POLITYKA OCHRONY DANYCH OSOBOWYCH

w Fundacji Jesuit Refugee Service Poland (JRS)

Celem Polityki ochrony danych osobowych, zwanej dalej „Polityką", jest wprowadzenie i utrzymanie wymaganej przez prawo właściwej ochrony danych osobowych.
Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w formie papierowej, jak i w systemach informatycznych. Dotyczy istniejących oraz przetwarzanych w przyszłości zbiorów danych osobowych. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych w JRS Poland.
W skład obszaru przetwarzania danych osobowych w JRS Poland wchodzą budynki i lokale położone w Warszawie, ul. Rakowiecka 61, Warszawie, ul. Andrzeja Boboli 12, Poznaniu, ul. Szewska 10, Nowym Sączu, ul. Batalionów Chłopskich 19, Gdyni, ul. Tatrzańska 33 i 35.

§ 1.

Definicje:

1) Administrator Danych Osobowych (ADO) – Zarząd Fundacji JRS;
2) przedstawiciel Administratora Danych Osobowych – Prezes Fundacji JRS Poland;
3) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) przetwarzanie danych osobowych – operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
5) JRS Poland – Fundacja JRS Poland z siedzibą w Warszawie, ul. Rakowiecka 61;
6) użytkownik – osoba upoważniona do przetwarzania danych osobowych;
7) system informatyczny – system (urządzenia, narzędzia, programy), w którym przetwarzane są dane osobowe;
8) zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

§ 2.

Zasady przetwarzania danych osobowych

1. Administrator Danych Osobowych przetwarza dane osobowe:

A. zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");

B. zbierając je w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami („ograniczenie celu");

C. adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");

D. prawidłowo i w razie potrzeby uaktualnia zebrane dane („prawidłowość");

E. przechowując je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których te dane są przetwarzane („ograniczenie przechowywania");

F. w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

2. W celu realizacji zasad, o których mowa w ust. 1, Administrator Danych Osobowych przetwarza dane osobowe legalnie. Pobiera dane osobowe adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza, wypełnia obowiązki informacyjne oraz wskazuje przysługujące im uprawnienia, takie jak:

A. prawo do informacji o przetwarzaniu danych,
B. prawo do żądania sprostowania danych,
C. prawo do żądania dokonania adnotacji i uzupełnienia danych,
D. prawo do żądania usunięcia danych,
E. prawo do żądania ograniczenia przetwarzania,
F. prawo do wniesienia skargi do organu nadzorczego.

3. Administrator Danych Osobowych zapewnia ochronę danych w przypadku korzystania z usług podmiotów zewnętrznych. W razie wystąpienia incydentu technicznego lub fizycznego, zapewnia zdolność do szybkiego przywrócenia dostępności do danych osobowych i dostępu do nich.
4. Potwierdzenie spełniania obowiązków informacyjnych przez Administratora Danych Osobowych stanowią klauzule informacyjne przekazywane osobom, których dane są przetwarzane.

§ 3.
Upoważnienia do przetwarzania danych osobowych

Administrator Danych Osobowych zapewnia, aby dostęp do danych osobowych w JRS Poland, miały tylko osoby zatrudnione w JRS Poland.

§ 4.
Analiza ryzyka

Administrator Danych Osobowych prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest w przypadku zaistnienia zagrożenia oraz cyklicznie nie rzadziej niż raz w roku.

§ 5.
Wykaz zabezpieczeń

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele

przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Administrator Danych Osobowych i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

§ 6.
Procedura postępowania z incydentami

1. Administrator Danych Osobowych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych.
2. Powiadomienia wymagają:
A. niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, udostępnienie haseł osobom postronnym,
B. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
C. nieprzestrzeganie zasad ochrony danych osobowych przez użytkowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),
D. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
E. dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,
F. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
G. nieuprawniona obecność osób postronnych w pomieszczeniach, gdzie przetwarzane są dane,
H. złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
I. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz pomieszczeń, gdzie przechowywane są dane osobowe, bez zezwolenia Administratora Danych Osobowych,
J. awarie serwera, komputerów, twardych dysków, oprogramowania,
K. udostępnienie danych osobowych osobom nieupoważnionym,
L. telefoniczne próby wyłudzenia danych osobowych,
M. kradzież, zagubienie komputerów lub CD, twardych dysków, pen-drive z danymi osobowymi,
N. maile nakłaniające do ujawnienia identyfikatora lub hasła,
O. zainfekowanie komputerów wirusem lub inne błędne zachowanie komputerów,
P. włamanie do systemu informatycznego lub pomieszczeń, gdzie przechowuje się dane osobowe,
R. kradzież danych/sprzętu,
S. świadome zniszczenie dokumentów.

3. Każda osoba uprawniona do przetwarzania danych osobowych ma obowiązek niezwłocznego poinformowania Administratora Ochrony Danych o możliwości wystąpienia incydentu lub o jego wystąpieniu.

§ 7.
Regulamin ochrony danych osobowych i szkolenia wewnętrzne

1. Administrator Danych Osobowych wprowadza w Fundacji JRS Poland, Regulamin ochrony danych osobowych, zwany dalej „Regulaminem", w celu zapewnienia osobom przetwarzającym dane osobowe pełny zakres wiedzy na temat zasad przetwarzania danych osobowych w JRS Poland oraz obciążających je obowiązków z tym związanych.
2. Każda osoba przed powierzeniem jej przetwarzania danych osobowych, powinna zostać zapoznana z Regulaminem.

Warszawa, dnia 01.11.2022 r.
Załącznik: Regulamin ochrony danych osobowych – załącznik nr 1