Polityka Ochrony Danych Osobowych
w Fundacji DeployingFuture
wersja z dnia 10 lutego 2023 r.

Rozdział I. Postanowienia ogólne

§1. Cel i zakres dokumentu

1. Niniejsza Polityka ochrony danych osobowych (dalej: Polityka) stanowi dokument wewnętrzny Fundacji DeployingFuture (dalej: Fundacja), określający zasady, środki i procedury zapewniające zgodność przetwarzania danych osobowych z RODO oraz przepisami prawa krajowego.
2. Polityka dotyczy wszystkich danych osobowych przetwarzanych w Fundacji, niezależnie od formy ich utrwalenia (papierowej, elektronicznej, audio-wizualnej).
3. Dokument obowiązuje wszystkich członków organów Fundacji, pracowników, współpracowników, wolontariuszy, stażystów oraz inne osoby przetwarzające dane na rzecz Fundacji, niezależnie od formy zatrudnienia lub zaangażowania.

§2. Podstawy prawne

Podstawą opracowania i wdrożenia Polityki są:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
2. ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
3. inne właściwe akty prawne Unii Europejskiej i Rzeczypospolitej Polskiej.

W przypadku projektów realizowanych w ramach programu Erasmus+ podstawą prawną jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

Rozdział II. Pojęcia i definicje

§3. Słownik użytych pojęć

- Dane osobowe – informacje o osobie fizycznej zidentyfikowanej lub możliwej do zidentyfikowania.
- Dane szczególnych kategorii – dane wskazane w art. 9 ust. 1 RODO, m.in. dane dotyczące zdrowia, poglądów, przynależności, pochodzenia, biometrii.
- Przetwarzanie danych – każda operacja wykonywana na danych osobowych, w tym zbieranie, modyfikowanie, przechowywanie, udostępnianie, usuwanie.
- UDW – ukryta kopia wiadomości e-mail (BCC) stosowana w celu ochrony danych odbiorców.
- Polityka czystego biurka – zasada zabezpieczania dokumentów zawierających dane osobowe poprzez ich niepozostawianie na widoku.
- IOD – Inspektor Ochrony Danych.
- Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, wyrażające akceptację przetwarzania danych.

Rozdział III. Zasady przetwarzania danych

§4. Zasady ogólne

Dane osobowe w Fundacji przetwarzane są:

- zgodnie z prawem (zasada legalizmu),
- rzetelnie i przejrzyście,
- w konkretnych, wyraźnych celach,
- w sposób ograniczony do niezbędnego minimum (minimalizacja),
- z dbałością o poprawność (aktualizacja),
- przez czas nie dłuższy niż to konieczne,
- przy zapewnieniu integralności i poufności,
- zgodnie z zasadą rozliczalności.

Fundacja stosuje zasadę „privacy by design” oraz „privacy by default”.

§5. Rejestr czynności przetwarzania

Fundacja prowadzi rejestr czynności przetwarzania zgodnie z art. 30 RODO.

Rejestr zawiera m.in. kategorie danych, cele przetwarzania, podstawy prawne, odbiorców danych, terminy przechowywania oraz opis zastosowanych zabezpieczeń.

Rejestr jest aktualizowany nie rzadziej niż raz na kwartał lub każdorazowo w razie zmiany sposobu przetwarzania.

Dla projektów realizowanych w ramach programu Erasmus+ fundacja prowadzi wyodrębniony Rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora danych (Komisji Europejskiej: Edukacja, Młodzież, Sport i Kultura (EAC)).

Rozdział IV. Środki bezpieczeństwa i organizacja ochrony danych

§6. Środki techniczne i organizacyjne

Fundacja stosuje adekwatne do poziomu ryzyka środki ochrony danych, w tym:

- pseudonimizację i szyfrowanie danych osobowych (dane szczególne oraz dane wrażliwe są szyfrowane lub zabezpieczane hasłami),
- środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów,
- regularne testowanie i ocenę skuteczności środków zabezpieczających.

Fundacja wdrożyła zasady:

- czystego biurka – dokumenty zawierające dane osobowe nie mogą być pozostawione na wierzchu; po zakończeniu pracy powinny być zabezpieczone w zamkniętych szafkach lub niszczone,

- czystego ekranu – obowiązek blokowania komputera za każdym razem, gdy pracownik odchodzi od stanowiska,

- segmentacji dostępu – tylko osoby upoważnione mają dostęp do określonych kategorii danych,

- rejestracji operacji – wszelkie operacje na danych podlegają ewidencji.

