inicjatyw Obywatelskich.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

6. REJESTR CZYNNOŚCI PRZETWARZANIA

W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Legnickie Stowarzyszenie Inicjatyw Obywatelskich taki odpowiedni rejestr prowadzi tj. Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).

7. AUDYTY

Zgodnie z art. 32 RODO, Legnickie Stowarzyszenie Inicjatyw Obywatelskich powinno regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, przynajmniej raz na rok.

8. WYKAZ ZABEZPIECZEŃ - ŚRODKI ORGANIZACYJNE I TECHNICZNE

Legnickie Stowarzyszenie Inicjatyw Obywatelskich jest zobowiązane do stosowania środków technicznych i organizacyjnych (zabezpieczeń) adekwatnych do zagrożeń naruszenia praw i wolności osób. Legnickie Stowarzyszenie Inicjatyw Obywatelskich prowadzi uproszczony wykaz stosowanych zabezpieczeń. Wykaz powinien być aktualizowany, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka / oceny skutków.

9. AKTUALIZACJA ZGODNA Z FEDS 2021 – 2027

9.1 Podwójna odpowiedzialność za ochronę danych

Legnickie Stowarzyszenie Inicjatyw Obywatelskich oraz Instytucja Pośrednicząca, w ramach realizacji projektów FEDS 2021 - 2027, działają jako odrębni administratorzy danych. LSIO zobowiązuje się do realizacji obowiązku informacyjnego zarówno we własnym imieniu, jak i w imieniu Instytucji Pośredniczącej. Klauzula informacyjna DWUP zostaje załączona jako wzór do stosowania.

9.2 Zakres i źródła pozyskiwania danych osobowych

Legnickie Stowarzyszenie Inicjatyw Obywatelskich oraz Instytucja Pośrednicząca przetwarzają dane osobowe pozyskiwane bezpośrednio od osób, których dane dotyczą, z systemu teleinformatycznego, lub z rejestrów publicznych, o których mowa w art. 92 ust. 2 ustawy wdrożeniowej.

9.3 Podstawa prawna przetwarzania danych

Przetwarzanie danych osobowych przez Legnickie Stowarzyszenie Inicjatyw Obywatelskich jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c, a w przypadku danych szczególnej kategorii art. 9 ust. 2 lit. g RODO), który określa:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2021/1060 z 24 czerwca 2021 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu

Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+) oraz uchylające rozporządzenie (UE) nr 1296/2013 (Dz. Urz. UE L 231 z 30.06.2021, str. 21, z późn. zm.)
- ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027, w szczególności art. 87-93,
- ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego,
- ustawa z 27 sierpnia 2009 r. o finansach publicznych.

W przypadku przetwarzania danych szczególnej kategorii obowiązują przepisy art. 9 ust. 2 lit. g RODO.

9.4 Okres przechowywania danych

Dane osobowe będą przechowywane przez okres niezbędny do realizacji celów projektów FEDS, zgodnie z przepisami o archiwizacji dokumentów projektowych. Przechowywanie danych będzie również zgodne z obowiązującymi przepisami prawa krajowego oraz unijnego.

9.5 Obowiązek informacyjny

Legnickie Stowarzyszenie Inicjatyw Obywatelskich wykonuje i udokumentowywuje, również w imieniu Instytucji Pośredniczącej, obowiązek informacyjny wobec osób, których dane pozyskuje. LSIO zapewnia, że obowiązek o którym mowa w zdaniu pierwszym jest wykonywany również przez podmioty, którym powierza realizację zadań w ramach Projektu. Obowiązek informacyjny w imieniu Instytucji Pośredniczącej oraz LSIO zostaje wykonany w postaci klauzuli informacyjnej:

Załącznik Nr 1 - Klauzula informacyjna – wzór
Załącznik Nr 2 - Klauzula informacyjna DWUP – wzór
Załącznik Nr 3 – Zgoda na przetwarzanie danych osobowych - wzór

Załącznik Nr 1 - Klauzula informacyjna - wzór

Klauzula informacyjna Beneficjentów/Realizatorów projektu:

W celu wykonania obowiązku nałożonego art. 13 i 14 RODO, w związku z art. 88 ustawy o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027, informujemy o zasadach przetwarzania Państwa danych osobowych:

I. Administrator

Odrębnym administratorem Państwa danych jest:

Legnickie Stowarzyszenie Inicjatyw Obywatelskich, ul. Roosevelta 23/1, 59-220 Legnica.

