WZÓR

Polityka ochrony danych

dla organizacji pozarządowych

Opracowanie: Fundacja LegisLab

Stan prawny na dzień: wrzesień 2026 r.

Wzór ma charakter pomocniczy i nie stanowi porady prawnej. Przed zawarciem umowy należy dostosować jej treść do rzeczywistego zakresu powierzenia danych osobowych w danej organizacji.

Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0.

Program finansowany jest przez Unię Europejską. Wyrażone opinie i poglądy są wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii

Europejskiej lub Komisji Europejskiej. Ani Unia Europejska, ani organ przyznający finansowanie nie mogą ponosić za nie odpowiedzialności.

I. UCHWAŁA ZARZĄDU FUNDACJI [NAZWA FUNDACJI]

1. nr [do uzupełnienia] z dnia [do uzupełnienia]

2. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych

Zarząd Fundacji [nazwa Fundacji] z siedzibą w [miejscowość], wpisanej do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego pod numerem KRS [do uzupełnienia], działając na podstawie postanowień statutu Fundacji oraz stosownie do wymogów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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), uchwala, co następuje:

§ 1

Zarząd przyjmuje Politykę Ochrony Danych Osobowych Fundacji [nazwa Fundacji] w brzmieniu stanowiącym załącznik do niniejszej uchwały.

§ 2

Polityka Ochrony Danych Osobowych stanowi wewnętrzny dokument Fundacji określający zasady przetwarzania i ochrony danych osobowych, organizację ochrony danych, środki bezpieczeństwa, procedury reagowania na naruszenia oraz reguły dokumentowania zgodności z przepisami o ochronie danych osobowych.

§ 3

Polityka Ochrony Danych Osobowych wchodzi w życie z dniem [do uzupełnienia].

§ 4

Wszyscy członkowie zarządu, pracownicy, współpracownicy, wolontariusze, stażyści, eksperci oraz inne osoby działające na rzecz Fundacji i mające dostęp do danych osobowych są zobowiązani do zapoznania się z treścią Polityki Ochrony Danych Osobowych oraz do przestrzegania jej postanowień, co potwierdzają podpisem złożonym na Oświadczeniu o zachowaniu poufności (Załącznik nr 3 do Polityki).

§ 5

Instrukcja do szablonu, usunąć przed przyjęciem dokumentu: wybierz jeden z poniższych wariantów odpowiadający sytuacji Fundacji. Usuń wariant, który nie dotyczy Fundacji, wraz z jego nagłówkiem.

Wariant A – Fundacja wyznaczyła Inspektora Ochrony Danych:

Nadzór nad wdrożeniem i bieżącą realizacją Polityki Ochrony Danych Osobowych sprawuje Inspektor Ochrony Danych wyznaczony przez Fundację. Dane kontaktowe IOD: [imię i nazwisko, adres e-mail, do uzupełnienia]. Zarząd zapewnia IOD zasoby i wsparcie niezbędne do wykonywania jego zadań oraz niezwłocznie informuje o ewentualnej zmianie danych kontaktowych IOD.

Wariant B – Fundacja nie wyznaczyła Inspektora Ochrony Danych:

Bieżącą koordynację ochrony danych osobowych w Fundacji sprawuje [imię i nazwisko] pełniący/a funkcję [stanowisko lub rola w Fundacji, do uzupełnienia]. Osoba ta nie jest Inspektorem Ochrony Danych w rozumieniu RODO. Za decyzje w zakresie ochrony danych odpowiada zarząd Fundacji. Dane kontaktowe koordynatora: [adres e-mail, do uzupełnienia].

§ 6

Niniejsza uchwała zastępuje wszelkie wcześniej obowiązujące wewnętrzne regulacje Fundacji w zakresie ochrony danych osobowych. [Usunąć, jeżeli nie dotyczy – jeżeli nie było wcześniejszych regulacji w tym zakresie.]

§ 7

Uchwała wchodzi w życie z dniem podpisania.

[Miejscowość], dnia [do uzupełnienia]

Imię i nazwisko	Funkcja w zarządzie	Podpis
[do uzupełnienia]	[do uzupełnienia]	……..……..
[do uzupełnienia]	[do uzupełnienia]	……
[do uzupełnienia]	[do uzupełnienia]	……

Dofinansowane przez Unię Europejską

sieć splot wartości

Wzór opracowany przez Fundację LegisLab. Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

POLITYKA OCHRONY DANYCH OSOBOWYCH FUNDACJI [NAZWA FUNDACJI]

Wersja: [do uzupełnienia]

Data wejścia w życie: [do uzupełnienia]

Zatwierdzona uchwałą zarządu nr: [do uzupełnienia] **z dnia:** [do uzupełnienia]

Dofinansowane przez Unię Europejską

sieć splot wartości

Wzór opracowany przez Fundację LegisLab. Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

Spis treści

I. POSTANOWIENIA OGÓLNE, CEL, ZAKRES I PODSTAWA POLITYKI 6
II. DEFINICJE I SKRÓTY 7
III. ADMINISTRATOR I ORGANIZACJA OCHRONY DANYCH 8
IV. ZASADY PRZETWARZANIA DANYCH I ROZLICZALNOŚĆ 9
V. PROCESY PRZETWARZANIA I DOKUMENTOWANIE ZGODNOŚCI 11
VI. OCENA NOWEGO DZIAŁANIA LUB PROCESU PRZETWARZANIA DANYCH 12
VII. DOPUSZCZANIE OSÓB DO PRZETWARZANIA DANYCH 13
VIII. ŚRODKI ORGANIZACYJNE I PODSTAWOWE ŚRODKI TECHNICZNE 14
IX. OBOWIĄZEK INFORMACYJNY I REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ 16
X. DANE SZCZEGÓLNEJ KATEGORII I DANE DZIECI 18
XI. PODMIOTY ZEWNĘTRZNE: POWIERZENIE, UDOSTĘPNIENIE I WSPÓŁADMINISTROWANIE 19
XII. PRZEKAZYWANIE DANYCH POZA EUROPEJSKI OBSZAR GOSPODARCZY 20
XIII. REAGOWANIE NA INCYDENTY I NARUSZENIA OCHRONY DANYCH 21
XIV. RETENCJA, ARCHIWIZACJA I USUWANIE DANYCH 23
XV. SZKOLENIA, KONTROLA I PRZEGLĄD POLITYKI 24
XVI. POSTANOWIENIA KOŃCOWE 24
XVII. Załączniki ..... **Błąd! Nie zdefiniowano zakładki.**

Dofinansowane przez Unię Europejską

sieć splot wartości

Wzór opracowany przez Fundację LegisLab. Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

II. POSTANOWIENIA OGÓLNE, CEL, ZAKRES I PODSTAWA POLITYKI

1. Niniejsza Polityka Ochrony Danych Osobowych, zwana dalej Polityką, stanowi wewnętrzny dokument Fundacji [nazwa Fundacji] z siedzibą w [adres siedziby, do uzupełnienia], określający zasady przetwarzania danych osobowych, organizację ochrony danych, stosowane środki bezpieczeństwa oraz reguły dokumentowania zgodności z przepisami o ochronie danych osobowych.

2. Celem Polityki jest zapewnienie, że przetwarzanie danych osobowych w Fundacji odbywa się:

    a. zgodnie z prawem – na właściwej podstawie prawnej i z poszanowaniem zasad wynikających z RODO,

    b. rzetelnie i w sposób przejrzysty wobec osób, których dane dotyczą,

    c. bezpiecznie – z zastosowaniem środków ochrony odpowiednich do ryzyka i skali działalności Fundacji,

    d. w sposób rozliczalny – tak, aby Fundacja mogła wykazać przestrzeganie zasad przetwarzania danych i spełnianie wymagań przepisów.

3. Zakres podmiotowy Polityki obejmuje wszystkie osoby mające dostęp do danych osobowych przetwarzanych przez Fundację, w szczególności:

    a. członków zarządu,

    b. pracowników,

    c. współpracowników, w tym osoby świadczące usługi na podstawie umów cywilnoprawnych,

    d. wolontariuszy,

    e. stażystów i praktykantów,

    f. ekspertów i konsultantów,

    g. inne osoby działające na rzecz Fundacji lub z upoważnienia Fundacji.

4. Zakres przedmiotowy Polityki obejmuje wszystkie dane osobowe przetwarzane przez Fundację, niezależnie od formy przetwarzania (papierowa i elektroniczna), miejsca przetwarzania (siedziba, praca zdalna, wyjazdy służbowe), używanych narzędzi (systemy, aplikacje, poczta elektroniczna, chmura) oraz nośników (komputery, telefony, dyski, dokumenty papierowe).

