|  |
| --- |
| UWAGA!Jednym z obowiązków administratora danych (np. stowarzyszenia, fundacji) jest przygotowanie i wdrożenie tzw. polityki bezpieczeństwa. Powinna ona być stworzona zawsze, jeżeli przetwarzamy jakieś dane, nie ma więc znaczenia, czy podlegają one rejestracji w GIODO.Załączony wzór polityki bezpieczeństwa jest wariantem rozszerzonym, który każda organizacja może modyfikować, dostosowując go do swoich potrzeb. **Pamiętać należy, że polityka bezpieczeństwa:*** powinna być aktualizowana – ponieważ organizacje rozwijają się, poszerzają zakres swoich działań i ich regulacje wewnętrzne powinny za tym nadążać,
* jest to dokument wewnętrzny, wprowadzany do stosowania w organizacji uchwałą zarządu – po odpowiednim dostosowaniu załączonego wzoru do potrzeb danej organizacji należy przygotować stronę tytułową, która może dodatkowo zawierać informacje o dacie opracowania dokumentu oraz początku jego obowiązywania.

**Odpowiedzialność zarządu**Przyjęcie polityki powinno wynikać z uchwały zarządu organizacji. W załączonym wzorze polityki bezpieczeństwa jest o tym mowa w dwóch miejscach:* definicje w pkt 6 (w którym jest mowa o Administratorze Bezpieczeństwa Informacji) – trzeba tam wpisać datę podjęcia uchwały zarządu wprowadzającej politykę bezpieczeństwa oraz numer tej uchwały,
* rozdział 9 Postanowienia końcowe pkt 8 – polityka bezpieczeństwa wchodzi w życie z dniem podjęcia uchwały zarządu organizacji lub w terminie określonym w treści tej uchwały (czyli zaczyna obowiązywać od momentu podjęcia uchwały albo organizacja daje sobie trochę czasu na zapoznanie się z nią wszystkich zainteresowanych osób i w treści uchwały określa początek terminu obowiązywania polityki).

 Oprócz polityki bezpieczeństwa organizacja powinna także stworzyć instrukcję zarządzania systemem informatycznym, jeśli przetwarza dane osobowe w ten sposób. Instrukcja zawiera na przykład takie informacje: procedury tworzenia kopii zapasowych zbiorów danych, sposób i miejsce przechowywania tych kopii, a także wszelkich innych elektronicznych nośników informacji, procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji.**Podstawa prawna**Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), rozdział 5: Zabezpieczenie danych osobowych 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) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536)Wzór dokumentu pochodzi ze strony <http://poradnik.ngo.pl/x/468747> i został opracowany w projekcie „Internetowe centrum wsparcia” przez p. Agnieszkę Majdzińską. |

**SPIS TREŚCI**

|  |
| --- |
| **Część I** |
| **Dokumentacja sposobu przetwarzania danych osobowych** |  |
|  |  |
| **Definicje** |  |  |
| **Wprowadzenie** |  |  |
| **Przepisy ogólne** |  |  |
| **Rozdział 1** | Polityka bezpieczeństwa w zakresie ochrony danych osobowych w ......... (pełna nazwa organizacji[[1]](#footnote-2)) |  |
|  | a) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe |  |
|  | b) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych |  |
|  | c) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi |  |
|  | d) sposób przepływu danych pomiędzy systemami |  |
|  | e) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych |  |
|  | f) pozostałe informacje |  |
| **Rozdział 2** | Przetwarzanie danych osobowych w projekcie/zadaniu, w którym ....... (pełna nazwa organizacji) jest partnerem  |  |
| **Rozdział 3** | Powierzenie przez ……. (pełna nazwa organizacji) podmiotowi zewnętrznemu przetwarzania danych osobowych w ramach realizacji zadań z zakresu monitoringu i ewaluacji projektu/zadania |  |
| **Rozdział 4** | Pozostałe przypadki przetwarzania danych osobowych w ....... (pełna nazwa organizacji) |  |
| **Rozdział 5** | Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 (PEFS 2007)

|  |
| --- |
| Więcej informacji na stronie internetowej [http://pokl.mazowia.eu/formularz-pefs-2007/](http://pokl.mazowia.eu/formularz-pefs-2007/formularz-pefs-2007.html) |

 |  |
|  | a) postanowienia ogólne |  |
|  | b) zakres oraz zasady zabezpieczania danych osobowych |  |
|  | c) obowiązki Administratora Bezpieczeństwa Informacji PEFS 2007 |  |
|  | d) przetwarzanie danych osobowych |  |
|  | e) postępowanie w przypadku naruszenia ochrony danych osobowych |  |
|  | f) kontrola nad przestrzeganiem ochrony danych osobowych |  |
|  | g) postanowienia końcowe |  |
| **Rozdział 6** | Opis zdarzeń naruszających ochronę danych osobowych |  |
| **Rozdział 7** | Zabezpieczenie danych osobowych |  |
| **Rozdział 8** | Postępowanie w przypadku naruszenia ochrony danych osobowych |  |
| **Rozdział 9** | Postanowienia końcowe |  |
| **Rozdział 10** | Arkusz zmian |  |
|  |  |  |
| **Część II** |  |  |
| **Instrukcja w sprawie zasad postępowania przy przetwarzaniu danych osobowych** |  |
|  |  |  |
| **Część III** |  |  |
| **Instrukcja dla osób upoważnionych do przetwarzania danych osobowych** |  |
|  |  |  |
| **Część IV** |  |  |
| Załączniki |  |  |
| 1 „A” | Oświadczenie o zapoznaniu się z treścią „Polityki bezpieczeństwa” |  |
| 1 „B” | Lista osób, które zapoznały się z „Polityką bezpieczeństwa” |  |
| 2 „A” | Upoważnienie do przetwarzania danych osobowych dla ABI |  |
| 2 „B” | Upoważnienie dla ABI do reprezentowania AD i udzielania/odwoływania upoważnienia |  |
| 3 | Upoważnienie do przetwarzania danych osobowych |  |
| 4 | Ewidencja osób upoważnionych do przetwarzania danych osobowych |  |
| 5 „A” | Odwołanie upoważnienia ABI do przetwarzania danych osobowych |  |
| 5 „B” | Odwołanie upoważnienia ABI do reprezentowania AD i udzielania/odwoływania upoważnienia |  |
| 6 | Odwołanie upoważnienia do przetwarzania danych osobowych |  |
| 7 | Rejestr zbiorów danych osobowych przetwarzanych w …….. (pełna nazwa organizacji) |  |
| 8 | Informacja o planowanym utworzeniu nowego zbioru danych osobowych |  |
| 9 | Raport z naruszenia ochrony danych osobowych |  |
| 10 | Analiza naruszenia ochrony danych osobowych |  |
| 11 | Protokół z naruszenia poufności nośnika danych |  |
| 12 „A” | Protokół przekazania |  |
| 12 „B” | Zestawienie przekazywanych danych osobowych |  |

**CZĘŚĆ I**

**Dokumentacja sposobu przetwarzania danych osobowych**

## **Definicje**

Ilekroć w niniejszym dokumencie jest mowa o:

1) „**Polityce bezpieczeństwa**”,„**dokumencie**” – należy przez to rozumieć „Politykę bezpieczeństwa w zakresie ochrony danych osobowych w ... (pełna nazwa organizacji)”.

2) ... (skrócona nazwa organizacji) – należy przez to rozumieć ... (pełna nazwa organizacji).

3) **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3a) **Osobie możliwej do zidentyfikowania** – należy przez to rozumieć osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

4) **Zbiorze danych** – należy przez to rozumieć każdy posiadający strukturę zestaw danych
o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

5) **Administratorze Danych** („**AD**”) – należy przez to rozumieć Zarząd ............ (pełna nazwa organizacji).

6) **Administratorze Bezpieczeństwa Informacji** („**ABI**”) – należy przez to rozumieć osobę wyznaczoną przez Zarząd ... (pełna nazwa organizacji) do nadzorowania przestrzegania zasad ochrony określonych Uchwałą Nr .............. Zarządu .............. (pełna nazwa organizacji) z dnia ................. w sprawie ustalenia polityki bezpieczeństwa w zakresie ochrony danych osobowych w ... (pełna nazwa organizacji) oraz wymagań w zakresie ochrony wynikających
z powszechnie obowiązujących przepisów o ochronie danych osobowych.

7) **Osobie upoważnionej** – należy przez to rozumieć: pracownika, współpracownika, wolontariusza, praktykanta, stażystę ....... (pełna nazwa organizacji) posiadającego pisemne upoważnienie do przetwarzania danych osobowych nadane przez AD lub ABI w imieniu AD.

8) **Przetwarzaniu danych** – należy przez to rozumieć 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.

8a) **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

8b) **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

9) **Usuwaniu danych** – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

10) **Zgodzie osoby, której dane dotyczą** – należy przez to rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli innej treści.

11) **Odbiorcy danych** – należy przez to rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. z 1997 r. Nr 133, poz. 883; tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926),

d) podmiotu, o którym mowa w art. 31 ww. Ustawy,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

12) „**Instrukcji...**” – należy przez to rozumieć „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w ....... (pełna nazwa organizacji)”.

## **Wprowadzenie**

Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych zawartych w systemach informatycznych w ….... (pełna nazwa organizacji)
– zwanej dalej …... (nazwa skrócona organizacji).

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę ....... (nazwa skrócona organizacji).

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa w zakresie ochrony danych osobowych
w ........ (pełna nazwa organizacji)” – zwany dalej: „Polityką bezpieczeństwa”, „Dokumentem”, wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych w ….... (nazwa skrócona organizacji).