II. Cel przetwarzania danych

Dane osobowe będą przetwarzane w związku z realizacją FEDS 2021-2027, w szczególności w celu monitorowania, sprawozdawczości, komunikacji, publikacji, ewaluacji, zarządzania finansowego, weryfikacji i audytów oraz do celów określania kwalifikowalności uczestników.

Podanie danych jest dobrowolne, ale konieczne do realizacji wyżej wymienionego celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

III. Podstawa przetwarzania

Państwa dane osobowe będą przetwarzane w związku z tym, że:

1. Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c, a w przypadku danych szczególnej kategorii art. 9 ust. 2 lit. g RODO), który określa:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2021/1060 z 24 czerwca 2021 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,
- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+) oraz uchylające rozporządzenie (UE) nr 1296/2013 (Dz. Urz. UE L 231 z 30.06.2021, str. 21, z późn. zm.)
- ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027, w szczególności art. 87-93,
- ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego,
- ustawa z 27 sierpnia 2009 r. o finansach publicznych.

2. Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 lit 1 ust. b RODO).

3. Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO).

IV. Zakres przetwarzanych danych.

Zakres danych, które możemy przetwarzać został określony w art. 87 ust.2 ustawy wdrożeniowej.

V. Sposób pozyskiwania danych

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, z systemu teleinformatycznego, lub z rejestrów publicznych, o których mowa w art. 92 ust. 2 ustawy wdrożeniowej.

VI. Dostęp do danych osobowych

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy administratora. Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane:

1. podmiotom, którym zleciliśmy wykonywanie zadań w FEDS 2021-2027,
2. organom Komisji Europejskiej, ministrowi właściwemu do spraw rozwoju regionalnego, ministrowi właściwemu do spraw finansów publicznych, ministrowi właściwemu do spraw zabezpieczenia społecznego, prezesowi zakładu ubezpieczeń społecznych,
3. podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.

VII. Okres przechowywania danych

Dane osobowe są przechowywane przez okres niezbędny do realizacji celów określonych w punkcie II.

VIII. Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

1. prawo dostępu do swoich danych oraz otrzymania ich kopii (art. 15 RODO),
2. prawo do sprostowania swoich danych (art. 16 RODO),
3. prawo do usunięcia swoich danych (art. 17 RODO) - jeśli nie zaistniały okoliczności, o których mowa w art. 17 ust. 3 RODO,
4. prawo do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. prawo wniesienia sprzeciwu wobec przetwarzania swoich danych (art. 21 RODO) – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e RODO – jeśli nie zaistniały okoliczności, o których mowa w art. 21 ust. 1 RODO,
6. prawo wniesienia skargi do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych (art. 77 RODO) - w przypadku, gdy osoba uzna, iż przetwarzanie jej danych osobowych narusza przepisy RODO lub inne krajowe przepisy regulujące kwestię ochrony danych osobowych, obowiązujące w Polsce.

IX. Zautomatyzowane podejmowanie decyzji

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

X. Przekazywanie danych do państwa trzeciego

Państwa dane osobowe nie będą przekazywane do państwa trzeciego.

XI. Kontakt z administratorem danych i Inspektorem Ochrony Danych

Jeśli mają Państwo pytania dotyczące przetwarzania przez Legnickie Stowarzyszenie Inicjatyw Obywatelskich danych osobowych, prosimy kontaktować się z Inspektorem Ochrony Danych (IOD) w następujący sposób:

- pocztą tradycyjną (ul. Roosevelta 23/1, 59-220 Legnica),
- elektronicznie (adres e-mail: lsio@lsio.org.pl.

Załącznik Nr 2 - Klauzula informacyjna DWUP - wzór

Klauzula informacyjna DWUP - Instytucji Pośredniczącej Funduszami Europejskimi dla Dolnego Śląska 2021-2027:

W celu wykonania obowiązku nałożonego art. 13 i 14 RODO, w związku z art. 88 ustawy o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027, informujemy o zasadach przetwarzania Państwa danych osobowych:

I. Administrator

Odrębnym administratorem Państwa danych jest:

1. Dyrektor Dolnośląskiego Wojewódzkiego Urzędu Pracy, ul. Ogrodowa 5B, 58-306 Wałbrzych.

II. Cel przetwarzania danych

Dane osobowe będą przetwarzane w związku z realizacją FEDS 2021-2027, w szczególności w celu monitorowania, sprawozdawczości, komunikacji, publikacji, ewaluacji, zarządzania finansowego, weryfikacji i audytów oraz do celów określania kwalifikowalności uczestników.