5. Polityka stanowi dokument wewnętrzny Fundacji. Nie jest przeznaczona do publicznego udostępniania jako całość. Udostępnia się ją osobom wymienionym w ust. 3, na zasadach określonych w rozdziale XV.
6. Podstawę prawną Polityki stanowią w szczególności przepisy RODO, nakładające na administratora danych osobowych obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania z przepisami o ochronie danych oraz zdolność do wykazania tej zgodności.

III. DEFINICJE I SKRÓTY

1. Na potrzeby niniejszej Polityki stosuje się następujące definicje:

    a. Administrator – Fundacja [nazwa Fundacji], która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych przetwarzanych w ramach swojej działalności.

    b. Dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

    c. Przetwarzanie – każda operacja lub zestaw operacji wykonywanych na danych osobowych, m.in. zbieranie, utrwalanie, przechowywanie, modyfikowanie, przeglądanie, wykorzystywanie, udostępnianie, ograniczanie, usuwanie lub niszczenie.

    d. Osoba upoważniona – osoba, której Fundacja nadała pisemne upoważnienie do przetwarzania danych osobowych.

    e. Podmiot przetwarzający (procesor) – podmiot zewnętrzny, który przetwarza dane osobowe w imieniu Fundacji na podstawie umowy powierzenia przetwarzania, wyłącznie na polecenie Fundacji i w zakresie przez nią określonym.

    f. Incydent – zdarzenie, które zagraża lub może zagrażać bezpieczeństwu danych osobowych przetwarzanych przez Fundację.

    g. Naruszenie ochrony danych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

    h. Dane szczególnej kategorii – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne; dane biometryczne przetwarzane w celu jednoznacznej identyfikacji osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

2. Na potrzeby Polityki stosuje się następujące skróty:

   a. RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych).

   b. IOD (Inspektor Ochrony Danych) – osoba wyznaczona przez administratora lub podmiot przetwarzający zgodnie z wymogami RODO, wykonująca zadania określone w RODO. [Zachowaj wyłącznie jeżeli Fundacja wyznaczyła IOD – Wariant A. Usuń, jeżeli nie dotyczy.]

   c. EOG (Europejski Obszar Gospodarczy) – obszar obejmujący państwa członkowskie Unii Europejskiej oraz Norwegię, Islandię i Liechtenstein.

   d. RCP (Rejestr Czynności Przetwarzania) – rejestr, o którym mowa w rozdziale V ust. 2 i Załączniku nr 1 do Polityki.

IV. ADMINISTRATOR I ORGANIZACJA OCHRONY DANYCH

1. Administratorem danych osobowych przetwarzanych w związku z działalnością Fundacji jest Fundacja [nazwa Fundacji] z siedzibą w [adres do uzupełnienia], wpisana do Krajowego Rejestru Sądowego pod numerem [do uzupełnienia], posiadająca NIP [do uzupełnienia], zwana dalej „Fundacją".

2. W sprawach dotyczących przetwarzania danych osobowych oraz realizacji praw osób, których dane dotyczą, można kontaktować się z Fundacją drogą elektroniczną, pod adresem e-mail: [do uzupełnienia, np. dane@fundacja.pl], albo pisemnie, na adres jej siedziby wskazany w ust. 1.

Wariant A – Fundacja wyznaczyła Inspektora Ochrony Danych:

3. Fundacja wyznaczyła Inspektora Ochrony Danych, z którym można kontaktować się we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz wykonywania praw przysługujących osobom, których dane dotyczą. Dane kontaktowe Inspektora Ochrony Danych są następujące: imię i nazwisko: [do uzupełnienia], adres e-mail: [do uzupełnienia], adres do korespondencji: [do uzupełnienia; może być adres siedziby Fundacji].

4. IOD wykonuje swoje zadania w sposób niezależny. Nie przyjmuje instrukcji dotyczących sposobu realizacji tych zadań. W szczególności IOD informuje i doradza w zakresie przepisów o ochronie danych i polityk wewnętrznych, monitoruje przestrzeganie przepisów, wspiera przy ocenie skutków dla ochrony danych, pełni funkcję punktu kontaktowego wobec Prezesa UODO oraz jest włączany we wszystkie

istotne sprawy dotyczące ochrony danych osobowych, w tym przeglądy Polityki i oceny nowych procesów.

Wariant B – Fundacja nie wyznaczyła Inspektora Ochrony Danych:

5. Fundacja nie wyznaczyła Inspektora Ochrony Danych. Bieżącą koordynację działań związanych z ochroną danych osobowych sprawuje [imię i nazwisko], pełniący/-a w Fundacji funkcję [rola w Fundacji], z którym/-ą można kontaktować się pod adresem e-mail: [do uzupełnienia].
6. Osoba ta nie jest Inspektorem Ochrony Danych w rozumieniu RODO. Koordynuje działania związane z ochroną danych, przyjmuje zgłoszenia incydentów, prowadzi rejestry i wspiera zarząd w realizacji obowiązków wynikających z RODO. Za decyzje w zakresie ochrony danych osobowych, w tym zgłoszenia naruszeń do organu nadzorczego, odpowiada zarząd Fundacji.
7. Osoby pełniące Funkcję w ramach fundacji mają następujące odpowiedzialności w zakresie ochrony danych:
    a. **Zarząd Fundacji** – odpowiada za zapewnienie zgodności działania Fundacji z przepisami o ochronie danych osobowych, wdrożenie i aktualizację Polityki, zapewnienie odpowiednich środków technicznych i organizacyjnych, podejmowanie decyzji dotyczących ochrony danych, w tym dotyczących zgłoszenia naruszeń do Prezesa UODO i zawiadomień osób.
    b. **IOD (Wariant A) lub koordynator ochrony danych (Wariant B)** – wspiera zarząd i osoby upoważnione w realizacji obowiązków wynikających z Polityki i RODO; przyjmuje i rejestruje zgłoszenia incydentów; prowadzi lub nadzoruje prowadzenie rejestrów wskazanych w rozdziale V; pełni funkcję punktu kontaktowego w sprawach ochrony danych.
    c. **Osoby odpowiedzialne za projekty i działania** – dbają o to, aby nowe działania były oceniane pod kątem ochrony danych przed ich uruchomieniem (wypełniają Kartę oceny – Załącznik nr 8); stosują zasady minimalizacji i celowości; niezwłocznie zgłaszają nowe lub istotnie zmienione procesy przetwarzania.
    d. **Osoby upoważnione** – przetwarzają dane wyłącznie w zakresie nadanego upoważnienia i w celach wskazanych przez Fundację; stosują zasady i środki bezpieczeństwa określone w Polityce; niezwłocznie zgłaszają incydenty i podejrzenia naruszeń.

V. ZASADY PRZETWARZANIA DANYCH I ROZLICZALNOŚĆ

1. Fundacja przetwarza dane osobowe zgodnie z następującymi zasadami:

a. **zgodności z prawem, rzetelności i przejrzystości** – dane są przetwarzane wyłącznie na podstawie właściwej przesłanki prawnej; wobec osób, których dane dotyczą, wykonuje się obowiązek informacyjny w sposób jasny i zrozumiały.

b. **ograniczenia celu** – dane zbiera się w konkretnych, wyraźnych i prawnie uzasadnionych celach; nie przetwarza się ich w sposób niezgodny z tymi celami.

c. **minimalizacji danych** – zbiera się i przetwarza wyłącznie dane adekwatne, stosowne i niezbędne do osiągnięcia celu. przed zebraniem danych Fundacja ocenia, które informacje są naprawdę potrzebne.

d. **prawidłowości** – dane są prawidłowe i w razie potrzeby aktualizowane; błędne lub nieaktualne dane są niezwłocznie poprawiane lub usuwane.

e. **ograniczenia przechowywania** – dane przechowuje się przez okres niezbędny do realizacji celu, chyba że przepisy prawa wymagają dłuższego przechowywania lub dane są niezbędne do dochodzenia lub ochrony roszczeń. Po upływie okresu retencji dane są usuwane lub skutecznie anonimizowane.

f. **integralności i poufności** – dane są chronione przed nieuprawnionym dostępem, ujawnieniem, utratą, zniszczeniem lub modyfikacją, z zastosowaniem odpowiednich środków technicznych i organizacyjnych.

g. **rozliczalności** – fundacja jest w stanie wykazać, że przestrzega zasad przetwarzania danych i spełnia obowiązki wynikające z RODO. Służą temu rejestry, dokumentacja i procedury opisane w niniejszej Polityce.

2. Fundacja wdraża ochronę danych już na etapie projektowania działań (**privacy by design**). Przed uruchomieniem nowego projektu, narzędzia lub procesu przetwarzania ocenia, jakie dane będą potrzebne, w jaki sposób będą przetwarzane i jak należy je zabezpieczyć, jeszcze zanim działanie zostanie uruchomione.

