Polityka Bezpieczeństwa
MAŁOPOLSKIEJ IZBY RZEMIOSŁA I PRZEDSIĘBIORCZOŚCI W KRAKOWIE

Spis treści

I. Wprowadzenie

1. Polityka bezpieczeństwa, dalej „Polityka bezpieczeństwa" opisuje procedury zapewnienia bezpieczeństwa danych osobowych w Małopolskiej Izbie Rzemiosła i Przedsiębiorczości w Krakowie zwanej dalej „MIRIP", w tym w szczególności:
- procedury określające sposób zabezpieczenia danych osobowych gromadzonych w postaci dokumentów pisanych;
- procedury określające sposób zabezpieczenia danych osobowych gromadzonych w systemie informatycznych MIRIP, opisane w Instrukcji zarządzania systemem informatycznym;
- organizacyjne i techniczne środki zabezpieczenia danych;
- klauzule informacyjne uwzględniające prawa przysługujące osobom przekazującym dane osobowe MIRIP lub podległym mu podmiotom;
- regulamin wykorzystania systemów monitoringu wizyjnego;
- sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.

2. Polityka bezpieczeństwa określa cele, zakres i sposoby przetwarzania danych osobowych, dostosowując odpowiednie środki techniczne i organizacyjne, z uwzględnieniem potencjalnych ryzyk i jest w szczególności przeznaczona dla pracowników MIRIP przetwarzających dane osobowe.
3. Podstawą prawną Polityki bezpieczeństwa jest:
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE opublikowane w Dzienniku Urzędowym UE L 119.s1, zwane dalej „Rozporządzeniem" lub „RODO";
4. Administratorem danych Osobowych jest Małopolska Izba Rzemiosła i Przedsiębiorczości w Krakowie, 31-008 Kraków, ul. Św. Anny 9, NIP 675-02-00-019, wpisany do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000035593 Administratorem

danych osobowych mogą być również inne instytucje, z którymi MIRIP współpracuje przy realizacji programów finansowanych ze środków Unii Europejskiej.
5. Zgodnie art. 37 RODO Administrator oddzielną decyzją powołuje Inspektora Ochrony Danych. Zadania inspektora ochrony danych zawarte są w art. 39 RODO. Kontakt do Inspektora Ochrony Danych Osobowych będzie podany do publicznej wiadomości, w tym na stronie www MIRIP i na tablicy informacyjnej z dniem powołania.

II. Definicje

Dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej**.**
Zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, czy dostępny jest w formie papierowej czy też elektronicznej.
Administrator - osoba fizyczna lub prawną, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego.
Dane wrażliwe – dane osobowe, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym oraz dotyczące osób skazanych wyrokami sądów, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
Dane genetyczne - dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
Dane biometryczne - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.
Dane dotyczące zdrowia - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.
Strona trzecia - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
Zgoda osoby, której dane dotyczą - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Osoba upoważniona – osoba posiadająca upoważnienie wydane przez administratora danych osobowych lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w danej komórce organizacyjnej w zakresie wskazanym w upoważnieniu.
Użytkownik systemu – osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
Odbiorca - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
Przedstawiciel - osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia.
Przetwarzanie - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
Przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
Ograniczenie przetwarzania - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
Profilowanie - dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się**.**
Pseudonimizacja - przetwarzanie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
Naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
Usuwanie danych osobowych – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

Bezpieczeństwo systemu informatycznego – wdrożenie przez IODO lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
.

