**OGÓLNE PROCEDURY POLITYKI BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH OBOWIĄZUJĄCE W FUNDACJI MUUVE W BIELSKU-BAŁEJ.**

**1. Przetwarzanie danych osobowych podlega ochronie w oparciu o:**

1) Od dnia 25 maja 2018 roku- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 Rodzporządzenie o Ochronie Danych ) (RODO).

2) Do dnia 24 maja 2018 roku : - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3.06.1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia Inspektora Ochrony Danych Osobowych (Dz. U. z 1998r., Nr 80, poz. 522 ze zm.),

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych ( Dz. U. z 2004r., Nr 100, poz. 1024),

- Art. 221 §1 - 5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity Dz. U. z 1998 r. Nr 21, poz.94 ze zm.) i przepisów wykonawczych z nią związanych,

**2. PODSTAWOWE DEFINICJE Z ZAKRESU OCHRONY DANYCH OSOBOWYCH**

W dokumencie przyjmuje się następującą terminologię:

**Urząd Ochrony Danych Osobowych** – organ do spraw ochrony danych osobowych.

**Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej 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. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

**Dane wrażliwe** - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

**Administrator danych (ADO**) – organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. ADO w przypadku tej procedury jest Fundacja Muuve, reprezentowane przez Zarząd.

**Inspektor Ochrony Danych Osobowych (IDO**) – osoba nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną. Fundacja nie ma obowiązku powołania

**Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Przetwarzanie danych - 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.

**System informatyczny -** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

**Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

**Zgoda osoby, której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

**Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

**Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

**Uwierzytelnianie –** działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

**Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

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

**Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

**3. NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH**

***3.1 URZĄD OCHRONY DANYCH OSOBOWYCH*** (PRZED 25 MAJA 2018 ROKU GIODO)

***Zadania UODO. Do zadań UODO należy:***

-kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

- wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,

- prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach,

- opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,

- inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,

- uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

***Kontrole GIODO.***

W celu wykonania w/w zadań Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura, zwani dalej „inspektorami”, mają prawo:

- wstępu, w godzinach od 6°° do 22°°, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,

- żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,

- wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,

- przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,

- zlecać sporządzanie ekspertyz i opinii.

 ***Działania GIODO w przypadku naruszenie przepisów.***

 W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

- usunięcie uchybień, uzupełnienie,

- uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,

- zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,

- wstrzymanie przekazywania danych osobowych do państwa trzeciego,

- zabezpieczenie danych lub przekazanie ich innym podmiotom,

- usunięcie danych osobowych.

W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie

***3.2 PRZETWARZANIE DANYCH***

Przetwarzanie danych jest dopuszczalne tylko wtedy gdy:

- Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana.

- Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwie, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.

- Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.

- Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

- Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Przetwarzanie danych jest zabronione w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących wskazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie tych danych jest jednak dopuszczalne, jeżeli:

- osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,

- przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,

- przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

- jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,

-przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

- przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

- przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

- przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

- jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

- przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

***3.3 OBOWIĄZKI INFORMACYJNE O PRZETWARZANIU DANYCH***

 ***Zbieranie danych osobowych od osób, których dane dotyczą.***

W przypadku zbierania danych od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,

- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

- prawie dostępu do treści swoich danych oraz ich poprawiania, dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

***Zbieranie danych osobowych nie od osób, których dane dotyczą.***

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,

- źródle danych,

- prawie dostępu do treści swoich danych oraz ich poprawiania,

- prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

- prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy Administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Podanych wyżej zasad nie stosuje się, jeżeli:

- dane są przetwarzane przez administratora na podstawie przepisów prawa,

- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,

- dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej,

- ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

 ***3.4 OBOWIĄZEK ZGŁOSZENIA PRZETWARZANIA DANYCH PRZED 25 MAJA 2018 ROKU.***

Administrator danych jest obowiązany zgłosić zbiory danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz zgłaszać zmiany w terminie 30 dni.