3. Fundacja stosuje zasadę domyślnej ochrony danych (**privacy by default**). Jeżeli dla danego celu nie jest konieczne przetwarzanie określonego zakresu danych, Fundacja nie zbiera tych danych. Domyślnie przetwarza się wyłącznie dane niezbędne do konkretnego celu.

4. Przed podjęciem nowego działania lub uruchomieniem nowego procesu przetwarzania danych osobowych osoba odpowiedzialna za to działanie ma obowiązek ocenić, czy i jakie dane osobowe będą przetwarzane, na jakiej podstawie, przez kogo, przez jaki czas i jakie ryzyka wiążą się z tym przetwarzaniem. Służy temu Karta oceny nowego działania lub procesu przetwarzania danych osobowych stanowiąca Załącznik nr 8 do Polityki.

VI. PROCESY PRZETWARZANIA I DOKUMENTOWANIE ZGODNOŚCI

1. Fundacja identyfikuje i dokumentuje wszystkie procesy przetwarzania danych osobowych związane ze swoją działalnością.

2. Fundacja prowadzi Rejestr Czynności Przetwarzania (RCP), stanowiący Załącznik nr 1 do niniejszej Polityki. RCP jest prowadzony w formie [elektronicznej / papierowej – wybrać właściwy wariant] i jest na bieżąco aktualizowany. Za prowadzenie i aktualizację RCP odpowiada [IOD / koordynator ochrony danych – wybrać właściwy wariant].

3. Fundacja prowadzi ponadto następującą dokumentację:
    a. ewidencję osób upoważnionych do przetwarzania danych (Załącznik nr 4),
    b. rejestr naruszeń ochrony danych osobowych (Załącznik nr 6),
    c. rejestr żądań osób, których dane dotyczą (Załącznik nr 7),
    d. wykaz podmiotów przetwarzających (Załącznik nr 9).

4. Fundacja stosuje klauzule informacyjne właściwe dla każdego procesu przetwarzania, dostosowane do grup osób, których dane dotyczą. Klauzule informacyjne mogą być wdrażane jako odrębne dokumenty, niestanowiące części niniejszej Polityki.

5. Każda osoba odpowiedzialna za nowe działanie lub istotną zmianę istniejącego działania ma obowiązek zgłosić ten fakt [IOD / koordynatorowi ochrony danych – wybrać właściwy wariant] przed uruchomieniem działania lub zmiany oraz wypełnić Kartę oceny (Załącznik nr 8).

6. Typowe procesy przetwarzania danych w fundacjach i organizacjach pozarządowych obejmują m.in. poniższe obszary (katalog przykładowy i otwarty):
    a. realizację działań statutowych i projektowych, w tym rekrutację uczestników,
    b. organizację wydarzeń, szkoleń, warsztatów i konferencji,
    c. wolontariat – nawiązanie, realizację i zakończenie współpracy,
    d. obsługę darowizn i korespondencję z darczyńcami,
    e. współpracę z ekspertami i konsultantami,
    f. obsługę zatrudnienia i umów cywilnoprawnych,
    g. obsługę finansowo-księgową i sprawozdawczość,
    h. korespondencję z partnerami, kontrahentami i instytucjami,

i. komunikację zewnętrzną (newsletter, media społecznościowe, formularze online),

j. korzystanie ze strony internetowej i narzędzi elektronicznych.

7. Każdy z tych procesów powinien być ujęty w RCP, o ile wiąże się z przetwarzaniem danych osobowych.

VII. OCENA NOWEGO DZIAŁANIA LUB PROCESU PRZETWARZANIA DANYCH

1. Przed uruchomieniem nowego działania lub istotną zmianą działania już prowadzonego osoba odpowiedzialna za to działanie ma obowiązek wypełnić Kartę oceny nowego działania lub procesu przetwarzania danych osobowych, stanowiącą Załącznik nr 8 do niniejszej Polityki.

2. Karta oceny służy:

   a. ustaleniu, czy działanie wiąże się z przetwarzaniem danych osobowych,

   b. określeniu celu, podstawy prawnej i zakresu przetwarzania,

   c. ocenie minimalizacji danych,

   d. zidentyfikowaniu odbiorców, podmiotów przetwarzających, miejsca przechowywania danych i ewentualnego transferu poza EOG,

   e. ustaleniu okresu retencji,

   f. ocenie podstawowych ryzyk i środków ochrony,

   g. podjęciu decyzji o tym, czy działanie może zostać uruchomione, czy wymaga dalszych kroków.

3. Karta oceny nie jest Oceną Skutków dla Ochrony Danych (DPIA) w rozumieniu RODO. Jest narzędziem wstępnej preselekcji i praktycznej kontroli zgodności przed uruchomieniem działania.

4. Jeżeli wynik Karty oceny wskazuje na możliwość wysokiego ryzyka dla praw i wolności osób, przed uruchomieniem działania przeprowadza się pogłębioną analizę ryzyka. W przypadkach wymaganych przepisami RODO przeprowadza się Ocenę Skutków dla Ochrony Danych (DPIA), której Karta oceny nie zastępuje. O konieczności przeprowadzenia DPIA decyduje [IOD / zarząd – wybrać właściwy wariant] na podstawie wyników Karty oceny.

5. Szczególnej ostrożności i konsultacji z [IOD / koordynatorem / zarządem – wybrać właściwy wariant] wymagają działania obejmujące:

a. dane szczególnej kategorii,

b. dane dzieci lub osób małoletnich,

c. dane osób w kryzysie lub wymagających szczególnego wsparcia,

d. przetwarzanie na szeroką skalę,

e. systematyczne monitorowanie osób,

f. profilowanie lub zautomatyzowane podejmowanie decyzji mające wpływ na osoby,

g. łączenie danych z różnych źródeł,

h. wdrożenie nowej technologii lub narzędzia,

i. transfer danych poza EOG.

VIII. DOPUSZCZANIE OSÓB DO PRZETWARZANIA DANYCH

1. Dostęp do danych osobowych mają wyłącznie osoby, którym jest on niezbędny do wykonywania ich zadań w Fundacji (zasada minimalnych uprawnień i potrzeby dostępu).

2. Podstawą dostępu do danych jest:

   a. pisemne upoważnienie do przetwarzania danych osobowych nadane przez Fundację zgodnie ze wzorem stanowiącym Załącznik nr 2 do Polityki, lub

   b. inna właściwa, udokumentowana podstawa, np. postanowienie umowy zawartej z osobą wykonującą usługi na rzecz Fundacji, jednoznacznie określające zakres dostępu i obowiązki w zakresie ochrony danych.

3. Każda osoba dopuszczona do przetwarzania danych osobowych przed uzyskaniem dostępu:

   a. zapoznaje się z niniejszą Polityką,

   b. odbywa szkolenie lub instruktaż dostosowany do swojej roli (patrz rozdział XV),

   c. podpisuje Oświadczenie o zachowaniu poufności (Załącznik nr 3),

   d. jest wpisywana do Ewidencji osób upoważnionych (Załącznik nr 4).

4. Każda osoba upoważniona korzysta z indywidualnego konta i indywidualnych danych dostępowych. Współdzielenie loginów i haseł jest niedopuszczalne.

5. Zakres dostępu i upoważnienia obejmuje wyłącznie dane niezbędne do wykonywania powierzonych zadań. Osoby upoważnione przetwarzają dane wyłącznie w celach i zakresie wynikającym z nadanego upoważnienia.

6. W przypadku zmiany zakresu zadań lub roli danej osoby upoważnienie jest niezwłocznie aktualizowane. W przypadku zakończenia współpracy z Fundacją upoważnienie jest cofane, dostępy są odbierane, a fakt ten jest odnotowywany w Ewidencji.

7. Fundacja przeprowadza przegląd upoważnień i dostępów nie rzadziej niż raz w roku oraz każdorazowo po istotnych zmianach personalnych lub organizacyjnych.

8. Zasady opisane w niniejszym rozdziale stosuje się do wszystkich osób wymienionych w rozdziale I ust. 3, w tym do wolontariuszy, członków zarządu, stażystów i ekspertów, niezależnie od formy ich zaangażowania w działalność Fundacji.

IX. ŚRODKI ORGANIZACYJNE I PODSTAWOWE ŚRODKI TECHNICZNE

1. Fundacja stosuje środki ochrony adekwatne do ryzyka i skali swojej działalności. Środki opisane w niniejszym rozdziale stanowią minimalny standard wymagany w Fundacji. Bardziej szczegółowe wymagania techniczne mogą zostać określone w odrębnej Polityce Bezpieczeństwa Informacji, jeżeli Fundacja zdecyduje się ją wdrożyć.