Podanie danych jest dobrowolne, ale konieczne do realizacji wyżej wymienionego celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

III. Podstawa przetwarzania

Państwa dane osobowe będą przetwarzane w związku z tym, że:

1. Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c, a w przypadku danych szczególnej kategorii art. 9 ust. 2 lit. g RODO), który określa:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2021/1060 z 24 czerwca 2021 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,
- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+) oraz uchylające rozporządzenie (UE) nr 1296/2013 (Dz. Urz. UE L 231 z 30.06.2021, str. 21, z późn. zm.)
- ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027, w szczególności art. 87-93,
- ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego,
- ustawa z 27 sierpnia 2009 r. o finansach publicznych.

2. Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 lit 1 ust. b RODO).
3. Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO).

IV. Zakres przetwarzanych danych.

Zakres danych, które możemy przetwarzać został określony w art. 87 ust.2 ustawy wdrożeniowej.

V. Sposób pozyskiwania danych

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, z systemu teleinformatycznego, lub

z rejestrów publicznych, o których mowa w art. 92 ust. 2 ustawy wdrożeniowej.

VI. Dostęp do danych osobowych

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy administratora. Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane:

1. podmiotom, którym zleciliśmy wykonywanie zadań w FEDS 2021-2027,
2. organom Komisji Europejskiej, ministrowi właściwemu do spraw rozwoju regionalnego, ministrowi właściwemu do spraw finansów publicznych, prezesowi zakładu ubezpieczeń społecznych,
3. podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.

VII. Okres przechowywania danych

Dane osobowe są przechowywane przez okres niezbędny do realizacji celów określonych w punkcie II.

VIII. Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

1. prawo dostępu do swoich danych oraz otrzymania ich kopii (art. 15 RODO),
2. prawo do sprostowania swoich danych (art. 16 RODO),
3. prawo do usunięcia swoich danych (art. 17 RODO) - jeśli nie zaistniały okoliczności, o których mowa w art. 17 ust. 3 RODO,
4. prawo do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. prawo wniesienia sprzeciwu wobec przetwarzania swoich danych (art. 21 RODO) – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e RODO – jeśli nie zaistniały okoliczności, o których mowa w art. 21 ust. 1 RODO,
6. prawo wniesienia skargi do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych (art. 77 RODO) - w przypadku, gdy osoba uzna, iż przetwarzanie jej danych osobowych narusza przepisy RODO lub inne krajowe przepisy regulujące kwestię ochrony danych osobowych, obowiązujące w Polsce.

IX. Zautomatyzowane podejmowanie decyzji

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

X. Przekazywanie danych do państwa trzeciego

Państwa dane osobowe nie będą przekazywane do państwa trzeciego.

XI. Kontakt z administratorem danych i Inspektorem Ochrony Danych

Jeśli mają Państwo pytania dotyczące przetwarzania przez Dyrektora Dolnośląskiego Wojewódzkiego Urzędu Pracy danych osobowych, prosimy kontaktować się z Inspektorem Ochrony Danych (IOD) w następujący sposób:

- pocztą tradycyjną (ul. Ogrodowa 5B, 58-306 Wałbrzych),
- elektronicznie (adres e-mail: iod@dwup.pl).

Załącznik Nr 3 – Zgoda na przetwarzanie danych osobowych - wzór

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

1. Oświadczam, iż są mi znane zawarte w niniejszym Formularzu klauzule informacyjne Instytucji Pośredniczącej - DWUP i Beneficjentów/Realizatorów Projektu: LSIO, dotyczące przetwarzania moich danych osobowych i akceptuję ich treść.

2. Oświadczam, iż dobrowolnie wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z zawartymi w niniejszym formularzu klauzulami informacyjnymi.