W przypadku przetwarzania danych w formie papierowej:

- dokumentacja musi być przechowywana w zamkniętej szafie pancernej, do której klucze posiadają wyłącznie osoby uprawnione,

- dokumenty po wykorzystaniu muszą być niszczone w niszczarkach spełniających standardy DIN 66399 (minimum poziom P-4).

§7. Szyfrowanie i bezpieczeństwo cyfrowe

Szyfrowanie stosowane jest w szczególności w odniesieniu do:

- przesyłania danych osobowych drogą elektroniczną (np. za pomocą haseł do plików .zip lub za pomocą komunikatorów z szyfrowaniem end-to-end),

- przechowywania baz danych z danymi wrażliwymi,

- nośników zewnętrznych (np. pendrive, dyski przenośne).

Komputery, serwery i urządzenia mobilne Fundacji:

- zabezpieczone są hasłami z odpowiednim poziomem złożoności,

- mają aktywne programy antywirusowe i zaporę sieciową,

- regularnie aktualizowane systemy operacyjne i oprogramowanie.

Rozdział V. Pracownicy, szkolenia i dostęp

§8. Obowiązki personelu

Każda osoba przetwarzająca dane na rzecz Fundacji (pracownik, wolontariusz, współpracownik):

- podpisuje oświadczenie o poufności,

- otrzymuje indywidualne upoważnienie do przetwarzania danych,

- przeszkolona jest w zakresie ochrony danych osobowych przed rozpoczęciem pracy,

- zobowiązana jest do nieudostępniania danych osobom nieupoważnionym.

Fundacja prowadzi rejestr upoważnień do przetwarzania danych osobowych, który zawiera:

- imię i nazwisko osoby upoważnionej,

- zakres dostępu,

- datę nadania upoważnienia i wygaśnięcia.

§9. Szkolenia

Fundacja zapewnia cykliczne szkolenia w zakresie RODO dla całego personelu.

Szkolenia obejmują m.in.:

- zasady przetwarzania danych,

- stosowanie polityki czystego biurka i ekranu,

- reakcję na naruszenia ochrony danych,

- procedury zgłaszania incydentów.

Rozdział VI. Inspektor ochrony danych

1. Fundacja jako administrator lub podmiot przetwarzający na dużą skalę dane szczególnych kategorii wyznacza inspektora ochrony danych osobowych.

2. Inspektor ochrony danych został wyznaczony na podstawie jego kwalifikacji zawodowych, w tym wiedzy oraz zdobytego doświadczenia, które to kwalifikacje zostały udokumentowane.
3. Administrator stwarza inspektorowi ochrony danych odpowiednie warunki, aby mógł realizować swoje obowiązki, w szczególności poprzez:
a) niezwłoczne oraz odpowiednie włączanie go we wszystkie sprawy dotyczące ochrony danych osobowych,
b) zapewnienie zasobów niezbędnych do wykonywania jego zadań oraz utrzymania jego fachowej wiedzy,
c) zapewnienie mu niezależności w sprawowaniu jego funkcji, m.in. poprzez niewydawanie instrukcji dotyczących wykonywania przez niego jego zadań, nieponoszenie przez inspektora negatywnych konsekwencji za wypełnianie przez niego jego zadań, zapewnienie odpowiedniej struktury organizacyjnej aby podlegał jedynie Zarządowi.

4. Zadania inspektora ochrony danych obejmują w szczególności:
a) podnoszenie świadomości wśród personelu przetwarzającego dane osobowe oraz podmiotów przetwarzających dane osobowe na zlecenie administratora, poprzez realizację szkoleń oraz informowanie o obowiązkach spoczywających na tych osobach i podmiotach;
b) monitorowanie przestrzegania przez Administratora przepisów Rozporządzenia i innych przepisów prawa ochrony danych osobowych oraz regulacji wewnętrznych przyjętych u administratora regulujących kwestie związane z przetwarzaniem danych osobowych;
c) wykonywanie audytów w kwestiach związanych z przetwarzaniem danych osobowych;
d) uczestniczenie oraz wspieranie administratora w dokonywaniu oceny skutków dla ochrony danych oraz monitorowanie wykonania oceny tych skutków;
e) współpraca z Urzędem Ochrony Danych Osobowych;
f) sprawowanie funkcji punktu kontaktowego dla osób, których dane dotyczą w kwestiach związanych z przetwarzaniem danych osobowych.