2. Środki organizacyjne:

    1) **zasada czystego biurka** – dokumenty zawierające dane osobowe nie są pozostawiane bez nadzoru na biurku, drukarce ani w ogólnie dostępnych miejscach. Po zakończeniu pracy dokumenty są chowane lub zamykane w szafie lub szufladzie.

    2) **zasada czystego ekranu** – ekrany urządzeń są blokowane podczas nieobecności użytkownika; użytkownicy nie pozostawiają otwartych aplikacji z danymi osobowymi bez nadzoru.

    3) **zabezpieczenie dokumentacji papierowej** – dokumenty zawierające dane osobowe są przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych (zamykane szafy, szuflady lub pomieszczenia). Dostęp do dokumentów mają wyłącznie osoby upoważnione.

    4) **niszczenie dokumentów** – dokumenty papierowe zawierające dane osobowe, które nie są już potrzebne, są niszczone w sposób uniemożliwiający ich odczytanie (niszczarka mechaniczna lub udokumentowane przekazanie do

profesjonalnego zniszczenia). Dokumentów z danymi osobowymi nie wrzuca się do otwartych pojemników na odpady.

5) **wydruki** – wydruki zawierające dane osobowe są niezwłocznie odbierane z drukarki. Niepotrzebne wydruki z danymi są niszczone zgodnie z zasadą opisaną powyżej.

6) **dostęp osób postronnych** – osoby nieuprawnione nie mają swobodnego dostępu do miejsc, w których przetwarzane są dane osobowe. W przypadku przyjmowania gości dba się o to, aby dokumenty papierowe i ekrany z danymi osobowymi nie były dla nich widoczne.

7) **praca zdalna i praca poza siedzibą** – osoby przetwarzające dane poza siedzibą Fundacji stosują te same zasady ochrony co w siedzibie: blokują ekrany, nie pozostawiają dokumentów bez nadzoru, unikają przetwarzania danych osobowych w miejscach publicznych przy braku odpowiedniego zabezpieczenia.

8) **transport dokumentów** – dokumenty zawierające dane osobowe przekazywane lub transportowane poza siedzibą Fundacji są zabezpieczone przed dostępem osób nieuprawnionych (np. w zamkniętej teczce; nie są pozostawiane bez nadzoru).

3. Podstawowe środki techniczne:

1) **indywidualne konta** – każda osoba przetwarzająca dane korzysta z indywidualnego konta w systemach, aplikacjach i skrzynkach e-mail. Kont i danych dostępowych nie współdzieli się.

2) **silne hasła** – hasła muszą mieć odpowiednią długość i złożoność; nie używa się tych samych haseł do różnych systemów; haseł nie przekazuje się innym osobom ani nie zapisuje w miejscach dostępnych dla osób nieuprawnionych. Zalecane jest korzystanie z menedżera haseł.

3) **uwierzytelnianie wieloskładnikowe (MFA)** – Fundacja stosuje MFA tam, gdzie jest ono dostępne i adekwatne do ryzyka, w szczególności dla kont pocztowych, chmury i systemów zawierających dane osobowe.

4) **blokowanie urządzeń** – urządzenia blokują się automatycznie po określonym czasie bezczynności; użytkownicy blokują ekrany urządzeń, gdy opuszczają stanowisko.

5) **aktualizacje** – system operacyjny, aplikacje i oprogramowanie zabezpieczające są regularnie aktualizowane; aktualizacje bezpieczeństwa są wdrażane niezwłocznie po ich udostępnieniu przez producenta.

6) **ochrona przed złośliwym oprogramowaniem** – na urządzeniach używanych do przetwarzania danych jest zainstalowane i regularnie aktualizowane oprogramowanie zabezpieczające.

7) **bezpieczne przesyłanie plików** – pliki zawierające dane osobowe są przesyłane w sposób zapewniający poufność (szyfrowanie pliku, bezpieczne łącze lub hasło do pliku przekazywane odrębnym kanałem niż zaszyfrowany plik).

8) **ostrożność przy korzystaniu z poczty elektronicznej** – użytkownicy sprawdzają adresatów przed wysłaniem wiadomości z danymi osobowymi; nie klikają w podejrzane linki i nie otwierają nieznanych załączników.

9) **chmura i narzędzia zewnętrzne** – korzystanie z usług chmurowych i zewnętrznych narzędzi odbywa się za zgodą i wiedzą Fundacji oraz po weryfikacji dostawcy pod kątem ochrony danych.

10) **nośniki zewnętrzne** – korzystanie z nośników zewnętrznych (pendrive'ów, dysków przenośnych) do przechowywania danych Fundacji wymaga odpowiedniego zabezpieczenia tych danych; zgubienie lub kradzież nośnika z danymi jest zgłaszana jako incydent.

11) **urządzenia prywatne** – korzystanie z prywatnych urządzeń do przetwarzania danych Fundacji jest możliwe wyłącznie po uzgodnieniu z zarządem i przy zastosowaniu środków ochrony równoważnych z wymaganiami niniejszej Polityki.

12) **kopie zapasowe** – Fundacja wykonuje kopie zapasowe danych w zakresie adekwatnym do ich znaczenia i ryzyka utraty. Kopie są przechowywane w bezpieczny sposób, w oddzielnym miejscu lub systemie od danych produkcyjnych.

X. OBOWIĄZEK INFORMACYJNY I REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Fundacja wykonuje obowiązek informacyjny wobec osób, których dane dotyczą:

   a. przy zbieraniu danych bezpośrednio od tych osób – w momencie pozyskiwania danych,

   b. jeżeli dane pozyskano z innego źródła niż osoba, której dotyczą – bez zbędnej zwłoki, nie później niż w terminie miesiąca od ich pozyskania, albo przy pierwszej komunikacji z tą osobą, albo przy pierwszym ujawnieniu danych innemu odbiorcy – w zależności od tego, co nastąpi wcześniej.

2. Klauzule informacyjne są przejrzyste, zrozumiałe i dostosowane do grupy osób, których dotyczą. Zawierają w szczególności: dane administratora i kontakt w sprawach danych, cel i podstawę przetwarzania, kategorie odbiorców, okres przechowywania danych, prawa osób oraz informację o prawie do wniesienia skargi do Prezesa UODO.

3. Klauzule informacyjne mogą być przygotowywane jako odrębne dokumenty, właściwe dla poszczególnych procesów przetwarzania. Szczegółowe wzory klauzul informacyjnych mogą stanowić odrębny moduł dokumentacji Fundacji.

4. Przyjmowanie i realizacja żądań osób, których dane dotyczą

5. Osoby, których dane dotyczą, mogą kierować do Fundacji żądania dotyczące swoich praw wynikających z RODO (dostęp do danych, sprostowanie, usunięcie, ograniczenie przetwarzania, przeniesienie danych, sprzeciw wobec przetwarzania):

    a. drogą e-mailową na adres wskazany w rozdziale III ust. 2,

    b. pisemnie na adres siedziby Fundacji,

    c. osobiście w siedzibie Fundacji.

6. Każde żądanie jest niezwłocznie rejestrowane w Rejestrze żądań osób, których dane dotyczą (Załącznik nr 7), i przekazywane do [IOD / koordynatora ochrony danych / zarządu – wybrać właściwy wariant].

7. Fundacja weryfikuje tożsamość osoby składającej żądanie wyłącznie w niezbędnym zakresie – nie żąda więcej danych, niż jest to konieczne do potwierdzenia tożsamości i rozpatrzenia żądania.

8. [IOD / koordynator / zarząd – wybrać właściwy wariant] analizuje zasadność i zakres żądania oraz podejmuje decyzję o sposobie jego realizacji.

9. Co do zasady Fundacja odpowiada na żądanie w terminie jednego miesiąca od jego otrzymania. W przypadku złożonych lub licznych żądań termin może zostać przedłużony o kolejne dwa miesiące; Fundacja informuje wówczas osobę o przedłużeniu w terminie miesiąca od otrzymania żądania, podając przyczynę opóźnienia.

10. Jeżeli Fundacja nie może zrealizować żądania, informuje o tym osobę i podaje uzasadnienie.

11. Realizacja żądania i sposób jego załatwienia są dokumentowane w Rejestrze żądań (Załącznik nr 7).

12. Fundacja informuje osobę składającą żądanie o przysługującym jej prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli osoba uzna, że przetwarzanie jej danych narusza przepisy o ochronie danych osobowych.