3. Oświadczam, iż dobrowolnie wyrażam zgodę na przekazywanie moich danych innym podmiotom (jeśli zachodzi taka potrzeba) w związku z realizacją celów określonych w ww. klauzulach informacyjnych.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

obowiązująca w Legnickim Stowarzyszeniu Inicjatyw Obywatelskich
z siedzibą w Legnicy przy ul. Roosevelta 23/1, 59-220 Legnica NIP: 6912309196
- wersja obowiązująca od dnia 01 września 2021 roku

I. POSTANOWIENIA OGÓLNE

1. Niniejszym wprowadza się niniejszą Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
2. Jeśli w niniejszej Instrukcję Zarządzania Systemem Informatycznym mowa o:
   a) **Administratorze Danych Osobowych (ADO) -** rozumie się przez to podmiot decydujący o celach i środkach przetwarzania danych osobowych;
   b) **Administratorze Systemów Informatycznych (ASI) -** rozumie się przez to osobę fizyczną nadzorującą bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych;
   c) **Haśle -** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
   d) **Identyfikatorze użytkownika -** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   e) **Instrukcji -** rozumie się przez niniejszą instrukcję zarządzania systemem informatycznym;
   f) **Odbiorcy danych -** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego prowadzonego przez nie postępowania;
   g) **Procesorze -** rozumie się przez to Organizację działającego jako podmiot, któremu właściwy ADO powierzył w drodze umowy przetwarzanie danych osobowych;
   h) **Organizacji -** rozumie się przez to Legnickie Stowarzyszenie Inicjatyw Obywatelskich z siedzibą w Legnicy przy ul. Roosevelta 23/1, 59-220 Legnica, NIP: 6912309196, który pełni rolę Administratora Danych Osobowych lub Procesora
   i) **Przetwarzaniu danych -** rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   j) **Systemie informatycznym -** rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   k) **Usuwaniu danych -** rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
   l) **Uwierzytelnianiu -** rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
   m) **Użytkowniku -** rozumie się przez to osobę, która posiada upoważnienie do przetwarzania danych osobowych i posiada uprawnienia do uwierzytelnionego dostępu do systemu informatycznego;

n) **Zbiorze danych -** rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

3. Organizacja wdraża niniejszą Instrukcję w celu zadośćuczynienia obowiązującym przepisom prawa i zapewnieniu ochrony danych osobowych, które przetwarza jako ADO lub Procesor.

4. Instrukcja odnosi się do danych osobowych przetwarzanych przez Organizację w systemach informatycznych w zakresie jego uprawnień i obowiązków wynikających z łączących go z poszczególnymi ADO umów o powierzenie przetwarzania danych osobowych; część z obowiązków wynikających z powszechnie obowiązujących przepisów może leżeć po stronie tych ADO jako głównych' administratorów danych osobowych znajdujących się w danym systemie informatycznym, natomiast Organizacja jako Procesor wdraża stosowne procedury i zabezpieczenia w odniesieniu do wykonywanego wyłącznie przez niego przetwarzania danych osobowych.

5. Organizacja zapewnia, że systemy informatyczne zachowują możliwość:

a) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

b) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

6. W toku przetwarzania przez siebie danych osobowych w systemie informatycznym Organizacja nie stosuje profilowania.

7. Organizacja zapewnia, że systemy informatyczne są regularne testowane, a skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania mierzona i oceniana.

8. Niezależnie od niniejszej Instrukcji Organizacja wdrożył Politykę Bezpieczeństwa.

II. PROCEDURY NADAWANIA, MODYFIKOWANIA I USUWANIA UPRAWNIEŃ ORAZ UWIERZYTELNIENIA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Organizacja samodzielnie pełni funkcję ASI.

2. Za nadawanie, modyfikowanie i usuwanie uprawnień Użytkownika do przetwarzania danych osobowych w systemach informatycznych, a także za rejestrowanie takich uprawnień w tymże systemie, odpowiedzialny jest ASI.

3. Uprawnienia dla nowego Użytkownika mogą być nadane wyłącznie osobie upoważnionej do przetwarzana danych osobowych zgodnie z Polityką Bezpieczeństwa.

4. Każdemu Użytkownikowi ASI przyznaje unikalny identyfikator oraz hasło.

5. Identyfikator Użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

ó. Użytkownik uwierzytelnia dostęp do systemu informatycznego poprzez wpisanie swojego unikalnego identyfikatora oraz hasła. Zmiana hasła następuje nie rzadziej niż co 30 dni.

7. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

8. Użytkownik ma obowiązek zachować hasło w tajemnicy w czasie jego obowiązywania oraz po ustaniu jego ważności.

9. Użytkownik systemu informatycznego zobowiązany jest niezwłocznie poinformować Organizację i ADO o stwierdzeniu naruszenia zabezpieczeń danych osobowych w systemie informatycznym.

10. ASI może zablokować Użytkownikowi dostęp do systemu informatycznego w każdym czasie, jeśli uzna to za konieczne dla zapewnienia bezpieczeństwa danych osobowych.

11. Po zakończeniu pracy w systemie informatycznym, Użytkownik zobowiązany jest wylogować się z systemu.

12. Identyfikatory i hasła Użytkowników przechowuje się w systemie informatycznym w postaci zaszyfrowanej.
13. Użytkownik, który utracił hasło, zobowiązany jest zgłosić to niezwłocznie ASI, który ustali nowe hasło.
14. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej (nie zapisywać go).

III. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. W celu uruchomienia podsystemu informatycznego Użytkownik powinien:
   a) uruchomić komputer;
   b) wybrać odpowiednią opcję umożliwiającą logowanie do systemu;
   c) zalogować się do systemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.
2. Za każdym razem, kiedy Użytkownik opuszcza stanowisko pracy, zobowiązany jest do wylogowania się z systemu.
3. Użytkownik jest zobowiązany do zapisywania i zamykania wszystkich dokumentów zawierających dane osobowe przed odejściem od komputera.
4. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.

IV. PROCEDURY TWORZENIA KOPII ZAPASOWYCH

1. Kopie zapasowe zbiorów danych osobowych tworzone mogą być tworzone na zewnętrznych nośnikach informatycznych (przenośne dyski, pendrive).
2. Kopie zapasowe są wykonywane za pomocą oprogramowania Organizacji.
3. Za tworzenie kopii zapasowych odpowiedzialny jest ASI lub wyznaczona przez niego osoba posiadająca upoważnienie do przetwarzania danych osobowych.

V. PROCEDURY PRZECHOWYWANIA NOŚNIKÓW DANYCH I KOPIE ZAPASOWE

1. Kopie zapasowe oraz nośniki systemów informatycznych nie mogą być zbywane ani przekazywane podmiotom nieuprawnionym.
2. Kopie zapasowe systemów informatycznych przechowywane na zewnętrznych nośnikach informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach lub szufladach Organizacji.
3. Kopie zapasowe systemów informatycznych, po ustaniu ich przydatności, są usuwane w sposób wykluczający ich odtworzenie.

VI. ZABEZPIECZENIE SYSTEMÓW INFORMATYCZNYCH

1. Organizacja stosuje w systemie informatycznym jak najbezpieczniejsze dostępne systemy operacyjne.
2. Systemy informatyczne są zabezpieczone przed atakami z zewnątrz za pomocą oprogramowania typu firewall.
3. Systemy informatyczne są zabezpieczone przed szkodliwym oprogramowaniem za pomocą aktualnego oprogramowania antywirusowego.
4. Użytkownicy nie mogą używać prywatnego sprzętu przenośnego, takiego jak płyt CD i DVD, pamięci masowych USB na komputerach, przy użyciu których, przetwarza się dane osobowe. Dotyczy to również podłączania do komputera telefonów komórkowych.
5. Użytkownicy, w przypadku korzystania przy przetwarzaniu danych osobowych z komputerów przenośnych, mają obowiązek zapewnić przechowywać i użytkować komputer przenośny w sposób

wykluczający jego uszkodzenie skutkujące usunięciem lub uszkodzeniem danych osobowych oraz przed dostępem osób trzecich.

6. W celu przeciwdziałania atakom zainfekowanych plików, system musi być skanowany przynajmniej raz dziennie pod kątem obecności w systemie wirusów i innych zagrożeń.
7. W przypadku wykrycia jakiegokolwiek zagrożenia Użytkownik niezwłocznie zawiadamia ASI.
8. W przypadku stwierdzenia braku zasilania należy zapisać dane osobowe oraz wylogować się.
9. Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem.
10. Monitory komputerów należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych, w szczególności nie mogą one być zwrócone w stronę okien i drzwi.
11. Użytkownik systemu zobowiązany jest do prawidłowej eksploatacji powierzonego sprzętu i oprogramowania oraz ochrony zasobów informatycznych przed dostępem osób nieupoważnionych, w tym zabezpieczenia komputerowych stanowisk dostępu do danych osobowych przed wglądem osób nieupoważnionych, zabezpieczenia danych przed ich zmianą.

