POLITYKA BEZPIECZEŃSTWA

Celem **Polityki bezpieczeństwa** przetwarzania danych osobowych w ramach działalności prowadzonej przez Fundacja Nizio „The Creators" (numer NIP: 5252334097) jest zapewnienie zachowania staranności wymaganej podczas przetwarzania i zabezpieczania danych osobowych zgodnie z wymogami prawa, dotyczącymi zasad ich przetwarzania i zabezpieczenia, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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").

§ 1. Definicje:

Ilekroć w Polityce bezpieczeństwa jest mowa o:

1) **Administratorze Danych** – należy przez to rozumieć Fundacja Nizio „The Creators" ul. Inżynierska 3/4
03-410 Warszawa; numer telefonu: 22 618 72 02; adres e-mail: fundacja@nizio.com.pl; NIP: 5252334097
2) **Dane osobowe** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
3) **Pomiot przetwarzający** – należy przez to rozumieć osobę fizyczną lub jednostkę organizacyjną, która przetwarza Dane osobowe w imieniu Administratora na podstawie umowy o powierzenia przetwarzana danych osobowych;
4) **Przetwarzanie danych** – należy przez to rozumieć operację lub zestaw operacji wykonywanych na Danych osobowych w sposób zautomatyzowany lub niezautomatyzowany (to jest poprzez Systemy informatyczne), taką 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;
5) **Strona trzecia** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, Administrator danych, Podmiot przetwarzający lub Użytkownik, które mogą przetwarzać Dane osobowe;
6) **Użytkownik** – należy przez to rozumieć osobę przetwarzającą Dane osobowe na podstawie upoważnienia udzielonego przez Administratora Danych;
7) **Zbiór danych** – należy przez to rozumieć każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.

§ 2. Postanowienia ogólne

1. Polityka bezpieczeństwa dotyczy wszystkich Danych osobowych przetwarzanych przez Administratora danych, niezależnie od formy przetwarzania.
2. Polityka bezpieczeństwa została sporządzona w formie pisemnej i jest przechowywana w siedzibę Administratora danych.
3. Jednobrzmiąca z pisemną elektroniczna forma Polityki bezpieczeństwa jest udostępniania Podmiotom przetwarzającym i Użytkownikom, w celu zapoznania z zasadami przetwarzania i zabezpieczania Danych osobowych wykorzystywanych w ramach działalności przedsiębiorstwa prowadzonego przez Administratora danych.

4. W celu wdrożenia i realizacji Polityki bezpieczeństwa Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii Danych objętych ochroną środki technicznie i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad Przetwarzaniem Danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.
5. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in.: nadzór nad działaniami Użytkowników i kontrolę Podmiotów przetwarzających; informowanie właściwych organów o naruszeniu bezpieczeństwa Danych osobowych zasad ochrony do danych; analizę przyjętych metod ochrony Danych osobowych, w tym zapewnienia integralności plików oraz skuteczności ochrony Danych przed atakami zewnętrznymi oraz wewnętrznymi.
6. Administrator Danych podejmuje wszelkie działania, które są celowe, uzasadnione i proporcjonalne w celu zapewnienia, aby czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem Danych osobowych były zgodne z Polityką bezpieczeństwa oraz przepisami prawa.

§ 3. Przetwarzanie danych przez Administratora danych

7. Dane osobowe przetwarzane przez Administratora uporządkowane są w Zbiorach danych.
8. Przetwarzanie danych przez Administratora danych nie będzie obejmowało czynności, które mogłyby wiązać się z dużym prawdopodobieństwem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób, których Dane dotyczą. W przypadku planowania takiego działania Administrator wykona czynności oceny skutków dla ochrony danych, o których mowa w art. 35 i n. RODO.
9. W przypadku planowania nowych czynności przetwarzania Danych osobowych w celach innych niż te, dla których zostały pozyskane, Administrator danych uzyska dla tych czynności ponowną zgodę osoby, której Dane dotyczą. Jedocześnie Administrator danych dokona analizy ich skutków dla ochrony danych osobowych oraz uwzględni kwestie ochrony danych w fazie projektowania nowych czynności.
10. Administrator danych może prowadzić rejestr czynności przetwarzania według wzoru stanowiącego Załącznik nr 1 do Polityki bezpieczeństwa.

§ 4. Zarządzania bezpieczeństwem Danych osobowych

11. Administrator danych, Podmioty przetwarzające i Użytkownicy zobowiązani są do przetwarzania Danych osobowych zgodnie z obowiązującymi przepisami oraz Polityką bezpieczeństwa, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych.
12. Przetwarzanie wszystkich Danych osobowych zawsze wymaga zachowania w szczególności następujących zasad:
    a) przetwarzanie Danych osobowych zawsze wymagana istnienia przynajmniej jednej z przewidzianych przepisami RODO podstaw dla przetwarzania danych;
    b) Dane osobowe są przetwarzane są zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osób, których dane dotyczą;
    c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
    e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane;
    f) czas przechowywania Danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane, chyba że ich dalsze przetwarzanie jest niezbędne ze względu na prawnie uzasadnione interesy przedsiębiorstwa lub Administratora Danych;
    g) wobec osób, których Dane dotyczą, zawsze koniecznej jest wykonanie obowiązku informacyjnego zgodnie z treścią art. 13 i art. 14 RODO;
    h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.

