Polityka bezpieczeństwa przetwarzania danych osobowych

Niniejsza polityka bezpieczeństwa opisuje reguły i zasady ochrony danych osobowych przetwarzanych przez Fundację im. Anny Pasek, ul. Małobądzka 101, 42-500 Będzin.

Rozdział I
Postanowienia ogólne

§ 1

Celem niniejszej polityki bezpieczeństwa jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe, w tym zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

§ 2

Niniejsza polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu ministra spraw wewnętrznych i administracji z 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. Po rozpoczęciu stosowania unijnego rozporządzenia o ochronie danych osobowych w dniu 25.05.2018 r., niniejsza polityka bezpieczeństwa również zachowuje swoją aktualność, zawierając w swojej treści jednocześnie rejestr czynności przetwarzania danych osobowych.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz samych użytkowników.

§ 4

Obok niniejszej polityki opracowano i wdrożono instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Określa ona sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

§ 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na

odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
    1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
    2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany
    3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie
    4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej
    5) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne
    6) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 6

1. Administratorem danych osobowych jest Fundacja im. Anny Pasek.
2. Administrator danych osobowych nie powołał administratora bezpieczeństwa informacji (inspektora ochrony danych osobowych), w związku z czym administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji (inspektora ochrony danych osobowych).
3. Administrator danych osobowych nie powołał również administratora systemów informatycznych, w związku z czym samodzielnie wykonuje jego zadania.

Rozdział II
Definicje

§ 7

Przez użyte w niniejszej polityce bezpieczeństwa określenia należy rozumieć:

1) **administrator danych osobowych –** Fundacja im. Anny Pasek,
2) **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922),
3) **rozporządzenie** – rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i

systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024),

4) **RODO** – 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,

5) **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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,

6) **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

7) **przetwarzanie danych –** operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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,

8) **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,

9) **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze,

10) **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

11) **administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,

12) **użytkownik** – upoważniony przez administratora danych osobowych pracownik, zleceniobiorca, wykonawca umowy o dzieło, wykonawca umowy o świadczenie usług, praktykant lub stażysta wyznaczony do przetwarzania danych osobowych; użytkownikiem może być również administrator danych osobowych,

13) **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

14) **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział III
Zakres stosowania

§ 8

Polityka bezpieczeństwa zawiera informacje dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 9

Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemach tradycyjnych,
2) danych osobowych przetwarzanych w systemach informatycznych,
3) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
4) rejestru osób dopuszczonych do przetwarzania danych osobowych,
5) innych dokumentów zawierających dane osobowe.

§ 10

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   3) wszystkich pracowników, zleceniobiorców, wykonawców umów o dzieło, wykonawców umów o świadczenie usług, praktykantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez Politykę bezpieczeństwa zobowiązani są wszyscy pracownicy, zleceniobiorcy, wykonawcy umów o dzieło, wykonawcy umów o świadczenie usług, praktykanci, stażyści i inne osoby mające dostęp do informacji podlegających ochronie.

3. Polityka bezpieczeństwa nie dotyczy podmiotów zewnętrznych, które przetwarzają dane osobowe powierzone im do przetwarzania przez administratora danych osobowych na podstawie stosownych umów powierzenia. Podmioty te stosują własne procedury i środki bezpieczeństwa związane z ochroną danych osobowych wymagane przez przepisy prawa, do czego zobowiązały się w ramach zawartych umów powierzenia przetwarzania danych osobowych. Powierzenie przetwarzana danych osobowych zostało dokonane na rzecz różnych podmiotów, które wskazane zostały w ramach opisów poszczególnych zbiorów danych osobowych stanowiących załącznik nr 1 do niniejszej polityki.

Rozdział IV
Opis działalności administratora danych osobowych, obszar przetwarzania danych osobowych i sprzęt wykorzystywany do przetwarzania danych osobowych

§ 11

1. Administrator danych osobowych jest organizacją pożytku publicznego (OPP).
2. W związku z prowadzoną działalnością OPP, dochodzi do przetwarzania danych osobowych.
3. Dane osobowe przetwarzane są zarówno w formie papierowej, jak i w formie elektronicznej, przy czym dominującą formą jest forma elektroniczna.