Potrzeba opracowania „Polityki bezpieczeństwa” wynika z przepisów § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych
i organizacyjnych, jakim powinny odpowiadać urządzenia służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

**Przepisy ogólne**

1. „Polityka bezpieczeństwa” określa tryb postępowania w przypadku, gdy:

1) stan urządzenia, zawartość rejestru danego zbioru danych osobowych, ujawnione metody pracy mogą wskazywać na naruszenie zabezpieczeń tych danych;

2) stwierdzono naruszenie bezpieczeństwa przetwarzanych danych w rejestrze danego zbioru danych.

2. „Polityka bezpieczeństwa” obowiązuje wszystkie osoby pracujące przy przetwarzaniu danych osobowych w ….. (nazwa skrócona organizacji).

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę
i udokumentowanie przypadków naruszenia bezpieczeństwa w danym rejestrze zbioru danych …... (nazwa skrócona organizacji).

4.1.1 Administrator Danych, którym jest Zarząd[[2]](#footnote-3) ....... (pełna nazwa organizacji), swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji zawartych w rejestrach zbiorów danych ….. (nazwa skrócona organizacji), którym jest[[3]](#footnote-4) ........

4.1.2 Administrator Danych może dodatkowo powierzyć Administratorowi Bezpieczeństwa Informacji wykonywanie funkcji Administratora Bezpieczeństwa Informacji PEFS 2007[[4]](#footnote-5).

4.1.3 Do Administratora Bezpieczeństwa Informacji PEFS 2007 mają zastosowanie wszystkie uregulowania dotyczące Administratora Bezpieczeństwa Informacji.

4.2 Administrator Danych upoważnia Administratora Bezpieczeństwa Informacji do przetwarzania wszystkich zbiorów danych osobowych zaewidencjonowanych w „Rejestrze zbiorów danych osobowych przetwarzanych w ..... (pełna nazwaorganizacji)”.

4.3 Upoważnienie, o którym mowa w pkt. 4.2 ma formę pisemną (załącznik nr 2 „A” do „Polityki bezpieczeństwa”).

4.4. Administrator Danych może w każdym czasie odwołać upoważnienie do przetwarzania danych osobowych udzielone Administratorowi Bezpieczeństwa Informacji.

4.5 Odwołanie upoważnienia, o którym mowa w pkt. 4.4 ma formę pisemną (załącznik nr 5 „A” do „Polityki bezpieczeństwa”).

4.6 Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji do:

a) udzielania upoważnień do przetwarzania danych osobowych:

* osobom wchodzącym w skład organów organizacji.
* pracownikom[[5]](#footnote-6),
* współpracownikom[[6]](#footnote-7),
* wolontariuszom, praktykantom i stażystom,
* pracownikom lub współpracownikom ... (pełna nazwa organizacji) w związku
z realizacją projektu/zadania, w którym ... (skrócona nazwa organizacji) jest lub może być partnerem[[7]](#footnote-8) [niezależnie od tego, czy lider projektu/zadania (realizator) udzielił takiego upoważnienia, czy też nie],
* pracownikom lub współpracownikom instytucji, którym ... (pełna nazwa organizacji) powierzy – na mocy stosownej pisemnej umowy – prowadzenie zadań z zakresu monitoringu i ewaluacji projektu/zadania, którego ...... (skrócona nazwa organizacji) jest realizatorem[[8]](#footnote-9),
* pracownikom ..... (pełna nazwa organizacji) w związku z pozostałymi przypadkami przetwarzania danych osobowych[[9]](#footnote-10) w .... (skrócona nazwa organizacji),

b) nadawania upoważnienia dla Administratora Systemu Informatycznego[[10]](#footnote-11),

c) odwoływania upoważnienia dla Administratora Systemu Informatycznego[[11]](#footnote-12).

4.7 Upoważnienia o których mowa w pkt. 4.6 mają formę pisemną[[12]](#footnote-13) [odpowiednio załącznik nr 3 do „Polityki bezpieczeństwa” oraz załączniki nr ... i nr .... do „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w ……. (pełna nazwa organizacji)”].

4.8 Administrator Bezpieczeństwa Informacji może w każdym czasie odwołać upoważnienie do przetwarzania danych osobowych udzielone osobom wymienionym w pkt. 4.6 „a”.

4.9 Odwołanie upoważnień, o których mowa w pkt. 4.8 ma formę pisemną (załącznik nr 6 do „Polityki bezpieczeństwa”).

4.10 Administrator Danych wyznacza Administratora Bezpieczeństwa Informacji do reprezentowania Administratora Danych.

4.11 Do wykonywania czynności określonych w pkt. 4.2, 4.6, 4.8 i 4.10 Administrator Danych wyda Administratorowi Bezpieczeństwa Informacji stosowne upoważnienia.

4.12 Upoważnienia, o których mowa w pkt. 4.11 mają formę pisemną (załącznik nr 2 „A”
i załącznik nr 2 „B” do „Polityki bezpieczeństwa”).

4.13 Odwołanie upoważnień, o których mowa w pkt. 4.12 może nastąpić w każdym czasie.

4.14 Odwołanie upoważnień, o których mowa w pkt. 4.12 ma formę pisemną (załącznik nr 5 „A” i załącznik nr 5 „B” do „Polityki bezpieczeństwa”).

5. Administrator Bezpieczeństwa Informacji wykonuje czynności określone w pkt. 4.2, 4.6, 4.8 i 4.10 oraz realizuje zadania w zakresie ochrony danych osobowych, a w szczególności
w zakresie:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach danych ... (pełna nazwa organizacji);

2) sprawowania kontroli nad wprowadzaniem i udostępnianiem danych osobowych;

3) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa”
w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym[[13]](#footnote-14) lub każdym innym;

4) niezwłocznego informowania Administratora Danych o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych;

5) nadzoru i kontroli – wraz z Administratorem Systemu Informatycznego (ASI) – systemów informatycznych[[14]](#footnote-15) służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

6. Osobę upoważnioną do zastępowania Administratora Bezpieczeństwa Informacji wyznacza Administrator Bezpieczeństwa Informacji (ABI).

7. Osoba zastępująca ABI powyższe zadania realizuje w przypadku nieobecności ABI.

8. Osoba zastępująca składa ABI relację z działań podejmowanych w czasie swojego zastępstwa.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U.
z 1997 r. Nr 133, poz. 883; tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).

2. Rozporządzeniem 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 służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

3. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji[[15]](#footnote-16) z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536).

**Rozdział 1**

**Polityka bezpieczeństwa w zakresie ochrony danych osobowych
w ...... (pełna nazwa organizacji)**

a) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar,
w którym przetwarzane są dane osobowe[[16]](#footnote-17):

…... (pełna nazwa organizacji) zajmuje się ... (opisać krótko, czym organizacja się zajmuje).

Siedziba organizacji znajduje się przy ul. ... w ... (nazwa miejscowości) w ... (budynku wolnostojącym, bloku mieszkalnym, siedzibie urzędu, instytucji, innej organizacji, zakładu pracy … – kto jest właścicielem, czy są jakieś kondygnacje, jaką część zajmuje organizacja).

Do lokalu/ siedziby ... (skrócona nazwa organizacji) prowadzą drzwi ... – opisać, jakie drzwi, ile i jakich jest w nich zamków, czy wewnątrz siedziby organizacji znajdują się jakieś pomieszczenia (jeśli TAK – to jakie drzwi do nich prowadzą, ile jest w nich zamków, czy są na nie zakładane plomby).

Wypisać nazwy tych pomieszczeń (jeśli są takie – np. SEKRETARIAT, KADRY, ZARZĄD...) wskazując ich lokalizację w siedzibie organizacji z zaznaczeniem, w których
z nich przetwarzane są dane osobowe.

Napisać:

* czy pomieszczenia, w których przetwarzane są dane osobowe, wyposażone są
w szafy (drewniane, metalowe) do przechowywania dokumentacji, a jeśli TAK – to jakie mają zabezpieczenia (zamki, kłódki, blokady, szyfry, ...),
* kto (nazwy stanowisk lub funkcji pełnionych w organizacji), kiedy, w jakich godzinach ma dostęp do pomieszczeń – czy tylko pracownicy organizacji czy może np. osoby z zewnętrznych firm sprzątających
* kto (nazwy stanowisk lub funkcji pełnionych w organizacji) ma dostęp do kluczy do siedziby organizacji,
* czy siedziba organizacji jest podłączona do monitoringu.

b) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych:

W ……. (pełna nazwa organizacji) przetwarza się dane osobowe[[17]](#footnote-18):

1) ……………………………………….. (wymienić po kolei od „1” do „n”)

Napisać, czy dane w powyższych zbiorach mają formę papierową i/lub elektroniczną,
i czy przetwarzane są w organizacji w formie papierowej lub papierowej i elektronicznej oraz czy są przetwarzane w zasobach systemu informatycznego (jeśli TAK – to wymienić nazwy tych programów).

Następnie przedstawić zakres danych osobowych przetwarzanych w ramach każdego ze zbiorów danych osobowych – np.:

Dane osobowe darczyńców organizacji przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

* imiona i nazwiska,
* pełny adres lub oznaczenie samej tylko miejscowości,
* serię i numer dowodu osobistego,
* numer ewidencyjny PESEL i/lub NIP,
* numer telefonu stacjonarnego i/lub komórkowego i/lub adres poczty elektronicznej,
* datę wpływu/przekazania darowizny,
* przedmiot darowizny (pieniężna i/lub rzeczowa),
* nazwę banku i numer rachunku bankowego (w przypadku darowizny pieniężnej).

Dane osobowe wolontariuszy, praktykantów i stażystów współpracujących z organizacją przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

* imiona i nazwiska,
* adres zamieszkania (miejscowość wraz z kodem pocztowym, ulica, numer domu, numer mieszkania),
* serię i numer dowodu osobistego, numer ewidencyjny PESEL i/lub NIP,
* ramy graniczne obowiązywania porozumienia o wolontariacie, porozumienia lub umowy o odbycie praktyk lub stażu, porozumienia o wykonanie prac społecznie użytecznych,

oraz:

* dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej).