Zgłoszenie powinno zawierać:

- wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,

- oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru,

- cel przetwarzania danych, w tym opis kategorii osób, których dane dotyczą oraz zakres przetwarzanych danych,

- sposób zbierania oraz udostępniania danych, w tym informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane, opis środków technicznych i organizacyjnych zastosowanych w celach ochrony danych,

- informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w dokumentacji ochrony danych osobowych, informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

***Z obowiązku rejestracji zwolnieni są Administratorzy danych***:

- objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa,

- ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,

- przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym oraz przetwarzanych przez Generalnego Inspektora Informacji Finansowej, a także przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej,

- dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,

- przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,

- dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,

- tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na Urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego,

- dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,

- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,

- powszechnie dostępnych,

- przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,

- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

**3.5 UDOSTĘPNIANE DANYCH**

Najważniejsze przesłanki i zasady udostępniania danych:

 - Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.

- Nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.

- Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.

- Dane osobowe, z wyłączeniem danych wrażliwych, mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

- Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.

- 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.

***3.6 POWIERZENIE PRZETWARZANIA DANYCH***

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora danych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

- umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron, -

- Podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie,

- Podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy oraz spełnić wymagania określone w przepisach, o których mowa w art.39a ustawy.

- W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych,

- odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na Administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową

- Do kontroli zgodności przetwarzania danych przez podmiot, któremu powierzono przetwarzanie danych, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19 ustawy.

***3.7 DOKUMENTOWANIE***

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Ponadto, Administrator danych:

- prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki organizacyjne i techniczne służące ochronie danych,
- wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony chyba, że sam wykonuje te czynności,

- nadaje upoważnienia do przetwarzania danych i dopuszcza do pracy wyłącznie osoby posiadające takie upoważnienie,

-zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,

- prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji opisującej ochronę danych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

***3.8 SANKCJE KARNE***

Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Jeżeli czyn ten dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonych w niniejszej dokumentacji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Orzeczona kara dyscyplinarna nie wyklucza odpowiedzialności karnej osoby winnej zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, póz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat

 **4. USTALENIA WSTĘPNE**

**4.1** Fundacja, z uwagi na skalę i rodzaj przetwarzania danych osobowych, nie jest obowiązana do powoływania Inspektora Ochrony Danych Osobowych.

4.2 Zarząd Fundacji jest świadomy zagrożeń związanych z przetwarzaniem danych w szczególności wynikających z dynamicznego rozwoju metod i technik przetwarzania danych w systemach informatycznych oraz sieciach telekomunikacyjnych.

Zarząd Fundacji zamierza doskonalić i rozwijać nowoczesne metody przetwarzania danych w celu skutecznego zapobiegania zagrożeniom wykradania zasobów komputerowych:

 a) związanych z: wirusami, spamami, stronami i komunikatorami internetowymi,

b) użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku poza Fundację,

c) możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki,

 d) możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane,

e) lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia,

f) brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy,

g) atakami z sieci uniemożliwiającymi przetwarzanie,

h) kradzieżą sprzętu lub nośników z danymi,

i) przekazywaniem sprzętu z danymi do serwisu,

j) innym możliwym zagrożeniom.

**5. ZAGROŻENIA BEZPIECZEŃSTWA**

***5.1. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ***

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

**- zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych,

**- zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

**5.2. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA**

- Przełamane zabezpieczenia tradycyjnych – zerwane plomby na drzwiach, szafach, segregatorach,

- 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., niewłaściwe 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, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

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

- jakość 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,

- próba lub modyfikacja danych oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

- niedopuszczalna manipulacja danymi osobowymi w systemie,

- ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu,

- praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy oraz wskazująca 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.

- ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki”, itp.,

- podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych,

- rażące naruszenia dyscypliny 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

**6. POLITYKA BEZPIECZEŃSTWA**

Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

**6.1. DEKLARACJA**

Administrator danych deklaruje dołożyć wszelkich starań, aby przetwarzanie danych osobowych odbywało się w zgodności z przepisami prawa. W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych.

 Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

**6.2. CHARAKTERYSTYKA INSTYTUCJI**

1. Fundacja pod nazwą MUUVE, zwana dalej Fundacją działa na podstawie Ustawy z dnia 6 kwietnia 1984 r. o fundacjach oraz postanowień niniejszego statutu.

2. Fundacja została ustanowiona przez Szymona Damek, zamieszkałego: 43-300 BielskoBiała, ul. Bystrzańska 46B/1N, zwanego dalej Fundatorem, aktem notarialnym z dnia 6 lutego 2018 roku, sporządzonym przez notariusza Agnieszkę Kaczmarczyk– w Kancelarii Notarialnej w Bielsku-Białej, ul. Ratuszowa 2/10, Repertorium A Nr 1733/2018.