Rozdział VII. Dane szczególnych kategorii

§10. Zasady szczególnej ochrony

Fundacja przetwarza dane szczególnych kategorii wyłącznie w przypadkach przewidzianych przez prawo, w szczególności:

- na podstawie wyraźnej zgody osoby, której dane dotyczą (art. 9 ust. 2 lit. a RODO),
- w celu wykonania obowiązków wynikających z przepisów prawa pracy i ubezpieczeń społecznych,

- w celu ochrony żywotnych interesów osoby, której dane dotyczą.

Dane te są przetwarzane w systemach posiadających:

- szyfrowanie,

- rejestrację dostępu,

- rozdzielenie uprawnień administracyjnych i operacyjnych.

Dostęp do danych szczególnych kategorii mają tylko osoby wyznaczone przez Zarząd Fundacji i imiennie upoważnione.

Rozdział VIII. Komunikacja e-mailowa i UDW

§11. Bezpieczne wysyłanie wiadomości e-mail

Wysyłając wiadomości e-mail do wielu adresatów, Fundacja:

- zawsze stosuje pole „Ukryta kopia” (UDW / BCC),

- nie umieszcza adresów e-mail w polu „Do” lub „DW” w sposób umożliwiający ich widoczność dla innych odbiorców.

W przypadku przesyłania dokumentów zawierających dane osobowe pliki są szyfrowane – oddzielne przekazanie hasła (np. SMS-em),

Fundacja nie wysyła danych osobowych przez nieautoryzowane komunikatory lub aplikacje bez szyfrowania.

Rozdział IX. Naruszenia ochrony danych i zgłaszanie incydentów

§12. Reakcja na incydenty

W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, każda osoba związana z Fundacją ma obowiązek niezwłocznie:

- powiadomić Inspektora Ochrony Danych lub wyznaczoną osobę odpowiedzialną,

- wypełnić formularz zgłoszenia incydentu.

Fundacja prowadzi rejestr naruszeń i incydentów oraz podejmuje działania naprawcze i zapobiegawcze.

W razie konieczności, Fundacja zgłasza naruszenie do Urzędu Ochrony Danych Osobowych (UODO) w terminie do 72 godzin oraz – jeśli wymagane – informuje osobę, której dane dotyczą.

Rozdział X. Przechowywanie i usuwanie danych

1. Fundacja przechowuje dane osobowe przez okres niezbędny do realizacji celu, w jakim zostały zebrane, z uwzględnieniem obowiązków prawnych dotyczących archiwizacji.

2. Po upływie wymaganego okresu dane są:
- trwale usuwane z systemów informatycznych,
- niszczone mechanicznie (w przypadku dokumentów papierowych),
- poddawane procedurze anonimizacji (jeśli wymagane jest ich dalsze przetwarzanie statystyczne).

3. Fundacja prowadzi ewidencję zniszczeń dokumentów zawierających dane osobowe.

Rozdział XI. Przekazywanie danych poza EOG

1. Dane osobowe co do zasady nie są przekazywane poza Europejski Obszar Gospodarczy (EOG).

2. Jeżeli przekazanie takie jest konieczne, Fundacja:
- stosuje odpowiednie środki ochrony (np. standardowe klauzule umowne, TIA),
- dokumentuje ocenę ryzyka i podstawę prawną przekazania danych,
- informuje osoby, których dane dotyczą, o przekazaniu danych.

3. Wszystkie przypadki przekazywania danych poza EOG są rejestrowane w Rejestrze Czynności Przetwarzania.

Rozdział XII. Prawa osób, których dane są przetwarzane

§13. Prawo do informacji

1. Osoby, których dane dotyczą, są informowane przez administratora o sposobie przetwarzania ich danych osobowych oraz przysługującym ich uprawnieniach w formie klauzuli informacyjnej, z którą mogą zapoznać się w każdej chwili w siedzibie administratora, jego jednostkach organizacyjnych oraz na stronie internetowej.

2. Klauzula informacyjna jest wydawana w czasie wyrażania zgody na przetwarzanie danych osobowych.

3. Klauzula informacyjna jest sporządzona prostym językiem, w sposób przejrzysty i wyczerpuje wszystkie informacje zgodnie z art. 13 oraz 14 RODO.