Do zasobów systemu informatycznego służącego do przetwarzania danych osobowych zalicza się[[18]](#footnote-19):

* System „PŁATNIK” – w którym przetwarzane są zbiory danych osobowych osób zatrudnionych w organizacji na podstawie umów o pracę oraz osób współpracujących
z organizacją w oparciu o umowy zlecenia.
* System informatyczny pod nazwą „SODiR – System Obsługi Dofinansowań
i Refundacji” (będący aplikacją Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych) – w którym przetwarzane są dane osobowe służące rozliczaniu dofinansowań do wynagrodzeń zatrudnionych pracowników niepełnosprawnych.
* „Formularz PEFS 2007” – w którym przetwarzane będą zbiory danych osobowych uczestników projektów realizowanych przez organizację (obowiązek ten nakłada na Organizację sprawozdawczość projektów współfinansowanych ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, realizowanych
w ramach Programu Operacyjnego Kapitał Ludzki.
* Ewentualnie inne programy branżowe – jeśli występują (np. systemy księgowo-kadrowo-płacowe).

Ponadto:

* można napisać, czy organizacja tworzy własne bazy danych (np. w programie WORD, EXCEL lub w programach Open Office) i jakich zbiorów danych osobowych to dotyczy.

Uzupełnieniem powyższych informacji może być rejestr zbiorów danych osobowych przetwarzanych w organizacji.

c) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi:

Wypisać w kolejności:

* nazwę zbioru danych osobowych,
* formę prowadzenia dokumentacji zbioru danych (papierowa, elektroniczna lub papierowo-elektroniczna),
* zakres przetwarzanych danych osobowych (np.: dane wprowadzane do programu „Płatnik”, „SODiR”, „PEFS 2007”, ale także dane pozyskiwane np. przed zatrudnieniem pracownika/współpracownika z formularzy takich jak: kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie, dane do umowy, kwestionariusz osobowy dla pracownika, informacja dla celów podatkowych, informacje dodatkowe do celów ubezpieczeń społecznych, oświadczenie dotyczące przekazywania wynagrodzenia na rachunek bankowy).

Np. w systemie „Płatnik” przetwarzane są w formie elektronicznej dane osobowe pracowników oraz osób współpracujących z organizacją na podstawie umów zleceń obejmujące:

* imiona i nazwiska,
* adres zameldowania, zamieszkania i do korespondencji,
* datę urodzenia,
* numer ewidencyjny PESEL i NIP,
* zwolnienia lekarskie,

oraz dane dotyczące:

* wysokości wynagrodzenia,
* posiadanych dzieci,
* współmałżonka/współmałżonki.

W ramach systemu „SODiR – System Obsługi Dofinansowań i Refundacji” przetwarzane są w formie elektronicznej dane osobowe służące rozliczaniu dofinansowań do wynagrodzeń zatrudnionych w organizacji pracowników niepełnosprawnych obejmujące:

* imiona i nazwiska,
* adres zamieszkania.
* numer ewidencyjny PESEL i NIP,
* serię i numer dowodu osobistego,
* stopień niepełnosprawności,
* koszty ubruttowione,
* miesiąc rozliczenia.

Można też w tym miejscu uwzględnić przetwarzanie danych osobowych w formie elektronicznej do celów realizacji przelewów bankowych i międzybankowych (np. z tytułu wynagrodzenia za pracę) obejmujących:

* imię i nazwisko,
* adres zamieszkania.

d) sposób przepływu danych pomiędzy systemami:

Wskazać, czy organizacja posiada bądź nie posiada własnego systemu informatycznego służącego do przetwarzania danych osobowych. Jeśli dane osobowe przetwarzane są przy użyciu edytora tekstu (MS Word), arkusza kalkulacyjnego (MS Excel) lub programów równorzędnych (np. pakiet Open Office) i innych dostępnych programów do tworzenia baz danych – trzeba o tym wspomnieć.

W zakresie zewnętrznych (obcych) systemów informatycznych użytkowanych przez Organizację do przetwarzania danych osobowych wymienić należy:

* System „Płatnik” – będący aplikacją Zakładu Ubezpieczeń Społecznych przeznaczoną dla płatników składek i zapewniającą pełną obsługę dokumentów ubezpieczeniowych i wymianę informacji z ZUS.
* System informatyczny „SODiR – System Obsługi Dofinansowań i Refundacji”
– będący aplikacją Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych,
w której przetwarzane są dane osobowe służące rozliczaniu dofinansowań do wynagrodzeń zatrudnionych pracowników niepełnosprawnych.
* „Formularz PEFS 2007” – w którym przetwarzane są zbiory danych osobowych uczestników projektów realizowanych przez organizację w ramach Programu Operacyjnego Kapitał Ludzki.
* Ewentualnie systemy księgowo-kadrowo-płacowe.

Wskazać, czy wszystkie wyżej wymienione systemy informatyczne są systemami odrębnymi
i nie współpracują ze sobą, czy przepływ danych pomiędzy tymi systemami występuje.

Przepływ danych może się pojawić np. w przypadku systemów księgowo-kadrowo-płacowych – jeśli takie są w organizacji wykorzystywane, to trzeba opisać, jak ten przepływ wygląda.

Podmioty, do których przekazywane są dane to:

1. Zakład Ubezpieczeń Społecznych,
2. Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych,
3. Ministerstwo Rozwoju Regionalnego z siedzibą w Warszawie (za pośrednictwem np. właściwego Urzędu Marszałkowskiego lub Wojewódzkiego Urzędu Pracy) – dot. PO KL,
4. Ministerstwo Pracy i Polityki Społecznej z siedzibą w Warszawie – dot. PO FIO,
5. pozostali grantodawcy nie wymienieni w pkt „c” i „d”.

Wskazać, czy podmiotom wymienionym w punktach „a” i „b” dane przesyłane są teletransmisyjnie za pośrednictwem Internetu, a pozostałym instytucjom np.: dane przekazywane są w formie papierowej i na nośnikach danych takich jak np. płyty CD i/lub DVD.

Wskazać, czy przy użyciu teletransmisji (za pośrednictwem internetu) realizowane są także przelewy bankowe i międzybankowe.

e) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych:

**Środki organizacyjne:**

Do zastosowanych przez Administratora Danych i osoby przez niego upoważnione w ... (pełna nazwa organizacji) środków organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy:

* opracowanie i wdrożenie „Polityki bezpieczeństwa w zakresie ochrony danych osobowych w ... (pełna nazwa organizacji)”,
* opracowanie i wdrożenie „Instrukcji Zarządzania Systemem Informatycznym[[19]](#footnote-20)
służącym do przetwarzania danych osobowych w ... (pełna nazwa organizacji)”,
* wyznaczenie przez AD Administratora Bezpieczeństwa Informacji (ABI) i nadanie mu upoważnienia do przetwarzania danych osobowych,
* nadanie przez ABI członkom organów organizacji, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom organizacji upoważnień do przetwarzania danych osobowych,
* nadawanie przez ABI pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w związku z realizacją projektów/zadań,
w których organizacja będzie partnerem[[20]](#footnote-21) [niezależnie od tego, czy lider projektu/zadania (realizator) udzieli takiego upoważnienia, czy też nie],
* nadawanie przez ABI pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w pozostałych przypadkach przetwarzania danych osobowych występujących w organizacji[[21]](#footnote-22),
* wyznaczenie Administratora Systemu Informatycznego (ASI) przez ABI[[22]](#footnote-23),
* sprawowanie przez ABI oraz ASI kontroli i nadzoru nad procesem wprowadzania danych osobowych do zbioru oraz ich udostępniania.

Osobami upoważnionymi do przetwarzania danych osobowych w organizacji są:

* wymienić nazwy funkcji/stanowisk od „1” do „n”.

Powyższy katalog osób upoważnionych do przetwarzania danych osobowych w organizacji nie ma charakteru zamkniętego i może zostać poszerzony o nowe stanowiska w razie wystąpienia uzasadnionej konieczności.

Dla potrzeb ochrony danych osobowych przetwarzanych w organizacji w formie papierowej stosuje się zabezpieczenia polegające na przechowywaniu:

* dokumentacji bieżącej – np. w szafach zamykanych na zamki lub kłódki w obszarach przetwarzania danych osobowych,
* dokumentacji archiwalnej i dokumentacji pracowniczej – np. w specjalnie do tego celu przeznaczonym pomieszczeniu (np. Biblioteka/Archiwum).

**Środki techniczne:**

Do zastosowanych przez AD w organizacji środków technicznych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy:

1. W przypadku zewnętrznych (obcych) systemów informatycznych dla potrzeb bieżącego użytkowania i przesyłania danych stosowane są zabezpieczenia podmiotów, którym przekazywane są dane:

* „Płatnik” (program ZUS) – czy organizacja posiada certyfikowany publiczny klucz dostępu do tego programu wydany na czas określony, ponadto czy co 30 dni zmieniane jest hasło dostępu do programu (program przypomina o upływie terminu ważności hasła), czy gwarancję zachowania poufności danych stanowi także ograniczony krąg osób upoważnionych do jego obsługi (wpisać stanowiska osób mających dostęp do programu).
* „SODiR – System Obsługi Dofinansowań i Refundacji” (program PFRON) – czy dostęp do programu chroniony jest wymogiem podania klucza klienta, czy gwarancję zachowania poufności danych stanowi także ograniczony krąg osób upoważnionych do jego obsługi (wpisać stanowiska osób mających dostęp do programu).
* „Formularz PEFS 2007” (program do prowadzenia sprawozdawczości projektów realizowanych w ramach Programu Operacyjnego Kapitał Ludzki) – czy dostęp do programu chroniony jest wymogiem podania loginu i hasła, czy gwarancję zachowania poufności danych stanowi także ograniczony krąg osób upoważnionych do jego obsługi (np. ABI PEFS 2007, ASI, kierownicy/koordynatorzy projektów/zadań i specjaliści ds. monitoringu i ewaluacji).
* Ewentualnie – opisać zabezpieczenia systemów księgowo-kadrowo-płacowych.
* Przelewy bankowe i międzybankowe – czy strony internetowe banków, w których organizacja posiada rachunki wymagają podania loginu i hasła, a każda osoba upoważniona do dokonywania przelewów posiada indywidualny klucz dostępu, czy gwarancję zachowania poufności danych stanowi także ograniczony krąg osób upoważnionych do jego obsługi (wpisać stanowiska osób mających dostęp do rachunków bankowych).