III. Postanowienia ogólne

Zbiór danych osobowych przetwarzanych przez Małopolską Izbę Rzemiosła i Przedsiębiorczości wykorzystywany jest do:
1. Wykonywania obsługi biurowej i organizacyjnej organów statutowych MIRIP.
2. Zarządzania danymi pracowników etatowych MIRIP i osób zatrudnionych w ramach umów cywilnoprawnych, zgodnie z odnośnymi uregulowaniami prawa.
3. Przetwarzania danych osobowych związanych z realizacją projektów z udziałem wsparcia finansowego ze środków Unii Europejskiej, zgodnie z zasadami określonymi odrębnymi przepisami odnoszącymi się do poszczególnych „źródeł wsparcia" oraz danych osobowych pozyskiwanych w celu realizacji innych zadań statutowych MIRIP jak działania w obszarze przedsięwzięć szkoleniowo-oświatowych.
4. Zbiory danych osobowych, o których mowa w pkt. 1 – 4, gromadzone są w bazach danych w wersjach papierowych oraz w postaci zapisów elektronicznych z wykorzystaniem systemu informatycznego.
5. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
5.1. Stan przechowywanych dokumentów, urządzeń, zawartość rejestru danego zbioru danych osobowych lub metody pracy mogą wskazywać na naruszenie zabezpieczeń tych danych.
5.2. Stwierdzono naruszenie bezpieczeństwa przetwarzanych danych w rejestrze danego zbioru danych.
6. Polityka bezpieczeństwa obowiązuje wszystkie osoby pracujące przy przetwarzaniu danych osobowych w MIRIP.
7. Wykonywanie postanowień Polityki bezpieczeństwa ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa w danym rejestrze zbioru danych MIRIP.
8. Administrator Danych Osobowych zapewnia:
8.1. Organizację bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych.
8.2. Stosowanie środków technicznych i organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych zapewniających ochronę danych osobowych, a w szczególności:
- zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym;
- zapobieganie przed zabraniam dokumentów przez osobę nieuprawnioną;
- zapobieganie przetwarzaniu danych przez osoby nieupoważnione oraz utracie i uszkodzeniu danych.
8.3. Uwzględnianie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadkach, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych.
8.4. Prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych.
8.5. Nadzór nad bezpieczeństwem danych osobowych, w tym kontrolę działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
8.6. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

8.7. Udzielanie pełnomocnictw do przetwarzania danych osobowych:
- osobom wchodzącym w skład organów organizacji,
- pracownikom,
- współpracownikom,
- wolontariuszom, praktykantom i stażystom,
- pracownikom lub współpracownikom MIRIP w związku z realizacją projektów i zadań,
  w których MIRIP jest lub może być partnerem,
- pracownikom lub współpracownikom instytucji, którym MIRIP powierzy na mocy pisemnej umowy – prowadzenie zadań z zakresu monitoringu i ewaluacji projektu/zadania, którego MIRIP jest realizatorem,
- pracownikom MIRIP w związku z pozostałymi przypadkami przetwarzania danych osobowych w MIRIP,
- innym osobom gdy zajdzie taka uzasadniona potrzeba.

8.8. Udzielanie oraz odwoływanie pełnomocnictw dla Inspektora Ochrony Danych Osobowych oraz – jeśli występuje - dla Administratora Systemu Informatycznego.
8.9. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych
9. Pełnomocnictwa oraz ich odwołanie ma formę pisemną i udzielane są na czas wykonywania przez osobę upoważnioną czynności na powierzonym stanowisku.
10. Wzór pełnomocnictwa do przetwarzania danych osobowych stanowi załącznik nr 1, natomiast Ewidencja osób upoważnionych do przetwarzania danych załącznik nr 2 do Polityki bezpieczeństwa.
11. ADO powołuje Inspektora Ochrony Danych Osobowych (dalej IODO).
12. ADO upoważnia IODO do przetwarzania wszystkich zbiorów danych osobowych zewidencjonowanych w „Rejestrze przetwarzania zbiorów danych osobowych MIRIP.
13. IODO prowadzi postępowania wyjaśniające w przypadku naruszenia ochrony danych osobowych, we współdziałaniu z ADO sprawuje nadzór nad bezpieczeństwem danych osobowych, w szczególności kontroluje działania komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
14. IODO inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych.