§ 14
Prawo dostępu do danych

1. Na żądanie osoby, której dane dotyczą, administrator udziela jej informacji o sposobie przetwarzania jego danych osobowych. Na żądanie osoby, której dane dotyczą, administrator udostępnia mu nieodpłatnie pierwszą kopię jego danych osobowych; za każdą kolejną kopię administrator może pobrać opłatę w rozsądnej wysokości.

2. Jeżeli żądanie wydania kopii danych zostało złożone administratorowi w formie elektronicznej a osoba, której dane dotyczą nie zaznacza inaczej - kopia wydawana jest w tej samej formie.

3. Administrator może udostępnić kopię w inny sposób, niż wybrany przez osobę, której dane dotyczą, jeżeli ze względów technicznych nie jest to możliwe (np. ze względu na wagę pliku w wersji elektronicznej); o niemożności dostarczenia kopii w wybrany przez osobę, której dane dotyczą, sposób oraz proponowanym alternatywnym rozwiązaniu administrator niezwłocznie powiadamia tę osobę.

§ 15
Prawo do sprostowania danych

1. Administrator umożliwia osobie, której dane dotyczą, niezwłoczne sprostowanie jego danych osobowych, jeżeli są one nieprawidłowe lub nieaktualne, lub ich uzupełnienie.

2. Administrator może żądać od osoby, której dane dotyczą, stosownych dokumentów w celu okazania, aby ustalić zasadność oraz zgodność z prawem dokonywanej zmiany danych osobowych.

§ 16
Prawo do usunięcia, ograniczenia i przenoszenia danych

1. Administrator usuwa bez zbędnej zwłoki dane osobowe osoby, której dane dotyczą, na jej żądanie, jeżeli na administratorze nie spoczywają obowiązki nakazujące dalsze przetwarzanie danych osobowych.

2. Odmowa realizacji prawa do usunięcia danych jest przekazywana przez administratora osobie, której dane dotyczą, wraz z uzasadnieniem przyczyny odmowy zawierającym podstawy prawne odmowy.

3. Na żądanie osoby, której dane dotyczą, administrator dokonuje ograniczenia przetwarzania jej danych osobowych.

4. Na żądanie osoby administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.

§ 17
Prawo do sprzeciwu

Jeżeli osoba, której dane dotyczą zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po jego stronie ważne

prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, albo zaistnieją podstawy do ustalenia, dochodzenia lub obrony roszczeń.

Rozdział XIII. Ryzyko

§18. Metodologia oceny ryzyka

Fundacja, jako administrator danych osobowych (lub podmiot je przetwarzający), prowadzi ocenę ryzyka w celu określenia i zminimalizowania zagrożeń związanych z przetwarzaniem danych osobowych. Przyjmuje się metodę jakościowo-ilościową, łączącą analizę kontekstu funkcjonowania z przypisaniem wartości liczbowych dla prawdopodobieństwa oraz skutków zagrożeń.

Przy wyznaczeniu poziomu ryzyka uwzględniane są następujące czynniki wpływające na prawdopodobieństwo wystąpienia incydentu: a) kontekst wewnętrzny i zewnętrzny funkcjonowania Fundacji,
b) brak konieczności wykonywania oceny skutków dla ochrony danych osobowych,
c) statystyki dotychczasowych zdarzeń i incydentów,
d) atrakcyjność danych i zasobów wspierających (sprzęt, oprogramowanie, personel, lokalizacja),
e) czynniki środowiskowe (fizyczne, klimatyczne, lokalizacyjne),
f) istniejące organizacyjne i techniczne środki ochrony,
g) podatności infrastruktury technicznej,
h) zgłoszenia i informacje pozyskiwane od użytkowników systemów.

Przyjmuje się pięciostopniową skalę prawdopodobieństwa wystąpienia zagrożenia:

- prawie pewne – 5
- prawdopodobne – 4
- możliwe – 3
- mało prawdopodobne – 2
- minimalne – 1

Równocześnie określana jest waga skutku, w przypadku materializacji zagrożenia:

- bardzo wysoki – 5

- wysoki – 4
- średni – 3
- niski – 2
- bardzo niski – 1

Poziom ryzyka (R) wyliczany jest według wzoru:
R = P × S,
gdzie:

R – poziom ryzyka,
P – prawdopodobieństwo wystąpienia zagrożenia,
S – skutek (waga skutku) danego incydentu.