Wskazać, czy dostęp do danych osobowych przetwarzanych w systemach informatycznych chroniony jest poprzez:

* zastosowanie loginów i haseł uniemożliwiających nieuprawnione korzystanie osobom nieupoważnionym,
* ustawienie monitorów komputerów w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

Czy loginy i hasła umożliwiające dostęp do komputerów znajdują się w zapieczętowanych kopertach? Gdzie przechowywane są koperty z loginami i hasłami?

Określić, czy w razie wystąpienia konieczności uzyskania dostępu do któregoś z komputerów w czasie nieobecności pracownika użytkującego komputer, ABI może otworzyć zapieczętowaną kopertę i umożliwić wykonanie niezbędnych czynności innemu pracownikowi. Czy po powrocie pracownika użytkującego dany komputer zmianie ulega hasło dostępu? Czy zdarzenie takie każdorazowo dokumentowane jest protokółem
z naruszenia poufności nośnika danych osobowych zawierającym:

* imiona i nazwiska osób korzystających z komputera podczas nieobecności pracownika,
* numer ewidencyjny komputera,
* datę zdarzenia,
* wskazanie przyczyny (powodu).

2. Czy w organizacji dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (MS Word), arkuszach kalkulacyjnych (MS Excel) lub programach równorzędnych (np. pakiet Open Office) i innych programach do tworzenia baz danych oraz w systemach informatycznych: „Płatnik”, „SODiR – System Obsługi Dofinansowań i Refundacji”, „Formularz PEFS 2007” do ochrony systemu informatycznego stosuje się systemy antywirusowe?

3. Czy elektroniczne przetwarzanie danych osobowych odbywa się na komputerach stacjonarnych, czy laptopach? Jakie działania podejmowane są dla zminimalizowania ryzyka dostania się ich zawartości w niepowołane ręce? Czy komputery zabezpieczone są hasłami,
a kadra organizacji została zapoznana z „Polityką bezpieczeństwa” i przeszkolona
w zakresie ochrony danych osobowych?

f) pozostałe informacje:

Czy w organizacji nie przetwarza się – poza uzasadnionymi przepisami prawa przypadkami przetwarzania danych o stanie zdrowia – danych wrażliwych (sensytywnych), do których należy przetwarzanie danych o stanie zdrowia:

* pracowników organizacji – przetwarzanie danych wynika z odrębnych przepisów prawa i dotyczy obowiązku przeprowadzenia badań lekarskich wstępnych (przed zawarciem umowy o pracę) oraz badań lekarskich okresowych (wykonywanych
w trakcie trwania zatrudnienia) i badań lekarskich pochorobowych (wykonywanych
w trakcie trwania zatrudnienia, przed powrotem do pracy po nieobecności spowodowanej długotrwałym zwolnieniem lekarskim),
* pracowników i współpracowników organizacji – przetwarzanie danych o stanie zdrowia w tym przypadku wynika z konieczności udokumentowania faktu bycia osobą niepełnosprawną poprzez przedstawienie orzeczenia o stopniu niepełnosprawności.

Czy przetwarzanie danych dotyczących pochodzenia rasowego i pochodzenia etnicznego oraz danych o stanie zdrowia w „Formularzu PEFS 2007” na rzecz Ministerstwa Rozwoju Regionalnego w Warszawie stanowi wyjątek?[[23]](#footnote-24)

Czy kandydaci do udziału w projekcie/zadaniu realizowanym przez organizację wyrażają pisemnie swoją zgodę na:

* przetwarzanie swoich danych osobowych w związku z prowadzoną rekrutacją do projektu/zadania realizowanego przez organizację;
* przetwarzanie danych o stanie swojego zdrowia w związku z prowadzoną rekrutacją do projektu/zadania realizowanego przez organizację?

Czy zapewnione są prawa osób, których dane podlegają przetwarzaniu?

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych przetwarzanych przez organizację, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;

3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania
w powszechnie zrozumiałej formie treści tych danych;

4) uzyskania informacji o źródle danych, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej;

5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji
o odbiorcach lub kategoriach odbiorców, którym dane te 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 z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926) albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

**Rozdział 2**

**Przetwarzanie danych osobowych w projekcie/zadaniu, w którym ….. (pełna nazwa organizacji) jest partnerem[[24]](#footnote-25)**

….. (pełna nazwa organizacji) może być partnerem w projekcie/zadaniu realizowanym przez inną instytucję bądź organizację pozarządową.

Jako partner projektu/zadania organizacja będzie realizowała zadania określone w treści stosownego porozumienia dotyczącego realizacji projektu/zadania.

Pracownicy i współpracownicy organizacji realizujący zadania przypisane w treści porozumienia, otrzymują od ABI pisemne upoważnienia do przetwarzania danych osobowych w zakresie określonym w treści tych upoważnień niezależnie od tego, czy lider projektu/zadania (realizator) udzielił takiego upoważnienia, czy też nie.

Upoważnienia do przetwarzania danych osobowych udzielane będą odrębnie dla każdego projektu/zadania, w którym organizacja będzie partnerem i będą obowiązywały do dnia ich odwołania.

Do udzielenia upoważnienia do przetwarzania danych osobowych w projekcie/zadaniu, w którym organizacja jest partnerem, stosuje się odpowiednio Załącznik nr 3 do niniejszej „Polityki bezpieczeństwa”.

Do odwołania udzielonego upoważnienia stosuje się odpowiednio Załącznik nr 6 do ww. dokumentu.

Do udzielania oraz odwoływania upoważnień do przetwarzania danych osobowych w projekcie/zadaniu, w którym organizacja będzie partnerem upoważniony jest ABI (Załącznik nr 2 „B” do ww. dokumentu).

AD będzie każdorazowo udzielał ABI upoważnienia do przetwarzania danych osobowych w projekcie/zadaniu, w którym organizacja będzie partnerem stosując odpowiednio Załącznik nr 2 „A” do ww. dokumentu.

Do odwołania udzielonego ABI upoważnienia do przetwarzania danych osobowych w projekcie/zadaniu, w którym organizacja będzie partnerem AD stosuje odpowiednio Załącznik nr 5 „A” do ww. dokumentu.

Miejscem przetwarzania danych osobowych w projekcie/zadaniu, w którym organizacja będzie partnerem będzie biuro projektu/zadania (najczęściej siedziba realizatora projektu/zadania).

**Rozdział 3**

**Powierzenie przez ….. (pełna nazwa organizacji) podmiotowi zewnętrznemu przetwarzania danych osobowych w ramach realizacji zadań z zakresu monitoringu i ewaluacji projektu/zadania[[25]](#footnote-26)**

…... (pełna nazwa organizacji) może być podmiotem, który na podstawie umowy zawartej w formie pisemnej powierzy podmiotowi zewnętrznemu przetwarzanie danych osobowych w realizowanym przez siebie projekcie/zadaniu.

Organizacja będzie w takim przypadku podmiotem powierzającym prowadzenie zadania związanego z prowadzeniem monitoringu i ewaluacji w projekcie/zadaniu, który realizuje.

Procedura nadawania i odwoływania pracownikom i współpracownikom instytucji, której powierzone zostanie przetwarzanie danych osobowych, upoważnień do przetwarzania tych danych w projekcie/zadaniu, które organizacja realizuje, jest tożsame z procedurą nadawania
i odwoływania uprawnień do przetwarzania danych osobowych pracownikom
i współpracownikom organizacji.

Pracownicy i współpracownicy instytucji prowadzącej zadania z zakresu monitoringu
i ewaluacji w projekcie/zadaniu, który realizuje organizacja, otrzymują od ABI organizacji pisemne upoważnienia do przetwarzania danych osobowych w zakresie określonym w treści tych upoważnień. Upoważnienia będą obowiązywały do dnia ich odwołania.

Do udzielenia upoważnienia do przetwarzania danych osobowych w projekcie/zadaniu,
w którym organizacja powierza podmiotowi zewnętrznemu prowadzenie zadania związanego
z monitoringiem i ewaluacją stosuje się odpowiednio Załącznik nr 3 do „Polityki bezpieczeństwa”.

Do odwołania udzielonego upoważnienia stosuje się odpowiednio Załącznik nr 6 do ww. dokumentu.

Do udzielania oraz odwoływania upoważnień do przetwarzania danych osobowych
w projekcie/zadaniu, w którym organizacja powierza podmiotowi zewnętrznemu prowadzenie zadań z zakresu monitoringu/ewaluacji projektu/zadania, upoważniony jest ABI (Załącznik nr 2 „B” do „Polityki bezpieczeństwa”).

Miejscem przetwarzania danych osobowych w projekcie/zadaniu, w którym organizacja powierza prowadzenie zadań z zakresu monitoringu i ewaluacji projektu/zadania podmiotowi zewnętrznemu, będzie siedziba wykonawcy.

Dokumenty związane z prowadzeniem zadań z zakresu monitoringu i ewaluacji
w projekcie/zadaniu, w którym organizacja powierza podmiotowi zewnętrznemu prowadzenie tych zadań, przechowywane będą: (np. w zamykanym na klucz pomieszczeniu
w siedzibie wykonawcy). Dokumenty te będą przechowywane w siedzibie wykonawcy do momentu, w którym przestanie obowiązywać umowa w sprawie powierzenia przetwarzania danych osobowych.