IV. Zabezpieczenie dostępu do danych osobowych

Zabezpieczenia organizacyjne

1. Zabezpieczenia organizacyjne stanowią procedury określone w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym.
2. Powołanie IODO i udzielenie IODO odpowiedniego pełnomocnictwa do działania.
3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych, bądź osobę przez niego upoważnioną.
4. Każdy pracownik posiadający dostęp do danych osobowych przechowywanych w wersji papierowej oraz w wersji elektronicznej składa oświadczenie na piśmie zawierające świadome zobowiązanie do przestrzegania zasad gromadzenia, przechowywania i przetwarzania danych osobowych w sposób zgodny z przepisami prawa i niniejszej Polityki bezpieczeństwa. Wzór oświadczenia pracownika stanowi załącznik Nr 3 do Polityki bezpieczeństwa.
4. Dane osobowe przetwarza się na przystosowanych do tego stanowiskach pracy według zasad określonych w Polityce bezpieczeństwa.

5. Opracowano procedurę postępowania w sytuacji naruszenia ochrony danych osobowych.
6. Osoby przetwarzające dane osobowe w trakcie wykonywania powierzonych im zadań zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie potrzeby przestrzegania bezpieczeństwa w trakcie pracy w systemie informatycznym MIRIP.
7. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.
8. Przetwarzanie danych osobowych dokonywane jest w warunkach chroniących je przed dostępem osób nieupoważnionych.
9. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
10. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
11. Wprowadzono zasadę „czystego biurka" i „białej kartki".
12. Wprowadzono zasady korzystania z poczty elektronicznej.
13. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła;
14. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
15. Nie udziela się informacji zawierających dane osobowe przez telefon, względnie udziela się je po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych.
16. Kontrola dostępu do pomieszczeń przeznaczonych do przetwarzania danych osobowych.

Zabezpieczenia danych osobowych przechowywanych w postaci papierowej

1. Szafy i urządzenia służące do przetwarzania danych osobowych i dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach.
2. Dane osobowe przetwarzane w formie papierowej przechowuje się w zamykanych szafach metalowych i niemetalowych wyposażonych w zamki uniemożliwiające dostęp osób niepowołanych, do których wydawane są za pokwitowaniem pojedyncze egzemplarze kluczy.
3. Jednostkami zbiorów danych osobowych gromadzonych i przetwarzanych w wersji papierowej są:
3.1. Segregatory zawierające teczki i podteczki, w których gromadzone są oryginalne dokumenty w formie kart papierowych;
3.2. Rejestry w postaci druku zwartego, introligowane w sposób uniemożliwiający usuwanie poszczególnych kart, z których każda jest oznaczona kolejnym numerem stanowiącym liczbę naturalną.
4. Pomieszczenia, w których zlokalizowane są szafy zamykane są na zamki, do których klucze wydawane są za pokwitowaniem odbioru osobom uprawnionym przez portiera w recepcji budynku.
5. Osoby dysponujące kluczami do szaf oraz do pomieszczeń obowiązane są do korzystania z dokumentów z wyłączeniem osób niepowołanych oraz ponoszą z tego tytułu odpowiedzialność służbową.
6. Zapasowe komplety kluczy do pomieszczeń przechowywane są w kasie pancernej Biura Techniczno-Administracyjnego, ruch kluczy zapasowych podlega kontroli przez Dyrektora Biura Techniczno-Administracyjnego.
7. Wykaz pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych wraz z wykazem pracowników upoważnionych do odbierania kluczy stanowi załącznik nr. 4 do Polityki bezpieczeństwa.
8. Obszar, na którym przetwarzane są dane osobowe, chroniony jest poprzez zastosowanie:

monitoringu wizyjnego.

Zabezpieczenia sieci komputerowej

1. Wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą urządzeń zabezpieczających, w tym kanałami dostępu VPN.
2. Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową i firewall.
3. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji.
4. Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika;
5. Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła;
6. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i 8 cyfrowego hasła minimalizując ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
7. Stosuje się zapisywanie danych w back-upach przechowywanych w zabezpieczonych szafach kierowników komórek organizacyjnych
8. W sytuacji braku aktywności trwającej ponad 5 minut następuje automatyczne blokowanie dostępu do komputera.
9. Dane osobowe przetwarzane są w systemach informatycznych COMARCH i PŁATNIK obsługiwanych przez pracowników Zespołu Księgowego, i Dyrektora. System wymusza zmianę hasła dostępu, co 90 dni. Dostęp do systemu mają wyłącznie upoważnieni pracownicy Zespołu Księgowego oraz Dyrektor MIRIP na podstawie imiennie wystawionych upoważnień.
10. Przelewy bankowe i międzybankowe – strony internetowe banków, w których MIRIP posiada rachunki wymagają podania loginu i hasła, a każda osoba upoważniona do dokonywania przelewów posiada indywidualny klucz dostępu, co daje gwarancję zachowania poufności danych, a także ogranicza krąg osób upoważnionych do obsługi (Dyrektor, Główny Księgowy).
11. Instrukcja zarządzania systemem informatycznym obejmująca rejestr zbiorów danych osobowych ze wskazaniem programu informatycznego do ich przetwarzania stanowi załącznik nr 5 do Polityki bezpieczeństwa.