4. Naruszenie lub usiłowanie naruszenia zasad przetwarzania i ochrony Danych osobowych stanowi:
    a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są Dane osobowe;
    b) udostępnianie lub pomocnictwo w udostępnieniu Danych podmiotom do tego nieupoważnionym;
    c) zaniechanie, w tym nieumyślne, dopełnienia obowiązku zapewnienia ochrony Danych osobowych;
    d) niedopełnienie obowiązku zachowania poufności Danych osobowych oraz zasad i sposobów ich zabezpieczenia;
    e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem, w jakim zostały przekazane;
    f) uszkodzenie, utratę, niekontrolowaną zmianę lub nieuprawnione kopiowanie Danych osobowych;
    g) naruszenie praw osób, których Dane dotyczą, w tym w szczególności praw, o których mowa w art. 15-18 RODO.
5. W przypadku stwierdzenia istnienia bezpośredniego ryzyka naruszenia Danych lub naruszenia zasad ochrony danych osobowych Administrator danych, Podmiot przetwarzający lub Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych działań, mających na celu zapobieżenie naruszeniu i ograniczenie skutków ewentualnego naruszenia.
6. Do obowiązków Administratora Danych w zakresie zatrudniania pracowników, na podstawie umów o pracę lub umów cywilnoprawnych, którzy w ramach swoich obowiązków będą przetwarzali Dane osobowe, należy:
    a) odpowiednie przeszkolenie pracowników w zakresie przepisów i zasad ochrony Danych osobowych, w tym zapoznanie z Polityką bezpieczeństwa i Instrukcją Korzystania z Systemu Informatycznego,
    b) udzielenie pracownikom pisemnego upoważnienia do przetwarzania danych zgodnie z wzorem stanowiącym Załącznik nr 3 do Polityki bezpieczeństwa,
    c) odebranie od pracowników zobowiązania do zachowania Danych osobowych w tajemnicy.
7. Użytkownicy zobowiązani są do:
    a) ścisłego przestrzegania zakresu nadanego upoważnienia;
    b) przetwarzania i ochrony Danych osobowych zgodnie z przepisami i zasadami ochrony Danych;
    c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    d) zgłaszania naruszeń i usiłowania naruszenia Danych osobowych i innych zdarzeń mogących mieć wpływ na bezpieczeństwo ochrony Danych.

§ 5. Miejsce przetwarzania danych osobowych

Dane osobowe przetwarzane są siedzibie Administratora danych oraz we wszystkich miejscach wykorzystywanych przez System informatyczny, o ile jest to niezbędne do jego prawidłowego funkcjonowania.

§ 6. Naruszenie zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Administrator danych dokonuje oceny, czy naruszenie spowodowało lub mogło spowodować ryzyko naruszenia praw lub wolności osób, których Dane dotyczą.
2. Jeżeli naruszenie spowodowało wysokie ryzyko naruszenia praw i wolności osoby, której Dane dotyczą, Administrator zawiadamia tę osobę o fakcie naruszenia.
3. Jeżeli naruszenie spowodowało ryzyko naruszenia praw lub wolności osób, których Dane dotyczą, Administrator danych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, według wzoru zgłoszenia określonego w Załączniku nr 4 do Polityki bezpieczeństwa.

§ 7. Powierzenie przetwarzania danych osobowych

1. Administrator danych powierzyć Przetwarzanie Danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, o ile podmiot ten zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by Przetwarzanie spełniało wymogi przepisów RODO i chroniło prawa osób, których Dane dotyczą.
2. Przed zawarciem umowy o powierzenie przetwarzania Danych osobowych Administrator danych w miarę możliwości uzyskuje informacje o dotychczasowych praktykach podmiotu, z którym umowa ma zostać zawarta, w celu sprawdzenia, czy podmiot ten zapewnia gwarancje, o których mowa w ust. 1.
3. Umowa o powierzenie przetwarzania Danych osobowych będzie zawierana według wzoru stanowiącego Załącznik nr 5 do Polityki bezpieczeństwa.

§ 8. Przekazywanie danych do państwa trzeciego

Administrator danych nie będzie przekazywał Danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której Dane dotyczą.

§ 9. Postanowienia końcowe

1. Naruszenie zasad Polityki bezpieczeństwa przez Użytkowników będzie powodowało odpowiedzialność określoną w Kodeksie pracy i przepisach o ochronie Danych osobowych.
2. Naruszenie zasad Polityki bezpieczeństwa przez Podmiot przetwarzający będzie powodowało odpowiedzialność określoną w Kodeksie cywilnym i przepisach o ochronie Danych osobowych.
3. Załącznikami do Polityki bezpieczeństwa są:
    a) wzór Rejestru czynności przetwarzania danych osobowych – Załącznik nr 1,
    b) wzór Upoważnienia do przetwarzania danych osobowych – Załącznik nr 3,
    c) wzór Zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego – Załącznik nr 4,
    d) wzór Umowy o powierzenie przetwarzania danych osobowych – Załącznik nr 5.
4. Polityka bezpieczeństwa wchodzi w życie od dnia 25 maja 2018 r.
5. Dane osobowe zebrane przez Administratora danych przed wejściem w życie Polityki bezpieczeństwa od dnia jej wejścia w życie podlegają przetwarzaniu zgodnie z Polityką bezpieczeństwa.