Przekazanie organizacji przez wykonawcę w całości powierzonych do przetwarzania danych osobowych nastąpi protokółem przekazania (stanowiącym Załącznik nr 12 „A” do „Polityki bezpieczeństwa”) w momencie zakończenia obowiązywania umowy w sprawie powierzenia przetwarzania danych osobowych.

**Rozdział 4**

**Pozostałe przypadki przetwarzania danych osobowych w ….. (pełna nazwa organizacji)[[26]](#footnote-27)**

W ... (pełna nazwa organizacji) dane osobowe mogą być przetwarzane (np.) w związku
z realizacją:

* szkoleń zlecanych przez instytucje zewnętrzne (np. finansowanych ze środków Unii Europejskiej).

Przetwarzanie danych będzie się odbywać na podstawie upoważnień.

Do udzielenia upoważnienia do przetwarzania danych osobowych stosowany będzie odpowiednio Załącznik nr 3 do „Polityki bezpieczeństwa”.

Do odwołania udzielonego upoważnienia stosowany będzie odpowiednio Załącznik nr 6 do ww. dokumentu.

Do udzielania oraz odwoływania upoważnień do przetwarzania danych osobowych upoważniony jest ABI (Załącznik nr 2 „B” do „Polityki bezpieczeństwa”).

AD będzie każdorazowo udzielał ABI upoważnienia do przetwarzania danych osobowych stosując odpowiednio Załącznik nr 2 „A” do ww. dokumentu.

Do odwołania udzielonego ABI upoważnienia do przetwarzania danych osobowych AD zastosuje odpowiednio Załącznik nr 5 „A” do „Polityki bezpieczeństwa”.

Miejscem przetwarzania danych osobowych może być siedziba organizacji lub miejsce wskazane przez instytucję zlecającą.

**Rozdział 5**

**Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 („PEFS 2007”)[[27]](#footnote-28)**

W tym miejscu dostosować odpowiednio wzór dokumentu[[28]](#footnote-29) przygotowany przez Instytucję Zarządzającą Programem Operacyjnym Kapitał Ludzki (Ministerstwo Rozwoju Regionalnego) lub umieścić informację, że uregulowania dotyczące tego zakresu zostały zamieszczone w odrębnym dokumencie, przyjętym odrębną uchwałą.

a) postanowienia ogólne

…...

b) zakres oraz zasady zabezpieczania danych osobowych

…...

c) obowiązki Administratora Bezpieczeństwa Informacji PEFS 2007 w ... (pełna nazwa organizacji)

…...

d) przetwarzanie danych osobowych

…...

e) postępowanie w przypadku naruszenia ochrony danych osobowych

…...

f) kontrola nad przestrzeganiem ochrony danych osobowych

…...

g) postanowienia końcowe

...

**Rozdział 6**

**Opis zdarzeń naruszających ochronę danych osobowych**

1. Podział zagrożeń:

1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu – ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) Zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych – zazwyczaj nie następuje uszkodzenie infrastruktury technicznej
i zakłócenie ciągłości pracy.

Zagrożenia te możemy podzielić na:

a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),

b) nieuprawniony dostęp do systemu z jego wnętrza,

c) nieuprawniony przekaz danych,

d) pogorszenie jakości sprzętu i oprogramowania,

e) bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:

1) **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu**, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

2) **niewłaściwe** **parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;

3) **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie
w kierunku naruszenia ochrony danych lub wręcz sabotaż;

4) **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

5) **pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego** wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację
w systemie;

6) **naruszenie lub próba naruszenia** integralności systemu lub bazy danych
w tym systemie;

7) stwierdzona **próba modyfikacji lub modyfikacja danych lub zmiana** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

8) **niedopuszczalna manipulacja** danymi osobowymi w systemie;

9) **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;

10) **nieprzypadkowe odstępstwa** **od zasad bezpieczeństwa pracy** **w systemie lub sieci komputerowej** wskazujące na przełamanie lub zaniechanie ochrony danych osobowych
– np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;

11) **istnienie nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki” itp.;

12) **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;

13) **rażące naruszenie dyscypliny pracy** w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości
w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

**Rozdział 7**

**Zabezpieczenie danych osobowych**

1. Administratorem danych osobowych zawartych i przetwarzanych w rejestrach zbiorów danych ... (pełna nazwa organizacji) – przedstawionych w Rozdziale 1: ... (pełna nazwa organizacji), podpunkt „b” niniejszej „Polityki bezpieczeństwa” – w systemach informatycznych i na nośnikach tradycyjnych wyszczególnionych w punktach:

* od „1” do „n”[[29]](#footnote-30) – jest Zarząd organizacji,
* „n+1” – jest Ministerstwo Rozwoju Regionalnego w Warszawie, organizacja natomiast przetwarza dane osobowe na jego rzecz [dotyczy uczestników (beneficjentów) projektów PO KL].

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych i na nośnikach tradycyjnych, a w szczególności do:

1) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,

2) zapobiegania kradzieży danych,

3) zapobiegania przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych
i przystosowanych do tego pomieszczeniach;

2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1;

3) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji
i nośników danych.

4. Do zastosowanych środków organizacyjnych należą następujące zasady:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych;

2) przeszkolenie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń
i programów związanych z przetwarzaniem i ochroną danych osobowych;

3) kontrolowanie otwierania i zamykania pomieszczeń wymienionych w pkt 3.1, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianiu pomieszczenia w czasie pracy bez nadzoru.

5. Niezależnie od niniejszych zasad, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, przy czym dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „Polityce bezpieczeństwa”.

6. AD za pośrednictwem ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

**Rozdział 8**

**Postępowanie w przypadku naruszenia ochrony danych osobowych**

1. W przypadku stwierdzenia :

* naruszenia zabezpieczeń systemu informatycznego,
* naruszenia technicznego stanu urządzeń,
* naruszenia zawartości zbioru danych osobowych,
* ujawnienia metody pracy lub sposobu działania programu,
* jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
* innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie ABI.

2. W razie niemożliwości zawiadomienia ABI lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia danych osobowych ABI lub upoważnionej przez niego osoby, należy:

* niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić
w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
* udokumentować wstępnie zaistniałe naruszenie;
* nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby przez niego upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, ABI lub osoba przez niego upoważniona:

* zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji;
* może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
* rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych AD;
* nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji.

5. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, ABI zasięga niezbędnych opinii
i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. ABI dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych
w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;

b) określenie czasu i miejsca: naruszenia/ujawnienia i powiadomienia o tym fakcie;

c) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;

d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;

e) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;

f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Raport, o którym mowa w pkt. 6, ABI niezwłocznie przekazuje AD.

8. Zaistniałe naruszenie/ujawnienie ochrony danych osobowych może stać się przedmiotem szczegółowej analizy prowadzonej przez AD i ABI.

9. Analiza, o której mowa w pkt. 8, powinna zawierać:

a) wszechstronną ocenę zaistniałego naruszenia/ujawnienia ochrony danych osobowych;

b) wskazanie odpowiedzialnych;

c) wnioski co do ewentualnych przedsięwzięć: proceduralnych, organizacyjnych, kadrowych
i technicznych, które powinny zapobiec podobnym naruszeniom/ujawnieniom w przyszłości.

**Rozdział 9**

**Postanowienia końcowe**

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych,
w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie ABI.

2. Osoby, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt poprzez podpisanie oświadczenia (załącznik
nr 1 „A” do „Polityki bezpieczeństwa”).

3. Ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, zobowiązany jest prowadzić ABI.

4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego
w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie
z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie.

5. Orzeczona kara wobec osoby uchylającej się od powiadomienia ABI nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. z 1997 r. Nr 133, poz. 883; tekst jednolity:
Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej przez organizację sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.

6. Wszystkie regulacje dotyczące systemów informatycznych określone w „Polityce bezpieczeństwa” dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

7. Wdrożenie „Polityki bezpieczeństwa” odbywa się poprzez:

a) zapoznanie osób wchodzących w skład organów organizacji, pracowników, współpracowników, wolontariuszy, praktykantów i stażystów organizacji z treścią „Polityki bezpieczeństwa”;

b) szkolenia z zakresu ochrony danych osobowych.

8. „Polityka bezpieczeństwa” wchodzi w życie z dniem podjęcia Uchwały Zarządu organizacji lub w terminie określonym w treści tej Uchwały.

Zmiany w „Polityce bezpieczeństwa” będą wchodzić w życie w terminach określonych
w Uchwałach Zarządu organizacji dotyczących wprowadzenia zmian w dokumencie.

Zmiany te dokumentuje się w Arkuszu Zmian (Rozdział 10).

**Rozdział 10**

**Arkusz zmian**

|  |  |  |
| --- | --- | --- |
| L.p. | Treść zmiany | Data |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |

**CZĘŚĆ II**

**Instrukcja w sprawie zasad postępowania przy przetwarzaniu danych osobowych**

§ 1

Instrukcja w sprawie zasad przetwarzania danych osobowych – zwana dalej „Instrukcją” – określa w szczególności:

1) Obowiązki osób upoważnionych do przetwarzania danych osobowych w ... (pełna nazwa organizacji) [zwanej dalej „….... (nazwa skrócona organizacji)”].

2) Tryb udzielania upoważnień do przetwarzania danych osobowych.

3) Sposób prowadzenia i aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych.

4) Sposób prowadzenia i aktualizacji rejestru zbiorów danych osobowych.

§ 2

Definicje zawarte w dokumencie pn.: „Polityka bezpieczeństwa w zakresie ochrony danych osobowych w ... (pełna nazwa organizacji)” stosuje się odpowiednio.