XI. DANE SZCZEGÓLNEJ KATEGORII I DANE DZIECI

Instrukcja do szablonu, usunąć przed przyjęciem dokumentu: Niniejszy rozdział ma charakter wariantowy i powinien być w Polityce zachowany niezależnie od tego, czy Fundacja aktualnie przetwarza dane szczególnej kategorii lub dane dzieci. Stanowi on zasadę ogólną i zabezpieczenie na przyszłość. Jeżeli Fundacja aktualnie nie przetwarza danych szczególnej kategorii ani danych dzieci, zachowaj rozdział w całości i odnotuj aktualną sytuację w ust. 1 poniżej. Jeżeli Fundacja prowadzi lub planuje prowadzić regularne działania z dziećmi lub przetwarzać dane o zdrowiu, niepełnosprawności, sytuacji socjalnej, przemocy lub podobne informacje – wdrożenie dodatkowego, odrębnego modułu dokumentacji jest silnie zalecane.

1. Fundacja aktualnie nie przetwarza danych szczególnej kategorii ani danych dzieci w ramach swojej standardowej działalności. [Dostosuj lub usuń to zdanie, jeżeli Fundacja przetwarza takie dane.]
2. Przetwarzanie danych szczególnej kategorii jest co do zasady zakazane. Fundacja może je przetwarzać wyłącznie wtedy, gdy zachodzi właściwa przesłanka prawna dopuszczająca przetwarzanie danych tej kategorii, i tylko w zakresie niezbędnym do realizacji konkretnego, uzasadnionego celu.
3. Przed rozpoczęciem przetwarzania danych szczególnej kategorii osoba odpowiedzialna za dane działanie ma obowiązek ustalić właściwą podstawę prawną i skonsultować ją z [IOD / koordynatorem ochrony danych / zarządem – wybrać właściwy wariant] oraz odnotować ją w Karcie oceny (Załącznik nr 8) i RCP.
4. Dostęp do danych szczególnej kategorii jest ograniczony wyłącznie do osób, którym jest on bezwzględnie niezbędny. Zakres i cel przetwarzania tych danych są minimalizowane.
5. Działania obejmujące dane szczególnej kategorii wymagają szczególnej oceny ryzyka; co do zasady podlegają pogłębionej analizie ryzyka, a w przypadkach wymaganych przepisami RODO – DPIA przeprowadzonej przed ich uruchomieniem.
6. Fundacja zachowuje szczególną ostrożność przy przetwarzaniu danych dzieci. Dane dzieci są zbierane i przetwarzane wyłącznie w zakresie niezbędnym do realizacji konkretnego działania, z zastosowaniem właściwych podstaw prawnych. W przypadku gdy dla przetwarzania danych dziecka poniżej 16 roku życia wymagana jest zgoda, ocenia się, czy zgodę powinien wyrazić rodzic lub opiekun prawny, i postępuje stosownie do tej oceny.

7. Fundacje prowadzące regularne działania z dziećmi lub przetwarzające dane o zdrowiu, niepełnosprawności, sytuacji socjalnej, przemocy lub podobne informacje powinny wdrożyć dodatkowe, odrębne moduły dokumentacji dostosowane do specyfiki tych działań. Niniejszy rozdział nie zastępuje takich modułów.

XII. PODMIOTY ZEWNĘTRZNE: POWIERZENIE, UDOSTĘPNIENIE I WSPÓŁADMINISTROWANIE

1. Przed przekazaniem danych osobowych podmiotowi zewnętrznemu Fundacja ustala rolę tego podmiotu:

    a. **podmiot przetwarzający (procesor)** – przetwarza dane wyłącznie na polecenie Fundacji, w celach i zakresie określonych przez Fundację (np. biuro rachunkowe obsługujące kadry i księgowość, dostawca hostingu, platforma do wysyłki newslettera, narzędzie do wideokonferencji z dostępem do danych Fundacji). Z podmiotem przetwarzającym wymagana jest pisemna umowa powierzenia przetwarzania danych, zawarta przed przekazaniem danych.

    b. **inny administrator** – przetwarza dane we własnym imieniu i na własne cele, niezależnie od Fundacji (np. organy publiczne, sądy, instytucje finansujące działające jako odrębni administratorzy). Dane są wówczas udostępniane, a nie powierzane; wymagana jest właściwa podstawa prawna udostępnienia.

    c. **współadministrator** – wspólnie z Fundacją ustala cele i sposoby przetwarzania danych (np. partnerzy projektu wspólnie organizujący działania, w ramach których gromadzone są dane uczestników). Wymaga zawarcia stosownego porozumienia między współadministratorami.

2. Fundacja weryfikuje każdy podmiot przetwarzający przed powierzeniem mu danych, oceniając w szczególności:

    a. zakres danych, które będzie przetwarzał,

    b. cel i czas przetwarzania,

    c. stosowane środki bezpieczeństwa,

    d. ewentualnych podprzetwarzających i ich lokalizację,

    e. miejsce przetwarzania danych i ewentualny transfer poza EOG.

3. Fundacja zawiera pisemną umowę powierzenia przetwarzania danych z każdym podmiotem przetwarzającym przed przekazaniem mu danych. Umowa powierzenia określa m.in. przedmiot, czas trwania i cel przetwarzania, rodzaj danych, kategorie osób, obowiązki i prawa Fundacji jako administratora.

4. Fundacja prowadzi Wykaz podmiotów przetwarzających stanowiący Załącznik nr 9 do niniejszej Polityki. Wykaz jest na bieżąco aktualizowany.
5. Fundacja przeprowadza okresową weryfikację, czy podmioty przetwarzające nadal spełniają wymagania dotyczące bezpieczeństwa i zgodności z umową powierzenia – nie rzadziej niż raz w roku oraz przy każdej istotnej zmianie zakresu lub charakteru współpracy.

XIII. PRZEKAZYWANIE DANYCH POZA EUROPEJSKI OBSZAR GOSPODARCZY

1. Transfer danych poza EOG może wystąpić, gdy Fundacja korzysta z dostawców, narzędzi lub platform przetwarzających dane w państwach spoza EOG. Dotyczy to w szczególności usług chmurowych, hostingu i poczty elektronicznej, platform do wideospotkań, formularzy online, narzędzi do newslettera, analityki internetowej, mediów społecznościowych i serwisów płatnościowych.
2. Przed rozpoczęciem korzystania z narzędzia lub usługi mogącej wiązać się z transferem danych poza EOG, osoba odpowiedzialna identyfikuje tę okoliczność w Karcie oceny (Załącznik nr 8) i konsultuje ją z [IOD / koordynatorem / zarządem – wybrać właściwy wariant].
3. Transfer danych poza EOG jest dopuszczalny wyłącznie wtedy, gdy istnieje właściwa podstawa prawna, w szczególności:
    a. decyzja Komisji Europejskiej stwierdzająca odpowiedni poziom ochrony w danym państwie trzecim, lub
    b. odpowiednie zabezpieczenia w rozumieniu RODO, takie jak standardowe klauzule umowne zatwierdzone przez Komisję Europejską, lub
    c. inne zabezpieczenia lub wyjątki przewidziane w RODO (stosowane incydentalnie i po spełnieniu warunków określonych w RODO).
4. Fundacja dokumentuje ocenę podstawy prawnej transferu danych poza EOG, w szczególności w Karcie oceny nowego działania lub w RCP.
5. W umowach z dostawcami, których usługi wiążą się z transferem poza EOG, Fundacja dąży do zawarcia postanowień zapewniających wymagany poziom ochrony danych.
6. *[Usunąć lub zachować jako punkt informacyjny zgodnie z aktualną sytuacją Fundacji:* Fundacja aktualnie nie korzysta z usług wiążących się z transferem danych poza EOG. W przypadku uruchomienia takich narzędzi lub usług zastosowanie znajdą postanowienia niniejszego rozdziału.*]*

XIV. REAGOWANIE NA INCYDENTY I NARUSZENIA OCHRONY DANYCH

1. Każda osoba działająca w Fundacji, która odkryje lub podejrzewa zdarzenie mogące zagrażać bezpieczeństwu danych osobowych, ma obowiązek niezwłocznie zgłosić ten fakt [IOD / koordynatorowi ochrony danych / zarządowi – wybrać właściwy wariant] za pomocą Formularza zgłoszenia incydentu (Załącznik nr 5) lub w inny dostępny sposób (osobiście, telefonicznie, e-mailowo na adres: [do uzupełnienia]).

2. Osoba zgłaszająca nie musi samodzielnie oceniać, czy zdarzenie stanowi naruszenie ochrony danych w rozumieniu RODO.

3. Przykładowe zdarzenia wymagające niezwłocznego zgłoszenia:

    a. omyłkowe wysłanie wiadomości e-mail z danymi osobowymi do niewłaściwego adresata,

    b. ujawnienie linku do dokumentu z danymi osobowymi osobom nieuprawnionym,

    c. utrata lub kradzież urządzenia (laptopa, telefonu, dysku, pendrive'a) zawierającego dane osobowe,

    d. kradzież lub zgubienie dokumentów papierowych z danymi osobowymi,

    e. podejrzenie phishingu lub włamania do konta e-mail,

    f. przejęcie dostępu do konta lub systemu przez osobę nieuprawnioną,

    g. nieuprawniony dostęp do danych ze strony osoby wewnątrz organizacji,

    h. przypadkowe trwałe usunięcie danych,

    i. wyciek danych przez dostawcę lub podmiot przetwarzający,

    j. infekcja złośliwym oprogramowaniem systemu lub urządzenia zawierającego dane osobowe.