V. Wykaz zbiorów danych osobowych stosowanych do przetwarzania danych.

W Małopolskiej Izbie Rzemiosła i Przedsiębiorczości przetwarza się dane osobowe gromadzone w następujących zbiorach i rejestrach:

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych w następujących polach: imię i nazwisko, telefon. Dane przetwarzane są w formie elektronicznej i papierowej.
2. Akta osobowe pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
3. Zbiory informacji o pracownikach, oświadczenia na potrzeby ZFŚS, w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie papierowej.
4. Ewidencja zwolnień lekarskich w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.

5. Skierowania na badania okresowe w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
6. Ewidencja urlopów, czasu pracy i wyjść w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
7. Rejestr delegacji służbowych w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie i papierowej.
8. Listy płac pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
9. Deklaracje ubezpieczeniowe pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
10. Deklaracje i kartoteki ZUS pracowników w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
11. Deklaracje podatkowe pracowników, w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
12. Rejestr wypadków w następujących polach: imię i nazwisko, adres zamieszkania, telefon, email. Dane przetwarzane są w formie papierowej.
13. Rejestr umów najmu z najemcami w następujących polach: podmiot, imię i nazwisko osób reprezentujących, adres siedziby, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej.
14. Rejestr umów z innymi podmiotami zewnętrznymi /kontrahentami/ w następujących polach: podmiot, NIP, imię i nazwisko osób reprezentujących, adres siedziby, telefon, email. Dane przetwarzane są w formie elektronicznej i papierowej. Rejestr dostawców i odbiorców usług.
15. Rejestr czynności przetwarzania danych osobowych. Dane przetwarzane są w formie elektronicznej.
16. Rejestr członków MIRIP w następujących polach: nazwa organizacji, adres, telefon kontaktowy, adres email. Dane przetwarzane są w formie papierowej i elektronicznej.
Dane przetwarzane są w formie papierowej i elektronicznej.
17. Rejestr Delegatów na Walne Zebranie Delegatów w następujących polach: nazwa organizacji, imię i nazwisko delegata, data urodzenia, adres zamieszkania, adres zakładu pracy, telefon, wykształcenie. Dane przetwarzane są w wersji papierowej i elektronicznej.
18. Pocztowa książka nadawcza w następujących polach: adresat instytucja, imię i nazwisko, adres miejsca doręczenia. Dane przetwarzane są w wersji papierowej.
19. Rejestr wniosków o wydanie duplikatu świadectwa (bez rejestru) w następujących polach: imię i nazwisko, data i miejsce urodzenia, PESEL, adres zamieszkania, dane świadectwa /nr księgi wieczystej, data wydania/. Dane przetwarzane są w wersji elektronicznej i papierowej.
20. Rejestr odznaczeń w następujących polach: organizacja, imię i nazwisko, przyznane odznaczenia, data przyznania), imiona rodziców, data i miejsce urodzenia, miejsce zamieszkania, wykonywane rzemiosło lub zawód, miejsce zatrudnienia, okresy członkostwa w organizacjach, pełnione funkcje samorządowe, przyznane odznaczenia. Dane przetwarzane są w wersji papierowej i elektronicznej.
21. Rejestr byłych i obecnych pracowników, osób zatrudnionych na umowy cywilnoprawne i innych osób współpracujących w następujących polach: imię i nazwisko, PESEL, NIP, data urodzenia, miejsce urodzenia, adres zameldowania, adres zamieszkania, adres do korespondencji, telefon, adres e-mail, nr rachunku bankowego. Dane przetwarzane są w formie papierowej i elektronicznej.
22. Rejestr byłych i obecnych pracowników, osób zatrudnionych na umowy cywilnoprawne i innych osób współpracujących w następujących polach: imię i nazwisko, PESEL, seria i nr dowodu osobistego, data urodzenia, miejsce urodzenia, adres zameldowania, adres