VII. INFORMACJE INFORMATYCZNE ODNOTOWANE PRZEZ SYSTEM

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - System informatyczny zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu;
   b) identyfikatora Użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   d) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, oraz dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   e) wniesienia przez osobę, której dane są przetwarzane, sprzeciwu w przypadkach przewidzianych w stosownych przepisach.
2. Odnotowanie informacji, o których mowa w rozdziale VII ust. 1 pkt 1 i 2 niniejszej Instrukcji, następuje automatycznie po zatwierdzeniu przez Użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w rozdziale VII ust. 1 niniejszej Instrukcji.
4. W przypadku przetwarzania danych osobowych w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w rozdziale VII ust. 1 pkt 4 niniejszej Instrukcji, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

VIII. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW INFORMATYCZNYCH

1. Przynajmniej raz w roku wykonuje się przegląd Systemu informatycznego.
2. Konserwacji poszczególnych elementów Systemu informatycznego dokonuje się tak często, jak to wynika z ich specyfiki - nie rzadziej niż raz w roku.
3. Przeglądy i konserwacje ewidencjonuje się w Załączniku nr 1 do niniejszej Instrukcji.
4. W przypadku awarii systemu informatycznego lub nośników informacji naprawia się je lub odzyskuje dane z zachowaniem tajemnicy danych osobowych zgodnie z Polityką Bezpieczeństwa.

5. Gdy niemożliwa jest naprawa Systemu informatycznego, jego elementu lub nośnika danych, w celu przywrócenia sprawności działania systemu należy zastąpić go nowym oraz posłużyć się kopią zapasową.
6. W przypadku przekazania innym podmiotom elementów Systemu informatycznego lub nośnika danych w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte albo należy zabezpieczyć umieszczone na nim dane osobowe przed dostępem podmiotów trzecich.

IX. POSTANOWIENIA KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązków lub naruszenia innych zasad wynikających z niniejszej Instrukcji mogą stanowić podstawę do pociągnięcia danej osoby do odpowiedzialności, adekwatnie do łączącego ją z Organizacją stosunku prawnego.
2. W sprawach nieuregulowanych niniejszą Instrukcję oraz Polityką Bezpieczeństwa mają zastosowanie stosowne przepisy.

Legnickie Stowarzyszenie
Inicjatyw Obywatelskich

WYKAZ ZABEZPIECZEŃ - ŚRODKI ORGANIZACYJNE I TECHNICZNE

Środki organizacyjne

1. Opracowano i wdrożono politykę bezpieczeństwa.
2. Opracowano i wdrożono instrukcję zarządzania systemem informatycznym.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
4. Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy.
6. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
7. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
8. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności pracownika Legnickiego Stowarzyszenia Inicjatyw Obywatelskich upoważnionego do przetwarzania tych danych oraz w warunkach zapewniających bezpieczeństwo danych.

Środki ochrony fizycznej danych

1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2. Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej niemetalowej szafie.
3. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
4. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy.
5. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.
2. Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
5. Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
6. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

7. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych

1. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
6. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Legnickie Stowarzyszenie
Inicjatyw Obywatelskich

REJESTR CZYNNOŚCI PRZETWARZANIA NA PODSTAWIE ART. 30, UST 1 RODO

1. Administrator:

1) Legnickie Stowarzyszenie Inicjatyw Obywatelskich
uL Roosevelta 23/1,59-220 Legnica - lsio@lsio.org.pl

2) Dyrektor Dolnośląskiego Wojewódzkiego Urzędu Pracy, ul. Ogrodowa 5B, 58-306 Wałbrzych

2. Dane kontaktowe inspektora ochrony danych (jeśli jest powołany):

1) Dla Legnickiego Stowarzyszenia Inicjatyw Obywatelskich - Nie dotyczy
2) Dla DWUP - Dyrektor Dolnośląskiego Wojewódzkiego Urzędu Pracy, ul. Ogrodowa 5B, 58-306 Wałbrzych - iod@dwup.pl

W załączeniu tabela z rejestrem czynności przetwarzania