

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

w Fundacji Konewka

1. Postanowienia ogólne

Niniejsza Polityka bezpieczeństwa przetwarzania danych osobowych (dalej: „Polityka”) określa zasady, sposób i środki ochrony danych osobowych przetwarzanych przez Fundację Konewka z siedzibą w Krakowie, os. Na Skarpie 63/16 (dalej: „Fundacja”), w związku z realizacją jej celów statutowych.

Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz właściwych przepisów prawa krajowego.

Celem Polityki jest zapewnienie, aby wszystkie operacje przetwarzania danych osobowych w Fundacji odbywały się zgodnie z prawem, były adekwatne, bezpieczne, udokumentowane i rozliczalne.

2. Zakres przedmiotowy i podmiotowy

Polityka obejmuje wszystkie procesy przetwarzania danych osobowych w Fundacji, w szczególności dotyczące:

- a) dzieci-uczestników zajęć,
- b) rodziców/opiekunów prawnych,
- c) dorosłych uczestników zajęć/warsztatów/spotkań
- d) wolontariuszy, prowadzących zajęcia i współpracowników,
- e) darczyńców, partnerów, kontrahentów, grantodawców; beneficjentów projektów,
- f) użytkowników strony internetowej i mediów społecznościowych Fundacji,
- g) subskrybentów newslettera.

Polityka dotyczy wszystkich osób przetwarzających dane w imieniu Fundacji: członków organów, pracowników, współpracowników, wolontariuszy, a także podmiotów przetwarzających dane na podstawie umów powierzenia (np. biuro rachunkowe, dostawcy usług IT).

3. Zasady przetwarzania danych

Fundacja stosuje wszystkie zasady przetwarzania danych osobowych wynikające z RODO:

Zasada legalności – dane są przetwarzane na podstawie ważnej podstawy prawnej (m.in. zgoda, umowa, obowiązek prawny, uzasadniony interes).

Zasada przejrzystości – osoby, których dane dotyczą, są w jasny sposób informowane o celach, podstawach i zakresie przetwarzania (klauzule informacyjne, polityka prywatności).

Zasada celowości – dane zbierane są w konkretnych, wyraźnych celach (np. organizacja zajęć, rozliczanie projektów) i nie są przetwarzane dalej w sposób niezgodny z tymi celami.

Zasada minimalizacji danych – Fundacja zbiera tylko takie dane, które są niezbędne do realizacji danego celu (np. do zajęć: imię, nazwisko, kontakt do rodzica, informacje o zdrowiu tylko jeśli konieczne).

Zasada prawidłowości – dane są aktualne i poprawne; Fundacja wprowadza mechanizmy ich aktualizacji na wniosek osoby lub z inicjatywy Fundacji.

Zasada ograniczenia przechowywania – dane są przechowywane nie dłużej, niż jest to konieczne (np. okres trwania projektu + okres wymagany przepisami księgowymi/archiwizacyjnymi).

Zasada integralności i poufności – Fundacja zapewnia odpowiedni poziom bezpieczeństwa danych (środki techniczne i organizacyjne).

Zasada rozliczalności – Fundacja dokumentuje sposób przetwarzania danych (rejstry, procedury) i jest w stanie wykazać zgodność z RODO.

4. Kategorie danych i główne cele przetwarzania

Dzieci uczestniczące w zajęciach – imię, nazwisko, data urodzenia, klasa/grupa, szkoła, obecności na zajęciach, ewentualne informacje o stanie zdrowia niezbędne dla zapewnienia bezpieczeństwa, wizerunek (jeśli jest zgoda). Cele: organizacja zajęć, zapewnienie bezpieczeństwa, rozliczanie projektów, dokumentacja i ewaluacja działań.

Dorośli uczestnicy - imię, nazwisko, obecności na zajęciach, wizerunek (jeśli jest zgoda). Cele: organizacja zajęć, rozliczanie projektów, dokumentacja i ewaluacja działań.

Rodzice/opiekunowie prawni – dane identyfikacyjne, kontaktowe, podpisy na zgodach i umowach, oświadczenia. Cele: kontakt organizacyjny, realizacja zgód, rozliczanie udziału dziecka w projekcie.

Prowadzący zajęcia / wolontariusze – dane identyfikacyjne, kontaktowe, dane potrzebne do rozliczeń (umowy, rachunki, ZUS, US). Cele: zawarcie i wykonanie umów, rozliczenia, sprawozdawczość.

Darczyńcy, partnerzy, kontrahenci, grantodawcy – dane identyfikacyjne, kontaktowe, dane rozliczeniowe. Cele: współpraca, sprawozdawczość, księgowość.

