

**POLITYKA
BEZPIECZEŃSTWA
DANYCH OSOBOWYCH
W
W FIRMIE
MIROŚŁAWA BANDYK
PROWADZĄCEGO DZIAŁALNOŚĆ
GOSPODARCZĄ
POD NAZWĄ
BUD MI-K F.R.B.
W WIELICZCE**

data sporządzenia 24.05.2018 r.

obowiązuje od 25.05.2018 r.

Niniejsza Polityka Bezpieczeństwa Danych Osobowych, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

SPIS TREŚCI

I. Wykaz podstawowych skrótów	4
II. Wykaz podstawowych definicji	4
III. Wprowadzenie	7
IV. Cele Polityki Bezpieczeństwa Danych Osobowych	8
V. Zakres rozpowszechnienia Polityki Bezpieczeństwa Danych Osobowych	9
VI. Osoby upoważnione do przetwarzania danych osobowych	9
VII. Podstawowe zasady ochrony danych osobowych	10
VIII. Powierzenie przetwarzania danych osobowych	12
IX. Udostępnianie danych osobowych	12
X. Przekazywanie danych osobowych poza Polskę	13
XI. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	13
XII. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	14
XIII. Opis sposobu przepływu danych pomiędzy poszczególnymi systemami	14
XIV. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	14
XV. Zarządzanie incydentami bezpieczeństwa danych osobowych	15

XVI. Postanowienia końcowe.....15

XVII. Załączniki16

I. WYKAZ PODSTAWOWYCH SKRÓTÓW

ADO – Administrator Danych Osobowych

ASI – Administrator Systemów Informatycznych

IOD – Inspektor Ochrony Danych

SI – System Informatyczny

PBDO – Polityka Bezpieczeństwa Danych Osobowych

IZSI - Instrukcja Zarządzania Systemem Informatycznym

RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

II. WYKAZ PODSTAWOWYCH DEFINICJI

Administrator Danych Osobowych (ADO) – osoba fizyczna lub prawną, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, w niniejszej Polityce Bezpieczeństwa Danych Osobowych ADO to Mirosław Bandyk, prowadzący działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce, Siercza nr 441.

Administrator Systemu Informatycznego (ASI) – pracownik ADO, inna osoba lub podmiot zewnętrzny odpowiedzialni za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

Inspektor Ochrony Danych (IOD) – osoba odpowiedzialna za bieżący nadzór stosowania przepisów dotyczących ochrony danych osobowych;

Osoba upoważniona (użytkownik) – osoba upoważniona przez ADO do przetwarzania danych osobowych, pracownik Spółki, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż;

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Możliwa do zidentyfikowania osoba fizyczna - 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 osobowych – uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony lub podzielony funkcjonalnie lub geograficznie;

Przetwarzanie danych osobowych – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, w szczególności takie 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, a zwłaszcza te, które wykonuje się w systemach informatycznych;

Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;

Odbiorca danych - 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 odpowiednio do celów przetwarzania;

Bezpieczeństwo danych osobowych – zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał ich poufność, integralność oraz dostępność;

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

Dostępność danych – właściwość zapewniająca, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;

Rozliczalność danych – właściwość zapewniająca, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie przetwarzania danych osobowych w takim systemie

Hasło – ciąg znaków literowych, cyfrowych lub innych znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

Naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa danych osobowych 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.

Incydent – naruszenie bezpieczeństwa danych osobowych ze względu na poufność, dostępność i integralność;

Zagrożenie - potencjalna możliwość wystąpienia incydentu;

Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych;

Państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego;

III. WPROWADZENIE

1. Polityka Bezpieczeństwa Danych Osobowych (PBDO) określa reguły przetwarzania danych osobowych oraz sposoby ich zabezpieczenia, określając zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce. PBDO zawiera w szczególności informacje dotyczące rozpoznawania procesów przetwarzania

danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

2. PBDO dotyczy wszystkich Danych Przetwarzanych w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce, niezależnie od formy ich przetwarzania (przetwarzane tradycyjne zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.

3. PBDO jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie ADO.

4. PBDO jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych celem zapoznania się z jej treścią.

5. ADO zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa, w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

IV. CELE POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Celem Polityki Bezpieczeństwa Danych Osobowych (PBDO) jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce, a w szczególności:

- a) zapewnienie spełnienia wymagań prawnych, określonych obowiązującymi przepisami;
- b) zapewnienie poufności, integralności, dostępności oraz rozliczalności danych osobowych przetwarzanych w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce;
- c) podnoszenie świadomości osób przetwarzających dane osobowe w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K

F.R.B. w Wieliczce;

d) zaangażowanie osób przetwarzających dane osobowe w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce w ochronę tych danych.

2. Dla skutecznej realizacji PBDO ADO zapewnia:

a) odpowiednie do zagrożeń i kategorii danych osobowych objętych ochroną środki techniczne i rozwiązania organizacyjne;

b) kontrolę i nadzór nad przetwarzaniem danych osobowych;

c) monitorowanie i kontrolę zastosowanych środków ochrony;

3. Monitorowanie przez ADO zastosowanych środków ochrony obejmuje, w szczególności działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi i wewnętrznymi.

V. ZAKRES ROZPOWSZECHNIANIA POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Z treścią niniejszej Polityki Bezpieczeństwa Danych Osobowych powinny zapoznać się wszystkie podmioty przetwarzające dane osobowe w imieniu Administratora Danych Osobowych.