zamieszkania, adres do korespondencji, telefon, adres e-mail. Dane przetwarzane są w formie papierowej i elektronicznej.
23. Rejestr – Archiwum obejmujący dokumentację archiwalną zlikwidowanych organizacji rzemieślniczych, akta osobowe pracowników, dokumentacja kadrowo - płacowa (wersja papierowa), zbiory danych osobowych uczestników projektów realizowanych przez organizację współfinansowanych ze środków Unii Europejskiej.
24. Wykaz zbiorów danych osobowych znajduje się w załączniku nr 6 do Polityki bezpieczeństwa. Załącznik jest aktualizowany w momencie wprowadzaniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują.

VI. Opis zdarzeń naruszających ochronę danych osobowych

1. Klasyfikacja zagrożeń:
1.1. 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.
1.2. 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.
1.3. Zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych – zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy.
2. Zagrożenia te podzielić na zagrożenia spowodowane:
- nieuprawnionym dostępem do systemu z zewnątrz (włamanie do systemu),
- nieuprawnionym dostępem do systemu od wewnątrz,
- nieuprawnionym przekazem danych,
- pogorszeniem jakości sprzętu i oprogramowania,
- bezpośrednim zagrożeniem materialnych składników systemu.

3. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to:
- 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.;
- niekorzystne parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż;
- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
- naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
- stwierdzona próba modyfikacji lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- niedopuszczalna manipulacja danymi osobowymi w systemie;
- ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą

procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;

- 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.;
- istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki" itp.;
- podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;
- 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.).

4. 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, nośnikach elektronicznych w formie niezabezpieczonej itp.

VII. Zasady postępowania w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik biorący udział w przetwarzaniu danych osobowych jest odpowiedzialny za bezpieczeństwo tych danych w przypadku stwierdzenia:
- naruszenia zabezpieczeń systemu informatycznego,
- naruszenia technicznego stanu urządzeń,
- naruszenia zawartości zbioru danych osobowych,
- ujawnienia metody pracy lub sposobu działania programu,
- pogorszenia 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 IODO.

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

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

3.1. Niezwłocznie – o ile istnieje taka możliwość – podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia oraz ustalić przyczyny lub sprawców naruszenia danych osobowych.

3.2. Udokumentować wstępnie zaistniałe naruszenie

3.3. Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IODO lub osoby przez niego upoważnionej.

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

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

4.2. Żąda zdania 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.
4.3. Rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych ADO.
4.4. Jeżeli zachodzi taka potrzeba nawiązuje bezpośredni kontakt ze specjalistami spoza organizacji.
5. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, IODO zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
6. IODO dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:
- wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;
- określenie czasu i miejsca naruszenia/ujawnienia i powiadomienia o tym fakcie;
- określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
- wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
7. Raport, o którym mowa w pkt. 6, IODO niezwłocznie przekazuje ADO. Wzór raportu stanowi załącznik nr 7 do „Polityki bezpieczeństwa".
8. Zaistniałe naruszenie/ujawnienie ochrony danych osobowych może stać się przedmiotem szczegółowej analizy prowadzonej przez ADO i IODO.
9. Analiza, o której mowa w pkt. 8, powinna zawierać:
- wszechstronną ocenę zaistniałego naruszenia/ujawnienia ochrony danych osobowych;
- wskazanie odpowiedzialnych;
- wnioski co do ewentualnych przedsięwzięć: proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom/ujawnieniom w przyszłości.