4. Osoba, która wykryła lub podejrzewa incydent:

    a. niezwłocznie ogranicza jego skutki, o ile jest to możliwe bez niszczenia dowodów (np. odłącza urządzenie od sieci, nie nadpisuje plików),

    b. nie usuwa śladów zdarzenia i nie ingeruje w systemy bez zgody [IOD / koordynatora / zarządu],

    c. niezwłocznie przekazuje informację o zdarzeniu i wypełnia Formularz zgłoszenia incydentu (Załącznik nr 5),

d. pozostaje dostępna do udzielenia wyjaśnień.

5. Po otrzymaniu zgłoszenia [IOD / koordynator / zarząd] niezwłocznie:

   a. ocenia charakter zdarzenia i ustala jego okoliczności,

   b. podejmuje dostępne działania ograniczające skutki zdarzenia,

   c. dokumentuje zdarzenie w Rejestrze naruszeń ochrony danych osobowych (Załącznik nr 6),

   d. dokonuje oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą.

6. Jeżeli naruszenie ochrony danych może powodować ryzyko naruszenia praw i wolności osób fizycznych, Fundacja zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych. Zgłoszenia dokonuje się bez zbędnej zwłoki – a jeżeli to możliwe, nie później niż w ciągu 72 godzin od chwili, w której Fundacja uzyska wystarczającą pewność, że do naruszenia doszło. Jeżeli zgłoszenie w tym terminie nie jest możliwe, dołącza się do niego wyjaśnienie przyczyn opóźnienia.

7. Zgłoszenia nie dokonuje się, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób.

8. Zgłoszenia dokonuje się za pomocą formularza dostępnego na stronie internetowej UODO (www.uodo.gov.pl).

9. Jeżeli naruszenie może powodować **wysokie** ryzyko naruszenia praw i wolności osób, Fundacja zawiadamia te osoby bez zbędnej zwłoki, chyba że:

   a. Fundacja wdrożyła odpowiednie środki techniczne i organizacyjne, które sprawiają, że dane są niemożliwe do odczytania przez osoby nieuprawnione (np. skuteczne szyfrowanie), lub

   b. Fundacja zastosowała środki eliminujące prawdopodobieństwo wysokiego ryzyka, lub

   c. zawiadomienie wymagałoby niewspółmiernie dużego wysiłku – wówczas wydaje się publiczny komunikat lub stosuje podobny środek.

10. Decyzję o zawiadomieniu lub braku zawiadomienia podejmuje zarząd, dokumentując uzasadnienie w Rejestrze naruszeń.
11. Po zakończeniu obsługi zdarzenia Fundacja analizuje jego przyczyny i wdraża działania naprawcze i zapobiegawcze. Wnioski uwzględnia się przy przeglądzie Polityki i środków bezpieczeństwa.

XV. RETENCJA, ARCHIWIZACJA I USUWANIE DANYCH

1. Fundacja przechowuje dane osobowe wyłącznie przez okres niezbędny do realizacji celu przetwarzania lub wykonania obowiązku prawnego, albo do czasu upływu okresu przedawnienia roszczeń mogących wiązać się z danym przetwarzaniem – w zależności od tego, który z tych terminów jest dłuższy.

2. Okresy przechowywania danych są określane dla każdego procesu przetwarzania w RCP (Załącznik nr 1) oraz w Karcie oceny nowego działania (Załącznik nr 8). Przy ustalaniu okresu retencji uwzględnia się:

    a. wymogi wynikające z przepisów prawa (m.in. przepisy podatkowe, archiwalne, prawa pracy),

    b. cel, dla którego dane zostały zebrane,

    c. ewentualne roszczenia lub postępowania, do których dane mogą być potrzebne.

3. Po upływie okresu retencji dane są:

    a. trwale i bezpiecznie niszczone w przypadku dokumentów papierowych (niszczarka lub udokumentowane przekazanie do profesjonalnego zniszczenia),

    b. trwale usuwane lub skutecznie anonimizowane w przypadku danych elektronicznych. Anonimizacja jest skuteczna wyłącznie wtedy, gdy po jej przeprowadzeniu nie jest możliwa ponowna identyfikacja osoby.

4. Po zakończeniu współpracy z osobą (pracownikiem, wolontariuszem, współpracownikiem, ekspertem) Fundacja niezwłocznie:

    a. odbiera dostępy tej osoby do systemów i danych,

    b. usuwa lub archiwizuje dane tej osoby stosownie do okresu retencji,

    c. zwraca lub niszczy dokumenty i nośniki zawierające dane osobowe przekazane tej osobie w związku z działalnością na rzecz Fundacji.

5. Fundacja uwzględnia w umowach z podmiotami przetwarzającymi postanowienia dotyczące obowiązku zwrotu lub trwałego i bezpiecznego usunięcia danych osobowych przez podmiot przetwarzający po zakończeniu współpracy lub na żądanie Fundacji.

XVI. SZKOLENIA, KONTROLA I PRZEGLĄD POLITYKI

1. Każda osoba dopuszczona do przetwarzania danych osobowych zapoznaje się z niniejszą Polityką przed uzyskaniem dostępu do danych i podpisuje Oświadczenie o zachowaniu poufności (Załącznik nr 3).

2. Przed dopuszczeniem do danych każda osoba odbywa szkolenie wstępne lub instruktaż dostosowany do swojej roli – w zakresie zasad przetwarzania danych, stosowanych środków bezpieczeństwa, obowiązku zgłaszania incydentów i realizacji praw osób. Szkolenie może mieć formę rozmowy, materiałów pisemnych, e-learningu lub inną formę dostosowaną do potrzeb i skali Fundacji.

3. Fundacja organizuje cykliczne przypomnienia i szkolenia w zakresie ochrony danych. Częstotliwość i forma jest dostosowana do specyfiki i skali działalności Fundacji. Szkolenie lub przypomnienie jest organizowane niezwłocznie po istotnym incydencie lub po istotnej zmianie przepisów mających wpływ na przetwarzanie danych w Fundacji.
4. Fundacja przeprowadza przegląd Polityki, rejestrów, upoważnień, dostępów i środków bezpieczeństwa nie rzadziej niż raz w roku.

5. Przegląd jest przeprowadzany niezwłocznie w przypadku:

    a. uruchomienia nowego projektu lub narzędzia,

    b. wdrożenia nowego dostawcy lub usługi,

    c. istotnej zmiany składu zespołu,

    d. wystąpienia incydentu lub naruszenia ochrony danych,

    e. istotnej zmiany zakresu przetwarzanych danych,

    f. zmiany przepisów prawa wpływającej na sposób przetwarzania danych.

6. Wynik przeglądu jest dokumentowany w prostej formie (notatka, wpis w rejestrze lub protokół) wskazującej datę przeglądu, osobę przeprowadzającą, zakres przeglądu oraz ewentualne wnioski lub działania do podjęcia.
7. Zmiany Polityki wymagają zatwierdzenia przez zarząd Fundacji. Osoby działające w Fundacji są informowane o istotnych zmianach.

XVII. POSTANOWIENIA KOŃCOWE

1. Polityka wchodzi w życie z dniem [do uzupełnienia].

2. Polityka jest udostępniana wszystkim osobom wymienionym w rozdziale I ust. 3, w formie [elektronicznej / papierowej – wybrać właściwy wariant], w miejscu

dostępnym dla osób uprawnionych [do uzupełnienia, np.: wspólny dysk, segregator w siedzibie, intranet].

3. W Fundacji stosuje się zawsze aktualną wersję Polityki. Wcześniejsze wersje są archiwizowane z zachowaniem dat ich obowiązywania.
4. Integralną częścią niniejszej Polityki są następujące załączniki:

Nr	Nazwa załącznika
Załącznik nr 1	Rejestr czynności przetwarzania danych osobowych
Załącznik nr 2	Upoważnienie do przetwarzania danych osobowych (wzór)
Załącznik nr 3	Oświadczenie o zachowaniu poufności (wzór)
Załącznik nr 4	Ewidencja osób upoważnionych do przetwarzania danych
Załącznik nr 5	Formularz zgłoszenia incydentu (wzór)
Załącznik nr 6	Rejestr naruszeń ochrony danych osobowych
Załącznik nr 7	Rejestr żądań osób, których dane dotyczą
Załącznik nr 8	Karta oceny nowego działania lub procesu przetwarzania danych osobowych
Załącznik nr 9	Wykaz podmiotów przetwarzających

5. Fundacja może stosować dodatkowe dokumenty dostosowane do specyfiki swojej działalności, w szczególności szczegółowe klauzule informacyjne dla poszczególnych grup osób, politykę prywatności i politykę cookies strony internetowej, wzory umów powierzenia przetwarzania danych, moduły dotyczące danych szczególnej kategorii lub danych dzieci oraz Politykę Bezpieczeństwa Informacji.