§ 3

ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych zapewniając bezpieczeństwo danych osobowych w systemie informatycznym, w szczególności przeciwdziałając dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmując odpowiednie działania w przypadku wykrycia naruszeń w systemie zabezpieczeń.

§ 4

ABI i AD współpracują ze sobą przy realizacji zadań z zakresu ochrony danych osobowych.

§ 5

ABI zobowiązany jest do nadzoru nad postępowaniem przy przetwarzaniu danych osobowych w organizacji, a w szczególności do:

1) zastosowania niezbędnych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych, a w szczególności zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, kradzieżą, przetwarzaniem z naruszeniem przepisów prawa, zmianą, utratą, uszkodzeniem lub zniszczeniem.

2) kontroli nad wykonywaniem operacji przetwarzania danych osobowych przez osoby upoważnione.

3) zwracania się do AD w przypadku istotnych wątpliwości wynikających ze stosowania przepisów ustawy o ochronie danych osobowych oraz przepisów wykonawczych.

§ 6

Osoba upoważniona do przetwarzania danych zobowiązana jest do:

1) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych.

2) zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą.

3) stosowania określonych przez AD procedur i środków przetwarzania oraz zabezpieczania danych osobowych.

4) podporządkowania się poleceniom ABI i AD w zakresie ochrony danych osobowych.

5) zachowania danych osobowych w tajemnicy.

6) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa,
a w szczególności:

a) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem.

b) zabezpieczenia danych osobowych przed ich zmianą.

c) zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym.

d) zamykania i zabezpieczania pomieszczeń, w których przetwarzane są dane osobowe
w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

e) dopilnowania, by przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej.

f) dopilnowania, by przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie.

g) przetwarzania danych osobowych zgodnie z celem, dla którego zostały zebrane.

§ 7

W przypadku stwierdzenia naruszenia zasad postępowania przy przetwarzaniu danych osobowych lub naruszeniu zabezpieczenia danych osoba upoważniona zobowiązana jest niezwłocznie poinformować ABI, który przekazuje tę informację AD.

§ 8

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez AD.

2. ABI ponosi odpowiedzialność za zaznajomienie pracownika, który ma być dopuszczony do przetwarzania danych osobowych z przepisami towarzyszącymi ochronie danych osobowych. Fakt zapoznania się z przepisami pracownik potwierdza własnoręcznym podpisem.

3. ABI wydaje upoważnienia do przetwarzania danych osobowych organom organizacji, każdemu pracownikowi, współpracownikowi, wolontariuszowi, praktykantowi, stażyście, który przy wykonywaniu powierzonych mu zadań przetwarza dane osobowe.

4. Upoważnienie udzielane jest na czas wykonywania przez osobę upoważnioną czynności na powierzonym stanowisku.

5. ABI zobowiązany jest niezwłocznie poinformować AD o zaprzestaniu wykonywania czynności przetwarzania danych osobowych przez osobę upoważnioną.

§ 9

1. Każda osoba upoważniona powinna odbyć szkolenie z zakresu ochrony danych osobowych.

2. Szkolenie z zakresu ochrony danych osobowych organizuje ABI.

§ 10

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest
w formie papierowej i/lub elektronicznej.

2. Ewidencję, o której mowa w pkt. 1, prowadzi ABI.

3. Za aktualizację ewidencji osób upoważnionych do przetwarzania danych osobowych odpowiada ABI.

4. O każdym zdarzeniu powodującym konieczność wprowadzenia zmian w ewidencji,
o której mowa w pkt. 1, musi zostać poinformowany ABI.

§ 11

1. **Rejestr zbiorów danych osobowych** przetwarzanych w organizacji prowadzony jest
w formie papierowej i/lub elektronicznej.

2. Rejestr zbiorów danych osobowych prowadzi ABI.

3. O planowanym utworzeniu nowego zbioru danych osobowych należy poinformować ABI. Informacja ta powinna zawierać:

a) nazwę zbioru.

b) podstawę utworzenia zbioru.

c) oznaczenie rodzaju zbioru.

d) określenie sposobu przetwarzania danych w zbiorze (system informatyczny, przetwarzanie elektroniczne, przetwarzanie odręczne).

e) określenie zakresu przetwarzania danych.

f) określenie celu przetwarzania danych.

g) informację o kategoriach odbiorców, którym dane mogą być przekazywane.

h) informację o sposobie udostępniania danych.

i) informację o tym, czy zbiór podlega obowiązkowi rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych.

j) uzasadnienie potrzeby utworzenia zbioru.

4. O każdej zmianie dotyczącej przetwarzania danych w zbiorze należy poinformować ABI.

**CZĘŚĆ III**

**Instrukcja dla osób upoważnionych do przetwarzania danych osobowych**

§ 1

Niniejsza „Instrukcja dla osób upoważnionych do przetwarzania danych osobowych” – zwana dalej „Instrukcją” – określa tryb postępowania w przypadku, gdy:

* stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie.
* stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 2

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:

1) **Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu**, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.

2) **Niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.

3) **Awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie
w kierunku naruszenia ochrony danych lub wręcz sabotaż.

4) **Pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.

5) **Jakość danych w systemie lub inne odstępstwo** od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.

6) **Nastąpiło naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie.

7) **Stwierdzono próbę lub modyfikację danych lub zmianę** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).

8) **Nastąpiła niedopuszczalna manipulacja danymi** **osobowymi** w systemie.

9) **Ujawniono osobom nieupoważnionym dane osobowe** lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń.

10) **Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa** od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.

11) **Ujawniono istnienie nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki”, itp.

12) **Podmieniono lub zniszczono nośniki z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe.

13) **Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

§ 3

1. Każda osoba w organizacji (reprezentująca organ organizacji bądź w niej zatrudniona lub współpracująca włącznie z wolontariuszami, praktykantami i stażystami), która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym lub przetwarzanych w inny sposób, powinna niezwłocznie poinformować
o tym osobę zatrudnioną przy przetwarzaniu tych danych, bezpośredniego przełożonego oraz ABI albo inną upoważnioną przez niego osobę.

2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych zobowiązana jest niezwłocznie powiadomić o tym ABI.

§ 4

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa – należy przeprowadzić postępowanie wyjaśniające czy dane osobowe należy uznać za ujawnione.

§ 5

Niezwłocznie po uzyskaniu informacji o naruszeniu danych osobowych należy podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych przez osoby niepowołane poprzez:

1) Fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej.

2) Wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

3) Zmianę hasła na konto ABI i użytkownika, poprzez które uzyskano nielegalny dostęp
w celu uniknięcia ponownej próby włamania.

4) Podjęcie innych – stosownych do zagrożenia – działań.

§ 6

ABI – po uzyskaniu sygnału o naruszeniu danych osobowych – powinien w pierwszej kolejności:

1) Zapisać wszelkie informacje związane z danym zdarzeniem.

2) Na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia.

3) Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia – zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby nieuprawnionej.

4) Wyniki postępowania zabezpieczającego oraz okoliczności naruszenia bezpieczeństwa danych osobowych należy ująć w raporcie i niezwłocznie przekazać AD.

§ 7

1. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI lub upoważnionej przez niego osoby należy:

1) Niezwłocznie podjąć czynności (określone w rozdziale 9 pkt 3 niniejszej „Polityki bezpieczeństwa”) niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców.

2) Rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia.

3) Zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się
z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę.

4) Podjąć inne działania przewidziane i określone w instrukcjach technicznych
i technologicznych – stosownie do objawów i komunikatów towarzyszących naruszeniu.

5) Podjąć stosowne działania – jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej.

6) Zastosować się do innych instrukcji i regulaminów – jeżeli odnoszą się one do zaistniałego przypadku.

7) Udokumentować wstępnie zaistniałe naruszenie.

8) Nie opuszczać – bez uzasadnionej potrzeby – miejsca zdarzenia do czasu przybycia ABI lub upoważnionej przez niego osoby.

2. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych ABI lub osoba go zastępująca:

1) Zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji.

2) Niezwłocznie informuje AD.

3) Może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

4) Nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji w porozumieniu z AD.

§ 8

1. Po dokonaniu czynności zabezpieczenia danych osobowych i ustaleniu przyczyn naruszenia ochrony danych osobowych należy niezwłocznie przywrócić normalny stan działania.

2. Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

3. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych ABI niezwłocznie zarządza przeprowadzenie dodatkowego szkolenia dla osób biorących udział przy przetwarzaniu danych osobowych. Dokumentację z przeprowadzonego szkolenia ABI załącza do raportu określonego w treści § 9.

§ 9

1. Po dokonaniu czynności przedstawionych powyżej ABI sporządza szczegółowy raport zawierający:

1) Opis zdarzenia.

2) Przyczynę zaistnienia.

3) Skutki naruszenia ochrony danych osobowych.

4) Podjęte działania, zastosowane środki.

5) Analizę zdarzenia oraz wnioski dotyczące przedsięwzięć:

a) organizacyjnych,

b) technicznych,

c) kadrowych.

2. Raport ABI przedkłada niezwłocznie AD, który wydaje pisemne zalecenia.

3. Całość dokumentacji w zakresie naruszenia systemu ochrony danych osobowych przechowuje ABI.

**CZĘŚĆ IV**

**Załączniki**

Załącznik nr 1 „A”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

………………………………………….

imię i nazwisko

…………………………………………

funkcja / stanowisko

**OŚWIADCZENIE**

Oświadczam, że zapoznałem/-am się z treścią „Polityki bezpieczeństwa w zakresie ochrony danych osobowych w ... (pełna nazwa organizacji)” i zobowiązuję się do stosowania zasad w niej zawartych.