10. Wzór analizy naruszenia ochrony danych osobowych stanowi załącznik nr 8 do Polityki Bezpieczeństwa
11. Po dokonaniu czynności sprawdzających oraz po przeprowadzeniu analizy naruszenia danych osobowych, sporządza się protokół stanowiący podstawę do wprowadzenia zabezpieczeń technicznych i organizacyjnych mających zapobiec podobnym naruszeniom w przyszłości.

VIII. Instrukcja w sprawie zasad postępowania przy przetwarzaniu danych osobowych

1. IODO 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.
2. IODO i ADO współpracują ze sobą przy realizacji zadań z zakresu ochrony danych osobowych.
3. Do zadań IODO należy zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

3.1. Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO.
3.2. Nadzorowanie opracowania i aktualizacji dokumentacji dotyczącej Polityki bezpieczeństwa danych osobowych w MIRIP.
3.3. Zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
3.4. Prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez ADO;
3.5. Kontrolę wykonywania operacji przetwarzania danych osobowych przez osoby upoważnione.
3.6. Zwracanie się do ADO w przypadku istotnych wątpliwości wynikających ze stosowania przepisów ustawy o ochronie danych osobowych oraz przepisów wykonawczych.
3.7. Niezwłoczne poinformowanie ADO o zaprzestaniu wykonywania czynności przetwarzania danych osobowych przez osobę upoważnioną.
4. Osoba upoważniona do przetwarzania danych zobowiązana jest do:
4.1. Zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych.
4.2. Zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą.
4.3. Stosowania określonych przez ADO procedur i środków przetwarzania oraz zabezpieczania danych osobowych.
4.4. Podporządkowania się poleceniom IODO i ADO w zakresie ochrony danych osobowych,
4.5. Zachowania danych osobowych w tajemnicy.
4.6. Przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, a w szczególności:
- zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem,
- zabezpieczenia danych osobowych przed ich zmianą,
- zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
- zamykania i zabezpieczania pomieszczeń, w których przetwarzane są dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,
- dopilnowania, by przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej,
- dopilnowania, by przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie,
- przetwarzania, udostępniania danych osobowych zgodnie z celem, dla którego zostały zebrane.

5. Każda osoba upoważniona powinna odbyć szkolenie z zakresu ochrony danych osobowych. Szkolenie z zakresu ochrony danych osobowych organizuje IODO.
6. Rejestr zbiorów danych osobowych przetwarzanych w organizacji prowadzony jest w formie papierowej i/lub elektronicznej przez IODO.

IX. Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

1. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) jednak wymaga to zgody indywidualnej IODO.
2. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się

wyłącznie za zgodą ADO w MIRIP i za wiedzą IODO. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony pracownika za wiedzą i zgodą IODO.

3. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. Użytkownik komputera przenośnego zobowiązany jest do:

- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
- transportowania komputera w bagażu podręcznym, nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp., zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych;
- korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego;
- nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe;
- zabezpieczania komputera przenośnego hasłem;
- blokowanie dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika;
- kopiowanie danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych;
- bieżącą aktualizację baz wirusowych programu antywirusowego zainstalowanego na komputerze przenośnym;
- utrzymanie konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł;
- wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe;
- zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

4. IODO zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:

4.1. Dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe,

4.2. Zabezpieczono dane osobowe przetwarzane na komputerach przenośnych poprzez zastosowanie oprogramowania szyfrującego te dane. Dostęp do danych jest możliwy wyłącznie po podaniu tego hasła.

4.3. Dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerach przenośnych.

4.4. Przeprowadzono aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

5. IODO jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych.

6. W razie zgubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia ABI lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