XVIII. ZAŁĄCZNIKI

ZAŁĄCZNIK NR 1 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

prowadzony zgodnie z art. 30 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)

[nazwa Fundacji]

1. Dane administratora danych osobowych

Nazwa administratora	
Dane kontaktowe administratora	
Dane kontaktowe przedstawiciela administratora	
Dane kontaktowe Inspektora Ochrony Danych	

2. Ogólne środki organizacyjne i techniczne ochrony danych osobowych

Poniższe środki mają charakter ogólny i stosowane są łącznie do wszystkich czynności przetwarzania wskazanych w rozdziale 3, niezależnie od dodatkowych, specyficznych środków wskazanych odrębnie przy każdym procesie.

2.1. Środki organizacyjne [należy dostosować do organizacji]

- wdrożona Polityka Ochrony Danych Osobowych wraz z załącznikami i procedurami wewnętrznymi, okresowo przeglądana i aktualizowana.
- imienne upoważnienia do przetwarzania danych osobowych (art. 29 RODO) nadawane każdej osobie przed dopuszczeniem do pracy z danymi, wraz z prowadzoną Ewidencją osób upoważnionych do przetwarzania.
- pisemne oświadczenia o zachowaniu poufności składane przez pracowników i współpracowników, obowiązujące bezterminowo, także po ustaniu zatrudnienia lub współpracy.
- obowiązkowe szkolenia wstępne oraz okresowe szkolenia przypominające z zakresu ochrony danych osobowych i cyberbezpieczeństwa dla wszystkich osób dopuszczonych do przetwarzania danych, potwierdzane pisemnie.
- szkolenia BHP (wstępne i okresowe) obejmujące zasady bezpiecznego korzystania ze stanowisk pracy, sprzętu służbowego i dokumentacji.
- procedura zgłaszania i obsługi naruszeń ochrony danych osobowych, w tym zasady zgłaszania naruszeń Prezesowi UODO w terminie 72 godzin oraz informowania osób, których dane dotyczą, gdy jest to wymagane; prowadzony rejestr naruszeń/incydentów.
- zasada ograniczonego dostępu do danych (need-to-know) oraz okresowy przegląd i weryfikacja nadanych uprawnień.

- umowy powierzenia przetwarzania danych osobowych (art. 28 RODO) zawierane z każdym podmiotem przetwarzającym dane w imieniu administratora.
- zasada czystego biurka i czystego ekranu; dokumentacja papierowa przechowywana w szafach i pomieszczeniach zamykanych na klucz, z dostępem ograniczonym do osób upoważnionych.
- nadzór Inspektora Ochrony Danych nad zgodnością procesów przetwarzania z RODO, w tym opiniowanie nowych procesów i udział w ocenie ryzyka.
- procedura nadawania, zmiany i cofania upoważnień/dostępów do systemów wraz z niezwłoczną dezaktywacją kont osób, które zakończyły zatrudnienie lub współpracę.

2.2. Środki techniczne [należy dostosować do organizacji]

- kontrola dostępu do systemów informatycznych za pomocą indywidualnych identyfikatorów i haseł, zgodnie z wewnętrzną polityką haseł.
- automatyczne blokowanie stacji roboczych po określonym czasie bezczynności.
- oprogramowanie antywirusowe oraz zapory sieciowe (firewall) na stanowiskach i serwerach.
- bieżące aktualizacje systemów operacyjnych i oprogramowania wykorzystywanego do przetwarzania danych.
- regularne wykonywanie i testowanie kopii zapasowych danych.
- szyfrowanie danych przekazywanych drogą elektroniczną, w szczególności zawierających dane szczególnych kategorii; hasła do zaszyfrowanych plików przekazywane odrębnym kanałem komunikacji.
- rejestrowanie (logowanie) zdarzeń i dostępu do systemów zawierających dane osobowe.
- fizyczne zabezpieczenie pomieszczeń, w których przetwarzane są dane osobowe (kontrola dostępu, zamki, w wybranych lokalizacjach monitoring wizyjny terenu i wejść).
- niszczenie dokumentacji papierowej i nośników danych w sposób uniemożliwiający odtworzenie danych (niszczarki, protokołowane niszczenie dokumentacji).
- ograniczenie zdalnego dostępu do systemów do niezbędnego minimum, z wykorzystaniem zabezpieczonych narzędzi dostępu zdalnego oraz nadzorem nad sesjami zdalnymi.

3. Wykaz czynności przetwarzania danych osobowych

Każdy z poniższych procesów podlega ogólnym środkom ochrony wskazanym w rozdziale 2. Kolumna „Dodatkowe środki ochrony danych" wskazuje wyłącznie środki specyficzne dla danego procesu, wykraczające poza standard ogólny.

1. NAZWA CZYNNOŚCI

Cel przetwarzania danych	
Kategorie osób, których dane dotyczą	
Kategorie danych osobowych	
Podstawa prawna	
Odbiorcy danych	
Przekazanie poza EOG	
Okres przechowywania danych	
Dodatkowe środki ochrony danych (właściwe dla procesu)	

2. NAZWA CZYNNOŚCI

Cel przetwarzania danych	
Kategorie osób, których dane dotyczą	
Kategorie danych osobowych	

Podstawa prawna	
Odbiorcy danych	
Przekazanie poza EOG	
Okres przechowywania danych	
Dodatkowe środki ochrony danych (właściwe dla procesu)	

ZAŁĄCZNIK NR 2 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upoważnienia: [do uzupełnienia]

Dane osoby upoważnianej	
Imię i nazwisko	[do uzupełnienia]
Funkcja / rola w Fundacji	[do uzupełnienia]
Forma zaangażowania	[pracownik / współpracownik / wolontariusz / stażysta / ekspert / członek zarządu – wybrać właściwy wariant]

Działając w imieniu Fundacji [nazwa Fundacji] z siedzibą w [adres siedziby], jako administrator danych osobowych,

z dniem [do uzupełnienia] upoważniam Panią / Pana [imię i nazwisko]

do przetwarzania danych osobowych w zakresie i na zasadach określonych poniżej.

Zakres danych osobowych objętych upoważnieniem:

[do uzupełnienia – np.: dane uczestników projektów Fundacji, dane wolontariuszy, dane kontrahentów – wpisać konkretny zakres adekwatny do roli danej osoby]

Rodzaj dozwolonych czynności przetwarzania:

[do uzupełnienia – np.: zbieranie, przechowywanie, przeglądanie, modyfikowanie, usuwanie danych w zakresie wskazanym powyżej, w ramach realizacji obowiązków wynikających z pełnionej funkcji]

Cel przetwarzania:

[do uzupełnienia – np.: realizacja projektów Fundacji, obsługa wolontariatu, przygotowanie sprawozdań]

Warunki upoważnienia:

1. Upoważnienie obejmuje przetwarzanie danych wyłącznie w celach i zakresie wskazanych powyżej, zgodnie z Polityką Ochrony Danych Osobowych Fundacji.

2. Upoważnienie zostaje nadane na czas trwania współpracy.

3. Upoważnienie może zostać zmienione lub cofnięte w każdym czasie, w szczególności w przypadku zmiany zakresu zadań lub zakończenia współpracy z Fundacją.

4. Upoważnienie wygasa z chwilą zakończenia współpracy z Fundacją.

5. Cofnięcie lub zmiana upoważnienia następuje w formie pisemnej lub elektronicznej i jest odnotowywane w Ewidencji osób upoważnionych (Załącznik nr 4).