...........………, dnia ……………….. …………………………………..

miejscowość podpis

.........................

pieczęć nagłówkowa organizacji[[30]](#footnote-31)

Załącznik nr 1 „B”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

**Lista osób, które zapoznały się**

**z „Polityką bezpieczeństwa w zakresie ochrony danych osobowych
w ….. (pełna nazwa organizacji)”**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Imię i nazwisko** | **Data** | **Podpis** |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |
| **6** |  |  |  |
| **7** |  |  |  |
| **8** |  |  |  |
| **9** |  |  |  |
| **10** |  |  |  |
| **11** |  |  |  |
| **12** |  |  |  |
| **13** |  |  |  |
| **14** |  |  |  |
| **15** |  |  |  |
| **16** |  |  |  |
| **17** |  |  |  |
| **18** |  |  |  |
| **...** |  |  |  |

.........................

pieczęć Administratora Danych[[31]](#footnote-32)

Załącznik nr 2 „A”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

**UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH**

**dla Administratora Bezpieczeństwa Informacji**

Z dniem .........................., na podstawie art. 37 ustawy z dnia
29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), upoważniam Panią/Pana\* ........................................., będącą/będącego\* Administratorem Bezpieczeństwa Informacji, do przetwarzania danych osobowych dotyczących[[32]](#footnote-33):

* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................

Upoważnienie obowiązuje do dnia odwołania.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Podpisy osób upoważnionych do reprezentowania Administratora Danych

\* Niepotrzebne skreślić.

.........................

pieczęć Administratora Danych

Załącznik nr 2 „B”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

**UPOWAŻNIENIE**

**dla Administratora Bezpieczeństwa Informacji**

**do reprezentowania Administratora Danych
oraz udzielania i odwoływania upoważnień**

Z dniem **..........................,** upoważniam **Panią/Pana\* .................................,** będącą/będącego\* Administratorem Bezpieczeństwa Informacji, do:

* reprezentowania Administratora Danych[[33]](#footnote-34);
* powoływania w imieniu Administratora Danych Administratora Systemu Informatycznego[[34]](#footnote-35) i nadawania ASI stosownego upoważnienia;
* odwoływania w imieniu Administratora Danych Administratora Systemu Informatycznego[[35]](#footnote-36) i nadanego ASI upoważnienia;
* udzielania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych: osobom wchodzącym w skład organów organizacji, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom organizacji;
* odwoływania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych udzielonych: osobom wchodzącym w skład organów organizacji, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom organizacji.

Upoważnienie obowiązuje do dnia odwołania.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Podpisy osób upoważnionych do reprezentowania Administratora Danych

\* Niepotrzebne skreślić.

.........................

pieczęć Administratora Danych

Załącznik nr 3

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

**UPOWAŻNIENIE[[36]](#footnote-37)
DO PRZETWARZANIA DANYCH OSOBOWYCH**

**Nr \_\_\_\_\_\_\_\_\_\_\_\_\_**

Z dniem **..........................,** na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r.
o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), upoważniam **Panią/Pana\* ...................................** do przetwarzania danych osobowych dotyczących[[37]](#footnote-38):

* ......................................................................
* ......................................................................
* ......................................................................
* ......................................................................

Upoważnienie obowiązuje do dnia odwołania.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Podpis Administratora Bezpieczeństwa Informacji

\* - niepotrzebne skreślić

.........................

pieczęć Administratora Danych

Załącznik nr 4

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

Ewidencja osób upoważnionych do przetwarzania danych osobowych
w ... (pełna nazwa organizacji)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Lp. | Imię i nazwisko | Data zapoznania z dokumentem | Stanowisko / funkcja | Typ umowy / porozumienia | Zakres rzeczowy uprawnienia | Ramy czasowe |
| Pracownik | Współpracownik | Wolontariusz | Praktyka / Staż | od …[[38]](#footnote-39) | do …[[39]](#footnote-40) |
| 1 |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |
| ... |  |  |  |  |  |  |  |  |  |  |

.........................

pieczęć Administratora Danych

Załącznik nr 5 „A”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

**ODWOŁANIE UPOWAŻNIENIA**

**DO PRZETWARZANIA DANYCH OSOBOWYCH**

**przez Administratora Bezpieczeństwa Informacji**

Z dniem **..........................,** na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r.
o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), odwołujemy upoważnienie **Pani/Pana\* ..................................,** będącej/będącego\* Administratorem Bezpieczeństwa Informacji, do przetwarzania danych osobowych dotyczących[[40]](#footnote-41):

* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................
* ........................................

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Podpisy osób upoważnionych do reprezentowania Administratora Danych

\* Niepotrzebne skreślić.

.........................

pieczęć Administratora Danych

Załącznik nr 5 „B”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

**ODWOŁANIE UPOWAŻNIENIA**

**Administratora Bezpieczeństwa Informacji**

**do reprezentowania Administratora Danych**

**oraz udzielania i odwoływania upoważnień**

Z dniem **..........................,** odwołujemy upoważnienie **Pani/Pana\*................................,** będącej/będącego\* Administratorem Bezpieczeństwa Informacji, do[[41]](#footnote-42):

* reprezentowania Administratora Danych;
* powoływania w imieniu Administratora Danych Administratora Systemu Informatycznego i nadawania ASI stosownego upoważnienia;
* odwoływania w imieniu Administratora Danych Administratora Systemu Informatycznego i nadanego ASI upoważnienia;
* udzielania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych: osobom wchodzącym w skład organów organizacji, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom organizacji;
* odwoływania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych udzielonych: osobom wchodzącym w skład organów organizacji, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom organizacji.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Podpisy osób upoważnionych do reprezentowania Administratora Danych

\* Niepotrzebne skreślić.

.........................

pieczęć Administratora Danych

Załącznik nr 6

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

**ODWOŁANIE[[42]](#footnote-43)**

**UPOWAŻNIENIA Nr \_\_\_\_\_\_\_\_\_\_\_\_
DO PRZETWARZANIA DANYCH OSOBOWYCH**

Z dniem **..........................,** na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r.
o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), odwołuję upoważnienie **Nr …………………...……… Pani/Pana\*** **...................................** do przetwarzania danych osobowych dotyczących[[43]](#footnote-44):

* ......................................................................
* ......................................................................
* ......................................................................
* ......................................................................
* ......................................................................
* ………………………………………..........

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Podpis Administratora Bezpieczeństwa Informacji

\* Niepotrzebne skreślić.

.........................

pieczęć Administratora Danych

Załącznik nr 7

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

Rejestr zbiorów danych osobowych przetwarzanych
w ….. (pełna nazwa organizacji)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Nazwa zbioru danych osobowych | Nazwa programu stosowanego do przetwarzania | Lokalizacja miejsca przetwarzania (budynek, pomieszczenie, nazwa komputera) | Obowiązek zgłoszenia zbioru danych osobowych GIODO\* TAK / NIE\*\* |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| … |  |  |  |  |

\* Generalny Inspektor Ochrony Danych Osobowych

\*\* wpisać właściwe

.........................

pieczęć Administratora Danych

Załącznik nr 8

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

Informacja o planowanym utworzeniu nowego zbioru danych osobowych
w ... (pełna nazwa organizacji)

|  |  |
| --- | --- |
| Nazwa zbioru |  |
| Podstawa prawna utworzenia zbioru |  |
| Oznaczenie rodzaju zbioru |  |
| Sposób przetwarzania danych w zbiorze (system informatyczny, przetwarzanie elektroniczne, przetwarzanie odręczne) |  |
| Zakres przetwarzania danych |  |
| Cel przetwarzania danych |  |
| Kategorie odbiorców, którym dane mogą być przekazywane |  |
| Sposób udostępniania danych |  |
| Obowiązek rejestracji zbioru przez GIODO\* (TAK / NIE\*\*) |  |
| Uzasadnienie potrzeby utworzenia zbioru |  |

 \* Generalny Inspektor Ochrony Danych Osobowych

\*\* wpisać właściwe

.........................

pieczęć Administratora Danych

Załącznik nr 9

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

Raport z naruszenia ochrony danych osobowych

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem | Określenie czasu i miejsca: naruszenia i powiadomienia | Określenie okoliczności towarzyszących naruszeniu i rodzaju naruszenia | Wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania | Wstępna ocena przyczyn wystąpienia naruszenia | Ocena przeprowadzonego postępowania wyjaśniającego i naprawczego |
|  |  |  |  |  |  |

…………………………………………....

Podpis Administratora Bezpieczeństwa Informacji

.........................

pieczęć Administratora Danych

Załącznik nr 10

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

Analiza naruszenia ochrony danych osobowych

|  |  |  |
| --- | --- | --- |
| Wszechstronna ocena zaistniałego naruszenia | Wskazanie odpowiedzialnych | Wnioski co do przedsięwzięć |
| proceduralnych | organizacyjnych | personalnych | technicznych |
|  |  |  |  |  |  |

……………………………………….....

Podpis Administratora Bezpieczeństwa Informacji

.........................

pieczęć Administratora Danych

Załącznik nr 11

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

Protokół z naruszenia poufności

nośnika danych osobowych

|  |  |
| --- | --- |
| Imię i nazwisko osoby korzystającej z komputera podczas nieobecności pracownika |  |
| Numer ewidencyjny komputera |  |
| Data zdarzenia |  |
| Wskazanie przyczyny (powodu) naruszenia poufności nośnika danych osobowych |  |

...................................

podpis osoby sporządzającej protokół

Załącznik nr 12 „A”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

..................................., dnia .......................

miejscowość

….. (pełna nazwa Przekazującego)

...... (dane adresowe Przekazującego)

..................................

..................................

..... (pełna nazwa organizacji)

...... (dane adresowe organizacji)

...................................

...................................

Dotyczy: ......................

 ......................

 ......................

PROTOKÓŁ PRZEKAZANIA

…... (pełna nazwa Przekazującego) niniejszym przekazuje ……. (pełna nazwa organizacji Naszej):

1. ......................................................................
2. ......................................................................
3. ......................................................................

Szczegółową specyfikację przedstawia załączone do niniejszego Protokółu Zestawienie przekazywanych danych osobowych.