VI. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH (UŻYTKOWNICY)

1. Do obowiązków osób upoważnionych do przetwarzania danych osobowych (użytkowników) należy:

a) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa Danych Osobowych (PBDO) i Instrukcji Zarządzania Systemami Informatycznymi (IZSI);

b) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych (ADO) w pisemnym upoważnieniu i tylko w

- celu wykonywania nałożonych obowiązków, w szczególności obowiązków służbowych;
- c) niezwłoczne informowanie odpowiednich organów o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce;
 - d) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
 - e) korzystanie z systemów informatycznych w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
 - f) bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
 - g) zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.
2. Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez ADO (*Załącznik nr 1 – wzór upoważnienia*) oraz złożyły stosowne oświadczenie dotyczące właściwej realizacji przepisów RODO (*Załącznik nr 2 – wzór oświadczenia*).
3. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

VII. PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

1. Dane osobowe w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce, przetwarzać należy zgodnie z obowiązującymi przepisami prawa.

2. Wobec osób, których dane osobowe podlegają przetwarzaniu należy spełnić obowiązek informacyjny wynikający z przepisów RODO.

3. Zgromadzone dane osobowe mogą być przetwarzane jedynie dla oznaczonych i zgodnych z prawem celów i nie mogą być poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

4. Przetwarzanie danych osobowych odbywa się zgodnie z zasadami merytorycznej poprawności oraz adekwatności celów w jakich dane te zostały zebrane.

5. Dane osobowe w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce mogą być przetwarzane nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.

6. Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce.

7. Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonymi postępowaniami, zgodnie z obowiązującymi w tym zakresie przepisami.

8. Przetwarzanie danych osobowych w firmie Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce może odbywać się zarówno w systemach zautomatyzowanych, w szczególności w systemach informatycznych, jak i w systemach niezautomatyzowanych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

9. W zakresie danych osobowych przetwarzanych w systemach niezautomatyzowanych (innych niż informatyczne) obowiązują również dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczeniu dokumentów służbowych.

10. Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

VIII. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych (ADO) może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi w obowiązujących w tym zakresie przepisach, w szczególności RODO, a zwłaszcza art. 28 RODO, a także jedynie w celu realizacji określonego zadania.

2. Przed powierzeniem przetwarzania danych osobowych ADO w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

3. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

IX. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Dane osobowe udostępnia się na wniosek.

2. Wniosek o udostępnienie danych, który wpłynął do firmy Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce rozpatruje właściciel zbioru danych osobowych.

3. Informacje, zawierające dane osobowe są udostępniane uprawnionym podmiotom:

- a) w formie wydruku listem poleconym lub za potwierdzeniem osobistego odbioru,
- b) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych),
- c) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru,
- d) w inny sposób określony przepisami prawa lub umową.

4. Udostępniane dane osobowe podlegają kontroli przez właściciela zbioru danych osobowych, z którego one pochodzą.

5. Ewidencja przypadków udostępnienia danych prowadzona jest przez właściciela zbioru danych osobowych, w wersji elektronicznej lub papierowej.

X. PRZEKAZYWANIE DANYCH OSOBOWYCH POZA POLSKĘ

1. Administrator Danych Osobowych może przekazywać dane osobowe do:
 - a) państw Europejskiego Obszaru Gospodarczego;
 - b) pozostałych państw (państwa trzecie).
2. Przekazywanie danych osobowych w ramach EOG traktuje się tak, jakby były przetwarzane na terenie Polski.
3. W przypadku przekazywania danych osobowych do państwa trzeciego, przekazywanie następuje zgodnie z obowiązującymi w tym zakresie przepisami, w szczególności treścią rozdziału V, art. 44 – 49 RODO.

XI. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Obszar, w którym przetwarzane są dane osobowe na terenie firmy Mirosława Bandyk, prowadzącego działalność gospodarczą pod nazwą BUD MI-K F.R.B. w Wieliczce obejmuje:
 - pomieszczenie biurowe zlokalizowane w Wieliczce, Siercza nr 441;
 - komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.
2. Administrator Danych Osobowych prowadzi aktualny wykaz obszarów przetwarzania danych osobowych.

XII. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH.

Administrator Danych Osobowych prowadzi aktualny wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

XIII. OPIS SPOSOBU PRZEPIYU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI.

Administrator Danych Osobowych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis sposobu przepływu danych pomiędzy poszczególnymi systemami.

XIV. OKREŚLENIE ŚRODKÓW TECHNICZNYCH i ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH.

1. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem. W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

2. Administrator Danych Osobowych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

XV. ZARZĄDZANIE INCYDENTAMI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W przypadku incydentu bezpieczeństwa danych osobowych, Administrator Danych Osobowych podejmuje decyzję o ewentualnych działaniach związanych ze zgłoszeniem incydentu do odpowiednich organów.

XVI. POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.

3. Integralną część niniejszej Polityki bezpieczeństwa stanowi Załączniki.

XVII. ZAŁĄCZNIKI

- 1) wzór upoważnienia do przetwarzania danych osobowych;
- 2) wzór oświadczenia dotyczącego prawidłowej realizacji przepisów RODO;

Mirosław Bandyk

.....
Administrator Danych Osobowych