Użytkownicy strony www, mediów społecznościowych i newslettera – dane z formularzy kontaktowych, zapisu na newsletter, dane w logach i plikach cookies. Cele: komunikacja, promocja działań, analiza statystyk.

5. Role i odpowiedzialności

Administratorem danych osobowych jest Fundacja Konewka (Zarząd Fundacji).

Fundacja może powołać Inspektora Ochrony Danych (IOD), jeśli spełnione są przesłanki z art. 37 RODO; w takim przypadku jego dane kontaktowe są publicznie dostępne.

Fundacja określa i dokumentuje zakres upoważnień do przetwarzania danych dla osób zaangażowanych w działania Fundacji (pracownicy, wolontariusze, współpracownicy). Każda taka osoba podpisuje upoważnienie i zobowiązanie do zachowania poufności.

Fundacja zawiera pisemne umowy powierzenia przetwarzania danych z podmiotami zewnętrznymi (np. biuro rachunkowe, dostawca hostingu, podmiot obsługujący system mailingowy), określając zakres i cel powierzenia oraz środki bezpieczeństwa.

6. Środki techniczne i organizacyjne bezpieczeństwa

Fundacja stosuje środki adekwatne do ryzyka, zgodnie z art. 32 RODO.

6.1 Środki organizacyjne:

- a) prowadzenie rejestru czynności przetwarzania (RCPD) i okresowy przegląd procesów przetwarzania,
- b) nadawanie upoważnień do przetwarzania danych, szkolenia z ochrony danych dla personelu i wolontariuszy,
- c) procedury postępowania z dokumentacją papierową (przechowywanie w zamkniętych szafach, kontrola dostępu do pomieszczeń),
- d) procedury reagowania na naruszenia ochrony danych (identyfikacja, dokumentacja, zgłoszenie do PUODO jeśli wymagane, informowanie osób).

6.2 Środki techniczne:

- a) stosowanie haseł, szyfrowania i uwierzytelniania do systemów informatycznych,
- b) regularne aktualizacje oprogramowania i stosowanie programów antywirusowych,
- c) tworzenie kopii zapasowych (backup) i ich bezpieczne przechowywanie,
- d) ograniczanie dostępu do danych elektronicznych tylko do upoważnionych osób, stosowanie kont indywidualnych.

7. Okresy przechowywania danych

Fundacja określa dla każdej kategorii danych czas przechowywania, uwzględniając cele przetwarzania i wymagania przepisów (np. podatkowych, rachunkowych, grantowych).

8. Prawa osób, których dane dotyczą

Fundacja zapewnia realizację praw osób wynikających z RODO: prawa dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, sprzeciwu, a także prawa do wycofania zgody.

Procedury wewnętrzne określają tryb przyjmowania i obsługi wniosków osób (terminy, sposób udzielania odpowiedzi, dokumentowanie czynności).

Fundacja informuje osoby o przysługujących im prawach w klauzulach informacyjnych dołączanych do formularzy zgód, umów i dokumentów projektowych.

9. Udostępnianie danych i przekazywanie do podmiotów trzecich

Dane osobowe mogą być udostępniane podmiotom uprawnionym na podstawie przepisów prawa (np. sądom, organom administracji) oraz partnerom i grantodawcom, gdy wynika to z umów i wymogów projektowych, w niezbędnym zakresie.

Fundacja nie sprzedaje danych osobowych i nie przekazuje ich do państw trzecich ani organizacji międzynarodowych, chyba że wynika to wprost z narzędzi używanych w komunikacji (np. system newsletterowy z serwerami poza UE) – wówczas zapewnia odpowiednie zabezpieczenia zgodnie z RODO.

10. Naruszenia ochrony danych osobowych

Naruszenie ochrony danych to każde zdarzenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia danych lub dostępu do nich.

Każda osoba współpracująca z Fundacją ma obowiązek niezwłocznie zgłosić podejrzenie naruszenia Zarządowi.

Fundacja prowadzi rejestr naruszeń i w każdym przypadku dokonuje oceny ryzyka dla praw i wolności osób; w razie potrzeby zgłasza naruszenie do Prezesa UODO oraz informuje osoby, których dane dotyczą.

11. Szkolenia i przegląd Polityki

Fundacja zapewnia odpowiedni poziom wiedzy w zakresie ochrony danych osobowych poprzez szkolenia wstępne i okresowe dla osób przetwarzających dane.

Polityka bezpieczeństwa podlega przeglądowi co najmniej raz na 2 lata lub częściej w przypadku zmian przepisów, struktury organizacyjnej Fundacji lub zakresu przetwarzanych danych.