…………………………….... ……………………………………

Przekazujący Odbierający

Załącznik nr 12 „B”

do „Polityki bezpieczeństwa

w zakresie ochrony danych osobowych

w ... (pełna nazwa organizacji)”

Załącznik nr 1

do Protokołu Przekazania

z dnia .................

str. ... z ... (np.: str. 1 z 3)

Zestawienie przekazywanych danych osobowych

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| L.p. | Imię i nazwisko | Rodzaj i forma nośnika danych osobowych | Dotyczy | L.p. | Imię i nazwisko | Rodzaj i forma nośnika danych osobowych | Dotyczy |
| 1 |  |  |  | 16 |  |  |  |
| 2 |  |  |  | 17 |  |  |  |
| 3 |  |  |  | 18 |  |  |  |
| 4 |  |  |  | 19 |  |  |  |
| 5 |  |  |  | 20 |  |  |  |
| 6 |  |  |  | 21 |  |  |  |
| 7 |  |  |  | 22 |  |  |  |
| 8 |  |  |  | 23 |  |  |  |
| 9 |  |  |  | 24 |  |  |  |
| 10 |  |  |  | 25 |  |  |  |
| 11 |  |  |  | 26 |  |  |  |
| 12 |  |  |  | 27 |  |  |  |
| 13 |  |  |  | 28 |  |  |  |
| 14 |  |  |  | 29 |  |  |  |
| 15 |  |  |  | ... |  |  |  |

1. **UWAGA:** ŻÓŁTYM kolorem w tekście zaznaczone są obszary przeznaczone do indywidualnej edycji, wypełnienia przez każdą organizację danymi, które jej dotyczą. [↑](#footnote-ref-2)
2. Mają go zarówno stowarzyszenia, jak i fundacje – i z tej przyczyny sugeruję organ ten wskazać do decydowania o celach i środkach przetwarzania danych osobowych (zgodnie z art. 7 pkt 4 ustawy z dnia
29 sierpnia 1997 r. o ochronie danych osobowych – tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926) [↑](#footnote-ref-3)
3. Prezes lub inny członek Zarządu organizacji albo wyznaczony pracownik organizacji – wówczas należy wpisać nazwę stanowiska zajmowanego przez pracownika [↑](#footnote-ref-4)
4. Dotyczy tylko organizacji realizujących projekty współfinansowane ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego (Program Operacyjny Kapitał Ludzki) [↑](#footnote-ref-5)
5. Jeśli dotyczy [↑](#footnote-ref-6)
6. Jeśli dotyczy [↑](#footnote-ref-7)
7. Jeśli dotyczy [↑](#footnote-ref-8)
8. Jeśli dotyczy [↑](#footnote-ref-9)
9. Jeśli dotyczy [↑](#footnote-ref-10)
10. Jeśli organizacja przetwarza dane w systemie/-ach informatycznym/-ych – wówczas upoważnienie takie powinno stanowić załącznik do instrukcji zarządzania systemem informatycznym [↑](#footnote-ref-11)
11. Wzór odwołania upoważnienia powinien także stanowić załącznik do instrukcji zarządzania systemem informatycznym [↑](#footnote-ref-12)
12. W przypadku przetwarzania danych osobowych uczestników projektów PO KL, ABI powinien:

a) prowadzić odrębną ewidencję osób upoważnionych do przetwarzania danych osobowych (na listowniku projektu),

b) wydawać upoważnienia do przetwarzania danych osobowych według wzoru stanowiącego załącznik do umowy o dofinansowanie realizacji konkretnego projektu,

c) odwoływać upoważnienia do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik do umowy o dofinansowanie realizacji konkretnego projektu. [↑](#footnote-ref-13)
13. Jeśli dane osobowe przetwarzane są w systemie informatycznym rozumianym zarówno jako sprzęt komputerowy i programy służące do przetwarzania danych osobowych [↑](#footnote-ref-14)
14. Jeśli dotyczy [↑](#footnote-ref-15)
15. Jeśli w organizacji wystąpi obowiązek zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO) [↑](#footnote-ref-16)
16. „Polityka bezpieczeństwa...” jest dokumentem wewnętrznym, stosowanym w konkretnej organizacji i ze względu na rodzaj i charakter informacji zawartych w tym punkcie nie powinna być publikowana na stronie WWW organizacji ani tym bardziej udostępniana w Internecie – bo opisuje „ścieżkę dostępu” do organizacji
i ujawnia jej techniczne zabezpieczenia [↑](#footnote-ref-17)
17. Wymienić po kolei nazwy wszystkich przetwarzanych w organizacji zbiorów danych osobowych – np. członków stowarzyszenia; darczyńców; kandydatów do pracy, pracowników; współpracowników; wolontariuszy, praktykantów i stażystów; kandydatów do udziału w projekcie; uczestników projektu etc. [↑](#footnote-ref-18)
18. Przykładowe systemy informatyczne. [↑](#footnote-ref-19)
19. Jeśli dotyczy. [↑](#footnote-ref-20)
20. Jeśli dotyczy. [↑](#footnote-ref-21)
21. Jeśli dotyczy. [↑](#footnote-ref-22)
22. Jeśli dotyczy. [↑](#footnote-ref-23)
23. Informacja dotyczy wyłącznie organizacji realizujących projekty PO KL [↑](#footnote-ref-24)
24. Jeśli ta sytuacja nie występuje w organizacji – rozdział można pominąć. [↑](#footnote-ref-25)
25. Jeśli ta sytuacja nie występuje w organizacji – rozdział można pominąć. [↑](#footnote-ref-26)
26. Jeśli ta sytuacja nie występuje w organizacji – rozdział można pominąć. [↑](#footnote-ref-27)
27. Dotyczy wyłącznie organizacji realizujących projekty PO KL [↑](#footnote-ref-28)
28. Wzór dostępny jest np. tutaj:

<http://pokl.wup.lodz.pl/index.php/component/content/article/1-latest-news/1813-80710> [↑](#footnote-ref-29)
29. Wymienić po kolei nazwy wszystkich przetwarzanych w organizacji zbiorów danych osobowych – np. członków stowarzyszenia; darczyńców; kandydatów do pracy, pracowników; współpracowników; wolontariuszy, praktykantów i stażystów; kandydatów do udziału w projekcie; uczestników projektu etc. [↑](#footnote-ref-30)
30. Pieczęć zawierająca pełną nazwę i kompletne dane teleadresowe [↑](#footnote-ref-31)
31. Pieczęć nagłówkowa organizacji zawierająca pełną nazwę i kompletne dane teleadresowe. [↑](#footnote-ref-32)
32. Wymienić nazwy przetwarzanych zbiorów danych osobowych – np. członków stowarzyszenia; darczyńców; kandydatów do pracy; pracowników; współpracowników; wolontariuszy, praktykantów i stażystów; kandydatów do udziału w projekcie; uczestników projektu etc. [↑](#footnote-ref-33)
33. Dotyczyć to będzie np. postępowań prowadzonych przed GIODO (rejestrowanie zbiorów danych osobowych), udzielania informacji zespołom kontrolującym realizację projektu PO KL w zakresie dotyczącym ochrony danych osobowych. [↑](#footnote-ref-34)
34. Jeśli dotyczy. [↑](#footnote-ref-35)
35. Jeśli dotyczy. [↑](#footnote-ref-36)
36. Wzór upoważnienia uniwersalny dla wszystkich osób przetwarzających dane osobowe w organizacji (niezależny od formy współpracy).

UWAGA!!!

W przypadku przetwarzania danych osobowych uczestników projektów PO KL ABI powinien: prowadzić odrębną ewidencję osób upoważnionych do przetwarzania danych osobowych (na listowniku projektu), upoważnienia do przetwarzania danych osobowych wydawać według wzoru stanowiącego załącznik do umowy o dofinansowanie realizacji konkretnego projektu, odwołania upoważnień do przetwarzania danych osobowych wydawać według wzoru stanowiącego załącznik do umowy o dofinansowanie realizacji konkretnego projektu.

Postępowanie zgodne z tą wskazówką pozwoli – w przypadku prowadzenia kontroli w trakcie realizacji lub po zamknięciu realizacji projektu – przedstawić zespołowi kontrolującemu tylko informacje dotyczące ochrony danych osobowych w tym konkretnym projekcie, bez konieczności ujawniania całości działań organizacji i tego, do jakich danych osobowych przetwarzanych w organizacji ma jeszcze dostęp kadra projektu. [↑](#footnote-ref-37)
37. Dla każdej osoby określić indywidualnie zakres danych osobowych (w ramach zbiorów przetwarzanych
w organizacji), które ta osoba będzie mogła przetwarzać wykonując swoje obowiązki stanowiskowe – np. członków stowarzyszenia; darczyńców; kandydatów do pracy, pracowników; współpracowników; wolontariuszy, praktykantów i stażystów; kandydatów do udziału w projekcie; uczestników projektu etc. [↑](#footnote-ref-38)
38. Data zatrudnienia lub nawiązania współpracy z daną osobą [↑](#footnote-ref-39)
39. Następny dzień roboczy po ustaniu zatrudnienia danej osoby lub zakończeniu z nią współpracy – wynika to z faktu, iż ostatniego dnia zatrudnienia/współpracy dana osoba może jeszcze musieć przetwarzać dane osobowe wykonując swoje obowiązki stanowiskowe [↑](#footnote-ref-40)
40. Zakres tożsamy z tym określonym w załączniku 2 „A” [↑](#footnote-ref-41)
41. Zakres tożsamy z tym określonym w załączniku 2 „B”. [↑](#footnote-ref-42)
42. Wzór odwołania upoważnienia uniwersalny dla wszystkich osób przetwarzających dane osobowe
w organizacji (niezależny od formy współpracy). [↑](#footnote-ref-43)
43. Zakres tożsamy z określonym w załączniku 3. [↑](#footnote-ref-44)