§ 12

1. Dane osobowe przetwarzane są w siedzibie administratora danych osobowych znajdującej się pod następującym adresem: ul. Małobądzka 101, 42-500 Będzin.
2. Opis siedziby administratora danych osobowych: Biuro Fundacji mieści się na 1 piętrze, w prawym skrzydle budynku o adresie wspomnianym w poprzednim punkcie.
3. Ponieważ administrator danych osobowych powierza przetwarzanie danych osobowych podmiotom trzecim, do przetwarzania danych osobowych dochodzi również w innych lokalizacjach, ale w tym zakresie czynności przetwarzania dokonuje podmiot trzeci lub ewentualnie podmioty do tego przez niego upoważnione. Administrator danych osobowych nie ma szczegółowej wiedzy na temat lokalizacji, w obrębie których dochodzi do przetwarzania danych przez podmioty, którym powierzył przetwarzanie danych osobowych, ale podmioty te zobowiązały się do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez przepisy prawa.
4. Administrator danych osobowych wdrożył odpowiednie środki ochrony danych osobowych wyłącznie w lokalizacji, o której mowa w ust. 1 powyżej oraz na komputerach i urządzeniach wykorzystywanych do przetwarzania danych osobowych. Jeżeli chodzi o podmioty, którym administrator powierzył przetwarzanie danych osobowych, oświadczyły one, że wdrożyły odpowiednie środki ochrony i bezpieczeństwa danych osobowych wymagane przez przepisy prawa i zobowiązały się je utrzymywać przez okres powierzenia przetwarzania danych.

5. Przetwarzanie danych osobowych w lokalizacji, o której mowa w ust. 1 powyżej, odbywa się w ten sposób, że z tej lokalizacji następuje logowanie do systemów informatycznych służących do przetwarzania danych osobowych. W tej lokalizacji przetwarzane są również dane osobowe w formie papierowej.
6. Z uwagi na to, że do przetwarzania danych osobowych wykorzystywane są urządzenia przenośne, nie jest możliwe jednoznaczne określenie obszaru przetwarzania danych osobowych, ponieważ dane mogą być przetwarzane przy użyciu urządzeń przenośnych z dowolnego miejsca poprzez zalogowanie się do systemów informatycznych dostępnych w modelu on-line. Użytkownicy stosują odpowiednie środki ochrony, bezpieczeństwa i ostrożności w związku z przetwarzaniem danych z wykorzystaniem urządzeń przenośnych.
7. Szczegóły dotyczące przetwarzania danych osobowych w ramach poszczególnych zbiorów znajdują się w opisach zbiorów stanowiących załącznik nr 1 do Polityki bezpieczeństwa.

§ 13

1. Dane osobowe przetwarzane są przy wykorzystaniu następujących urządzeń: Komputery stacjonarne, laptopy, tablety.
2. Przetwarzanie danych przy wykorzystaniu wskazanych powyżej urządzeń polega na tym, że następuje z niego logowanie do systemów informatycznych, w ramach których przetwarzane są dane osobowe. Część danych może być również przechowywana na dysku wskazanych urządzeń.

Rozdział V
Wykaz zbiorów danych osobowych

§ 14

1. Dane osobowe przetwarzane są przez administratora danych osobowych w ramach następujących zbiorów:
    1) zbiór „Stypendyści”,
    2) zbiór „Pracownicy”,
    3) zbiór „Korespondencja”,
    4) zbiór „Kontakty”,
    5) zbiór „Osoby upoważnione”.
2. Szczegóły dotyczące przetwarzania danych w ramach poszczególnych zbiorów znajdują się w opisie tychże zbiorów stanowiących załącznik nr 1 do niniejszej polityki.

Rozdział VI
Środki techniczne i organizacyjne zabezpieczenia danych

§ 15

1. Zabezpieczenia organizacyjne:
    1) sporządzono i wdrożono Politykę bezpieczeństwa,
    2) sporządzono i wdrożono Instrukcję zarządzania systemami informatycznymi,
    3) do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych osobowych,
    4) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
    5) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
    6) dane osobowe przetwarzane są w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
    7) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów,
    8) siedziba administratora zabezpieczona jest drzwiami antywłamaniowymi,
    9) w siedzibie administratora okna zabezpieczone są za pomocą rolet,
    10) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej metalowej szafie.
    11) pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojących gaśnic.
2. Zabezpieczenia techniczne:
    1) zastosowano system Firewall do ochrony dostępu do sieci komputerowej,
    2) zastosowano środki ochrony przed szkodliwym oprogramowaniem,
    3) zastosowano uwierzytelnienie z wykorzystaniem identyfikatora użytkownika oraz hasła przy dostępie do zbioru danych,
    4) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych,
    5) zastosowano uwierzytelnienie z wykorzystaniem identyfikatora użytkownika oraz hasła przy starcie systemu operacyjnego komputera,
    6) zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji,
    7) zastosowano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych,
    8) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych,
    9) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych,

10) zastosowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

3. Wskazane powyżej środki techniczne i organizacyjne zabezpieczenia danych dotyczą wyłącznie środków wdrożonych bezpośrednio przez administratora danych osobowych. W zakresie, w jakim administrator danych osobowych powierzył przetwarzanie danych osobowych innym podmiotom, podmioty te zobowiązały się utrzymywać odpowiednie środki ochrony danych osobowych wymagane przez przepisy prawa.