§19. Macierz ryzyka

Prawdopodobieństwo \ Skutek	1 (bardzo niski)	2 (niski)	3 (średni)	4 (wysoki)	5 (bardzo wysoki)
5 – prawie pewne	5	10	15	20	25
4 – prawdopodobne	4	8	12	16	20
3 – możliwe	3	6	9	12	15
2 – mało prawdopodobne	2	4	6	8	10
1 – minimalne	1	2	3	4	5

§21. Poziomy ryzyka

Na podstawie macierzy ryzyka, Fundacja przyjmuje następujące cztery poziomy ryzyka:

a) bardzo niski (1–3) – poziom akceptowalny, nie wymaga działań korygujących,
b) niski (4–6) – poziom akceptowalny, decyzja o ewentualnym działaniu pozostaje w gestii Administratora,
c) średni (7–12) – poziom akceptowalny, ale wymagający rozważenia środków zaradczych,
d) wysoki (13–25) – poziom nieakceptowalny, wymagający niezwłocznego wdrożenia działań zaradczych i/lub korygujących.

§22. Postępowanie z ryzykiem

Fundacja stosuje cztery możliwe scenariusze zarządzania ryzykiem:

- Redukcja ryzyka – wprowadzenie środków ograniczających prawdopodobieństwo lub skutki (np. wdrożenie kopii zapasowych z większą częstotliwością, zabezpieczenia UPS, automatyczne logowanie i backup).

- Akceptacja ryzyka – świadoma decyzja o niepodejmowaniu działań, gdy poziom ryzyka jest niski lub bardzo niski.

- Unikanie ryzyka – zmiana procesów lub zaniechanie działań powodujących powstawanie ryzyk (np. rezygnacja z pewnych zbędnych systemów gromadzących dane).

- Przeniesienie ryzyka – np. przez zawarcie umowy ubezpieczeniowej lub powierzenie przetwarzania kontrahentowi, z jednoczesnym zapewnieniem zgodności z RODO.

§23. Procedura i dokumentacja

Ocena ryzyka prowadzona jest:

- co najmniej raz do roku,

- każdorazowo w przypadku zmiany technologii, zakresu przetwarzania lub po incydencie.

Oceny dokonuje Administrator lub osoba przez niego wyznaczona, przy użyciu Arkusza oceny ryzyka, który stanowi załącznik do niniejszej Polityki.

Dokumentacja obejmuje:

- opis ryzyk,

- ich oceny (P, S, R),

- decyzję o sposobie postępowania,

- plan wdrożenia działań zaradczych (jeśli wymagane),

- daty i podpisy odpowiedzialnych osób.

Rozdział XIV. Pozostałe dokumenty

1. Administrator opracowuje i wdraża szczególne dokumenty, zapewniające transparentność i bezpieczeństwo przetwarzania danych osobowych.

2. Załącznikami do niniejszej Polityki są:
a) wzór arkuszu oceny ryzyka,
b) rejestr czynności przetwarzania,
c) rejestr upoważnień do przetwarzania danych osobowych,
d) wzór upoważnienia do przetwarzania danych osobowych
e) rejestr naruszeń ochrony danych osobowych,
f) wzór umowy powierzenia przetwarzania danych osobowych,
g) wzór ogólnej zgody na przetwarzanie danych osobowych oraz klauzuli informacyjnej,
h) wzór zgody na przetwarzanie danych medycznych dla podopiecznych Administratora oraz przeznaczona dla nich klauzula informacyjna,
i) wzór zgody na przetwarzanie danych medycznych dla podopiecznych Administratora oraz przeznaczona dla nich klauzula informacyjna, wyrażanej za pośrednictwem strony internetowej,
j) wzór zgody na przetwarzanie danych medycznych dla osób, które chorowały na chorobę rzadką lub ultrarzadką oraz przeznaczona dla nich klauzula informacyjna,
k) wzór upoważnienia do dostępu do dokumentacji medycznej i do informacji o stanie zdrowia,
l) opis technicznych i organizacyjnych środków zabezpieczeń.

3. Administrator stosuje zabezpieczenia techniczne i organizacyjne danych osobowych w sposób opisany w Opisie technicznych i organizacyjnych środków zabezpieczeń, stanowiącym załącznik do niniejszej Polityki.