X. Przetwarzanie danych osobowych powierzonych MIRIP przez inne podmioty

1. Możliwe jest powierzenie przetwarzania danych podmiotowi zewnętrznemu (Procesor). Wzór umowy powierzenia stanowi załącznik nr 12 do Polityki bezpieczeństwa.
2. Wykaz podmiotów, którym powierzono przetwarzanie danych stanowi załącznik nr 9, natomiast wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 10 do Polityki bezpieczeństwa.
3. Możliwe jest przetwarzanie w MIRIP danych osobowych powierzonych MIRIP przez inny podmiot (Zleceniodawcę). W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie umowy między MIRIP a Zleceniodawcą zawartej w formie pisemnej. Umowa ta musi zawierać ściśle określony zakres przetwarzanych danych. Przetwarzanie danych możliwe jest tylko w ustalonym przez umowę zakresie. Zawarcie umowy następuje w formie pisemnej poprzez złożenie podpisu na formularzy wykonania usługi informacyjnej, notatce z pierwszego spotkania z klientem lub podpisanie odrębnej umowy dot. przetwarzania danych osobowych.
4. Powierzone dane podlegają ochronie na takich samych zasadach jak dane będące własnością MIRIP, chyba, że umowa określi inne zasady ochrony danych osobowych. W szczególności może dotyczyć to nadawania uprawnień do przetwarzania danych osobowych.
5. Dostęp do powierzonych danych osobowych z sieci zewnętrznej (np. siedziby Zleceniodawcy) musi odbywać się z zachowaniem odpowiednich zabezpieczeń. W przypadku danych elektronicznych, dostęp do nich musi być chroniony identyfikatorem oraz hasłem, a połączenie sieciowe realizujące dostęp do danych musi być odpowiednio szyfrowane.
6. W przypadku przetwarzania danych związanych z obsługą projektów UE, administratorem danych jest również instytucja pośrednicząca, zarządzająca lub wdrażająca dany program unijny. Dane przetwarzane są na podstawie odrębnych umów.

XI. Wykaz budynków i pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

Wykaz budynków i pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych spełniających wymogi Rozporządzenia RODO stanowi załącznik Nr 4 do Polityki bezpieczeństwa

XII. Postanowienia końcowe

1. Wdrożenie Polityki bezpieczeństwa odbywa się poprzez przeszkolenie osób wchodzących w skład organów organizacji, pracowników, współpracowników, praktykantów i stażystów organizacji z zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, treścią Polityki bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u Administratora danych osobowych.
2. Za przeprowadzenie szkolenia odpowiada IODO.
3. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im upoważnień do przetwarzania danych osobowych..
4. Ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, zobowiązany jest prowadzić IODO. Wzór ewidencji stanowi załącznik nr 11 do „Polityki bezpieczeństwa”.

5. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce bezpieczeństwa i innych zwanych z nią dokumentach.
6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w RODO, ustawie i dokumentach wewnętrznych Organizacji, można wszcząć postępowanie dyscyplinarne.
7. Kara dyscyplinarna orzeczona wobec osoby winnej naruszenia zabezpieczeń systemu informatycznego i uchylającej się od powiadomienia ADO lub IODO nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
9. Polityka bezpieczeństwa wchodzi w życie z dniem podpisania przez Prezesa Zarządu MIRIP, przy czym dokument ten wymaga zatwierdzenia uchwałą Zarządu MIRIP.
10. W sprawach nieuregulowanych w Polityce bezpieczeństwa mają zastosowanie przepisy RODO i ustawy o ochronie danych osobowych.
11. Integralną część dokumentu stanowią załączniki:

Nr 1 Wzór pełnomocnictwa do przetwarzania danych osobowych
Nr 2 Ewidencja osób upoważnionych do przetwarzania danych osobowych
Nr 3 Wzór oświadczenia pracownika z zobowiązaniem do przestrzegania zasad gromadzenia, przechowywania i przetwarzania danych osobowych
Nr. 4 Wykaz budynków i pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych z wykazem pracowników upoważnionych do odbierania kluczy.
Nr 5 Instrukcja zarządzania systemem informatycznym obejmująca Rejestr zbiorów danych osobowych ze wskazaniem programu informatycznego do ich przetwarzania
Nr 6 Wykaz zbiorów danych osobowych wykorzystywanych w przetwarzaniu danych osobowych.
Nr 7 Wzór raportu z naruszenia ochrony danych osobowych.
Nr 8 Wzór analizy naruszenia ochrony danych osobowych.
Nr 9 Wzór umowy powierzenia przetwarzania danych
Nr 10 Wykaz podmiotów, którym powierzono przetwarzanie danych
Nr 11 Wzór ewidencji osób które zapoznały się z Polityką bezpieczeństwa