Rozdział VII
Zadania administratora danych osobowych i administratora systemu informatycznego

§ 16

1. Do najważniejszych obowiązków administratora danych osobowych należy:
   1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami obowiązujących przepisów prawa,
   2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
   3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych i zgłoszenie faktu naruszenia organowi nadzorczemu oraz zawiadomienie o tym osobę, której dane dotyczą,
   6) nadzór nad bezpieczeństwem danych osobowych,
   7) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
   8) przeprowadzanie szkoleń użytkowników zgodnie z ust. 2, 3, 4, 5 poniżej.
2. Każdy użytkownik, za wyjątkiem administratora danych osobowych, przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz z instrukcjami obowiązującymi u administratora danych osobowych.

§ 17

1. Administratorem systemu informatycznego jest osoba określona przez administratora danych osobowych. Powołanie administratora systemu informatycznego dokonywanej jest w formie pisemnej. Jeżeli administrator systemu informatycznego nie zostanie powołany, jego zadania wykonuje administrator danych osobowych.
2. Administrator systemu informatycznego odpowiedzialny jest za:

1) bieżący monitoring i zapewnienie ciągłości działania komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
2) optymalizację wydajności komputerów i innych urządzeń wykorzystywanych do przetwarzania danych osobowych oraz systemów operacyjnych,
3) instalację i konfiguracje sprzętu sieciowego i serwerowego,
4) instalację i konfigurację oprogramowania systemowego, sieciowego,
5) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
7) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,
8) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
9) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
10) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
11) przyznawanie na wniosek administratora danych osobowych ściśle określonych praw dostępu do informacji w danym systemie,
12) wnioskowanie do administratora danych osobowych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
13) zarządzanie licencjami, procedurami ich dotyczącymi,
14) prowadzenie profilaktyki antywirusowej.

3. Praca administratora systemu informatycznego jest nadzorowana przez administratora danych osobowych, chyba, że administrator danych osobowych nie powołał administratora systemu informatycznego – wtedy jego zadania realizuje samodzielnie administrator danych osobowych.

Rozdział VIII
Zgłaszanie i zawiadamianie o naruszeniu ochrony danych osobowych

§ 18

1. Każde naruszenie ochrony danych osobowych powinno być niezwłocznie zgłaszane przez użytkowników administratorowi danych osobowych. Szczegóły w zakresie postępowania w związku ze stwierdzonym naruszeniem ochrony danych osobowych przy korzystaniu z systemów informatycznych opisane zostały w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
2. Administrator danych osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte środki zaradcze.

Dokumentacja odbywa się z wykorzystaniem zestawienia incydentów naruszenia ochrony danych osobowych.

3. W przypadku naruszenia ochrony danych osobowych, na administratorze danych osobowych ciąży obowiązek zgłoszenia tego faktu do organu nadzorczego zgodnie z postanowieniami art. 33 RODO oraz zawiadomienia osoby, której dane dotyczą, zgodnie z postanowieniami art. 34 RODO.

Rozdział IX
Postanowienia końcowe

§ 19

1. Administrator danych osobowych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
3. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną.

Załącznik nr 1 – wykaz i opis zbiorów danych osobowych

1) Zbiór „**Stypendyści**”, w ramach którego przetwarzane są dane osób, które złożyły wniosek o Stypendium naukowe im. Anny Pasek. Wniosek składany jest za pośrednictwem strony internetowej. Założenie konta skutkuje zapisaniem danych użytkownika w bazie administratora danych osobowych. Dane przechowywane są w bazie przez czas funkcjonowania Konkursu, chyba, że użytkownik podejmie wcześniej decyzję o usunięciu konta. Usunięcie konta spowoduje usunięcie danych z bazy.

   W zbiorze przetwarzane są następujące informacje:

   1) imię i nazwisko,
   2) numer telefonu,
   3) adres e-mail,
   4) zaświadczenie o uczestnictwie w studiach doktoranckich

   Dane przetwarzane są w celu założenia i utrzymywania konta użytkownika.

   Podstawą prawną przetwarzania danych osobowych jest Regulamin Stypendium Naukowego im. Anny Pasek.

   Dane przetwarzane są w formie elektronicznej w ramach systemu Google Forms i przechowywane są na serwerze, na którym zainstalowany jest system Google Forms i na którym miejsce zapewnia administratorowi danych osobowych zewnętrzny hostingodawca, tj. Google inc. Administrator zawarł z tym podmiotem umowę powierzenia przetwarzania danych osobowych, a podmiot ten zobowiązał się do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez prawo.