3. Fundacja prowadzi działalność odpłatną i nieodpłatną w zakresie zapobiegania wykluczeniu społecznemu oraz przeciwdziałania chorobom psychicznym, w tym depresji, poprzez działalność profilaktyczną i edukacyjną.

 **6.3. WYKAZ ZBIORÓW OSOBOWYCH**

Na podstawie § 4 pkt 2 Rozporządzenia 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 tworzy się wykaz zbiorów osobowych zgodnie z załącznikiem do niniejszej dokumentacji. Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się, zgodnie z § 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. środki bezpieczeństwa na odpowiednim poziomie.

**6.4. WYKAZ MIEJSC PRZETWARZANIA**

Na podstawie § 4 pkt 1 Rozporządzenia 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, tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych. Wyznacza go siedziba Fundacji. Szczegółowy wykaz pomieszczeń, stanowi odrębny załącznik do niniejszej dokumentacji.

 **6.5. EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH**

 Zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych, a po 25 maja 2019 roku przepisami RODO, wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi odrębny załącznik do niniejszej dokumentacji. Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres, a w przypadku kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu.

Ewidencja stanowi podstawę wydania Upoważnienia do przetwarzania danych osobowych.

 **6.6. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH** W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- Przetwarzanie danych osobowych w Fundacji może odbywać się wyłącznie w ramach wykonywania zadań statutowych Fundacji.

- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.

- Wzór upoważnienia stanowi załącznik niniejszej dokumentacji.

- ADO prowadzi ewidencję osób upoważnionych, o której mowa w pkt 6.5 oraz na jej podstawie przygotowuje Upoważnienia do przetwarzania danych.

- Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego załącznik do niniejszej dokumentacji.

- Zabrania się przetwarzania danych poza obszarem do tego wyznaczonym.

- Nowo przyjęty pracownik zapoznaje się ze wszystkimi dokumentami, z zakresu polityki bezpieczeństwa, przed przystąpieniem do przetwarzania danych.

- Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa.

- Wzór potwierdzenia stanowi załącznik do niniejszej dokumentacji.

- Obszar przetwarzania danych osobowych określony w niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

- Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

- Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiedni załącznik przedmiotowej dokumentacji.

- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.

- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

- Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w załączniku.

**Dla zapewnienia kontroli przestrzegania zasad określonych w niniejszej dokumentacji wyznacza się następujące zadania Administratorowi bezpieczeństwa informacji:**

- Nadzór nad przetwarzaniem danych zgodnie z ustawą o ochronie danych osobowych i innymi przepisami prawa.

- Kontrola przestrzegania zasad ochrony – systematycznie,

- Kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:

- Kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony.

- Kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są informacje.

- Kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi. o Kontrola awaryjnego zasilania komputerów.

- Nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych.

- Kontrola systemu kontroli obecności wirusów komputerowych.

- Kontrola nadanych upoważnień.

- Przedstawianie Administratorowi danych wyników kontroli.

- Systematyczna analiza dokumentacji pod kątem obszarów, zbiorów oraz zasad ochrony. Szkolenie z ochrony danych osobowych oraz aktów wykonawczych.

- Podjęcie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu bezpieczeństwa informacji.

Zbiory danych przetwarzane w Fundacji zabezpiecza się poprzez:

 **\* Środki ochrony fizycznej.**

- Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zamykanymi na klucz przy opuszczaniu go przez osobę upoważnioną do przetwarzania danych .

- Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą , rolet.

- Zbiory danych osobowych w formie papierowej przechowywane są w segregatorach w szafie, lub zamykanych szufladach.

- Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie.

- Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

 \* **Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.**

- Zbiory danych osobowych przetwarzane są przy użyciu komputera przenośnego .

- Komputer służący do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową.

- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

**\* Środki ochrony w ramach systemowych narzędzi programowych i baz danych.**

Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

**7**. **Szczegółowe procedury dotyczące przetwarzania danych osobowych w Fundacji zastały zawarte w odrębnych dokumentach.**

**8. Instrukcja bezpieczeństwa systemu informatycznego została stworzona jako odrębny dokument.**

**9. Procedura wchodzi w życie z dniem zatwierdzenia.**

**Instrukcję zatwierdził Administrator Danych Osobowych.**

 -------------------------------------------------------------

 (data i podpis Administratora Danych Osobowych)