   Dostęp do danych wymaga zalogowania się do systemu Google Cloud z wykorzystaniem identyfikatora użytkownika oraz hasła, zdefiniowanych przez administratora danych osobowych. Wszyscy użytkownicy posiadają oddzielne identyfikatory użytkownika oraz hasła.

2) zbiór „**Pracownicy**”, zawierający dane osobowe pracowników, zleceniobiorców, wykonawców umów o dzieło oraz stażystów, wolontariuszy i praktykantów współpracujących z administratorem danych osobowych.

   Dane obejmują m.in.:

   1) imię i nazwisko,
   2) data i miejsce urodzenia,
   3) imiona rodziców,
   4) numer PESEL,
   5) adres zamieszkania,
   6) numer telefonu,
   7) adres e-mail,

8) numer rachunku bankowego.

Dane przetwarzane są w związku z zatrudnieniem u administratora danych osobowych.

Podstawą prawną przetwarzania danych osobowych jest wypełnianie przez administratora obowiązków związanych z zatrudnieniem.

Dane przetwarzane są w formie papierowej w ramach umów, kwestionariuszy osobowych i dokumentacji kadrowej przechowywanej w biurze rachunkowym, świadczącym na rzecz administratora usługi księgowe, w tym obsługę kadrową oraz w formie elektronicznej na dysku komputera wykorzystywanego do przetwarzania danych osobowych. W związku ze świadczeniem na rzecz administratora usług księgowych, w tym obsługi kadrowej, dochodzi do powierzenia przetwarzania danych osobowych na potrzeby świadczenia tych usług. Administrator zawarł z biurem (tj. Biuro Rachunkowe BRS Spółka z ograniczoną odpowiedzialnością 42-500 Będzin, ul. Małobądzka 101) umowę powierzenia przetwarzania danych osobowych, a biuro zobowiązało się do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez prawo.

3) zbiór „**Korespondencja**”, zawierający dane osobowe zawarte w korespondencji wymienianej przez administratora danych osobowych z klientami, potencjalnymi klientami, współpracownikami i innymi osobami w formie elektronicznej.

   Dane przetwarzane są celu wymiany oraz archiwizacji korespondencji.

   Podstawą prawną przetwarzania danych jest usprawiedliwiony cel administratora danych osobowych.

   Korespondencja realizowana jest za pośrednictwem poczty e-mail, a co za tym idzie przechowywana na serwerze skrzynki pocztowej. Serwer ten zapewniany jest przez firmę NAZWA.PL Administrator zawarł z tym podmiotem umowę powierzenia przetwarzania danych osobowych, a podmiot ten zobowiązał się do stosowania odpowiednich środków ochrony i bezpieczeństwa danych osobowych wymaganych przez prawo. Korespondencja może być również archiwizowana na dysku komputera wykorzystywanego do przetwarzania danych osobowych.

4) zbiór „**Kontakty**”, zawierający dane osób, do których chociaż raz została wysłana wiadomość e-mail oraz dane osób znajdujących się w książce telefonicznej administratora danych osobowych.

   Dane przetwarzane są w celu i w związku z kontaktami realizowanymi przez administratora danych osobowych z osobami trzecimi.

   Podstawą prawną przetwarzania danych jest usprawiedliwiony cel administratora danych osobowych.

   Dane przechowywane są na dysku komputera wykorzystywanego do przetwarzania danych osobowych w postaci list kontaktów w ramach programów pocztowych oraz w książce telefonicznej w telefonie administratora danych osobowych.

5) zbiór „**Osoby upoważnione**”, w ramach którego przetwarzane są dane osób, które zostały przez administratora danych osobowych upoważnione do przetwarzania danych osobowych.

   W zbiorze przetwarzane są następujące informacje:

   1) imię i nazwisko,
   2) identyfikator użytkownika,
   3) zakres upoważnienia,
   4) data nadania upoważnienia,
   5) data cofnięcia upoważnienia.

   Dane trafiają do zbioru w wyniku udzielenia danej osobie upoważnienia do przetwarzania danych osobowych. Upoważnienie udzielane jest na piśmie przez administratora danych osobowych.

   Dane przetwarzane są w celu nadania i przechowywania upoważnienia do przetwarzania danych osobowych.

   Podstawą prawną przetwarzania danych jest wypełnianie przez administratora obowiązków prawnych związanych z ochroną danych osobowych.

   Dane przetwarzane są w formie papierowej oraz elektronicznej w postaci listy osób upoważnionych. Lista przechowywana jest łącznie z wewnętrzną dokumentacją ochrony danych osobowych.