[Miejscowość], dnia [do uzupełnienia]

Podpis osoby reprezentującej Fundację **Podpis i data osoby upoważnionej (potwierdzenie odbioru)**

…… ……

imię i nazwisko, funkcja *imię i nazwisko, data*

COFNIĘCIE / ZMIANA UPOWAŻNIENIA *(wypełnić w momencie zmiany lub cofnięcia)*

Data cofnięcia / zmiany upoważnienia	
Przyczyna cofnięcia / zmiany	
Zakres zmiany (jeżeli dotyczy)	
Podpis osoby reprezentującej Fundację	

Dofinansowane przez Unię Europejską

sieć splot wartości

Wzór opracowany przez Fundację LegisLab. Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

ZAŁĄCZNIK NR 3 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

[Miejscowość], dnia ……

Imię i nazwisko: …… **Funkcja / rola w Fundacji:** ……
Forma zaangażowania: [pracownik / współpracownik / wolontariusz / stażysta / ekspert / członek zarządu – wybrać właściwy wariant]

Oświadczam, że przed dopuszczeniem do przetwarzania danych osobowych:

1. zapoznałam/zapoznałem się z Polityką Ochrony Danych Osobowych Fundacji [nazwa Fundacji] wraz z wszystkimi jej załącznikami,

2. odbyłam/odbyłem szkolenie wstępne lub instruktaż w zakresie zasad ochrony danych obowiązujących w Fundacji,

3. rozumiem zakres nadanego mi upoważnienia do przetwarzania danych osobowych.

Zobowiązuję się do:

1. przetwarzania danych osobowych wyłącznie w celach i zakresie wynikającym z nadanego upoważnienia i polecenia Fundacji,

2. zachowania w poufności wszelkich danych osobowych, do których uzyskałam/uzyskałem dostęp w związku z działalnością na rzecz Fundacji, zarówno w trakcie, jak i po zakończeniu współpracy,

3. zachowania w poufności sposobów zabezpieczenia danych osobowych stosowanych przez Fundację,

4. przestrzegania zasad określonych w Polityce Ochrony Danych Osobowych Fundacji i innych obowiązujących procedurach,

5. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem,

6. nieprzekazywania danych osobowych osobom nieuprawnionym bez wyraźnej zgody Fundacji,

7. niekopiowania i nieprzechowywania danych osobowych Fundacji na prywatnych nośnikach lub urządzeniach bez wiedzy i zgody Fundacji,

Dofinansowane przez Unię Europejską
sieć splot wartości

Wzór opracowany przez Fundację LegisLab. Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

8. niezwłocznego zgłaszania każdego zdarzenia, które może stanowić incydent lub naruszenie ochrony danych osobowych, zgodnie z procedurą opisaną w rozdziale XIII Polityki,

9. ochrony indywidualnych danych dostępowych (loginów, haseł) – nieudostępniania ich innym osobom i niestosowania do celów innych niż wykonywanie zadań na rzecz Fundacji,

10. po zakończeniu współpracy z Fundacją – zwrotu lub zniszczenia wszelkich nośników i dokumentów zawierających dane osobowe Fundacji oraz usunięcia danych z prywatnych urządzeń, jeżeli były na nich przechowywane.

Zobowiązanie do zachowania poufności obowiązuje bezterminowo, również po zakończeniu współpracy z Fundacją.

……

czytelny podpis osoby składającej oświadczenie

ZAŁĄCZNIK NR 4 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Fundacja: [nazwa Fundacji] **Prowadzona przez:** [IOD / koordynator ochrony danych – do uzupełnienia] **Data ostatniej aktualizacji:** [do uzupełnienia]

Lp.	Imię i nazwisko	Funkcja / rola	Nr i data upoważnienia	Data nadania dostępu	Data zmiany upoważnienia	Data cofnięcia dostępu	Uwagi
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							

Instrukcja do szablonu, usunąć przed przyjęciem dokumentu: Ewidencja może być prowadzona w formie elektronicznej (np. arkusz kalkulacyjny). Wiersze dodaje się w miarę potrzeby. Ewidencja jest aktualizowana niezwłocznie po każdej zmianie.

Dofinansowane przez Unię Europejską

sieć splot wartości

Wzór opracowany przez Fundację LegisLab. Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

ZAŁĄCZNIK NR 5 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

FORMULARZ ZGŁOSZENIA INCYDENTU

Fundacja [nazwa Fundacji]

Formularz przeznaczony dla osoby zgłaszającej. Nie musisz samodzielnie oceniać, czy zdarzenie stanowi naruszenie ochrony danych. Zgłoś zdarzenie i opisz je tak dokładnie, jak potrafisz.

1. Data i godzina zdarzenia lub jego wykrycia:

Data: ……. Godzina: …….

2. Osoba zgłaszająca:

Imię i nazwisko: …….. Funkcja / rola w Fundacji: …….. Kontakt (e-mail / telefon): ……..

3. Opis zdarzenia *(Co się stało? Opisz zdarzenie własnymi słowami – jak najpełniej i konkretnie.)*

……
……
……
……

4. Miejsce zdarzenia / dotyczy systemu lub urządzenia:

[Zaznacz i/lub opisz: komputer / telefon / pendrive / dysk zewnętrzny / chmura / poczta e-mail / dokumenty papierowe / inne: ……..]

Opis: ……

5. Dane osobowe, których dotyczy zdarzenie:

Kategorie osób: [np. uczestnicy projektu / wolontariusze / pracownicy / inne: ……..] Rodzaj danych: [np. imiona i nazwiska, adresy e-mail, numery telefonów, dane finansowe, inne: ……] Przybliżona liczba osób, których dane mogą być objęte zdarzeniem: ……..

6. Możliwi nieuprawnieni odbiorcy danych *(jeżeli wiadomo lub można przypuszczać):*

……

7. Działania już podjęte *(co zrobiłaś/zrobiłeś w związku ze zdarzeniem):*

……
……

8. Czy zdarzenie nadal trwa? Tak / Nie / Nie wiem

Dofinansowane przez Unię Europejską

sieć splot wartości

Wzór opracowany przez Fundację LegisLab. Grant realizowany ze środków Unii Europejskiej w ramach projektu SPLOT WARTOŚCI 2.0

9. Pilność zgłoszenia *(subiektywna ocena):*

☐ Zdarzenie zostało już zatrzymane, brak bezpośredniego zagrożenia ☐ Zdarzenie może nadal trwać lub eskalować – pilne ☐ Nie jestem w stanie ocenić

10. Załączniki i dodatkowe informacje *(zrzuty ekranu, e-maile, inne dokumenty – opisz, jeżeli dotyczy):*

……

Data i podpis zgłaszającego: …….. ……..

Adresat zgłoszenia: [IOD / koordynator ochrony danych / zarząd Fundacji – wybrać właściwy wariant] – adres e-mail: [do uzupełnienia]

Instrukcja do szablonu, usunąć przed przyjęciem dokumentu: Formularz powinien być dostępny dla wszystkich osób działających w Fundacji – np. jako plik w udostępnionym folderze, wydruk w siedzibie lub szablon w systemie pocztowym. Uzupełnij adres e-mail lub inne dane kontaktowe adresata zgłoszenia przed wdrożeniem formularza.

ZAŁĄCZNIK NR 6 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Fundacja: [nazwa Fundacji] **Prowadzony przez:** [IOD / koordynator ochrony danych – do uzupełnienia]

Podstawa: rozdział XIII Polityki Ochrony Danych Osobowych

Instrukcja do szablonu, usunąć przed przyjęciem dokumentu: Rejestr może być prowadzony w formie elektronicznej (arkusz kalkulacyjny, dokument tekstowy) lub papierowej. Każde zdarzenie, które zostało ocenione jako możliwe naruszenie lub naruszenie ochrony danych, powinno zostać wpisane do rejestru, niezależnie od tego, czy zostało zgłoszone do Prezesa UODO. Rejestr jest dokumentem wewnętrznym.

Nr	Data wykrycia	Opis zdarzenia	Kategorie danych i osób	Szacowana skala (liczba osób)	Działania ograniczające podjęte natychmiast	Wynik oceny ryzyka	Zgłoszenie do Prezesa UODO (tak/nie/nie dotyczy; data)	Zawiadomienie osób (tak/nie/nie dotyczy; data)	Działania naprawcze i zapobiegawcze	Data zamknięcia sprawy	Osoba odpowiedzialna za obsługę
1.											
2.											
3.											
4.											
5.											

ZAŁĄCZNIK NR 7 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

REJESTR ŻĄDAŃ OSÓB, KTÓRYCH DANE DOTYCZĄ

Fundacja: [nazwa Fundacji] **Prowadzony przez:** [IOD / koordynator ochrony danych – do uzupełnienia]

Podstawa: rozdział IX Polityki Ochrony Danych Osobowych

Instrukcja do szablonu, usunąć przed przyjęciem dokumentu: Rejestr może być prowadzony w formie elektronicznej lub papierowej. Każde żądanie osoby dotyczące jej praw powinno zostać wpisane do rejestru niezwłocznie po jego otrzymaniu. Termin odpowiedzi co do zasady wynosi jeden miesiąc od daty wpływu żądania.

Nr	Data wpływu żądania	Imię i nazwisko osoby składającej żądanie (lub opis: „osoba anonimowa“)	Rodzaj żądania	Kanał wpływu (e-mail / pismo / osobiście)	Sposób weryfikacji tożsamości	Wyznaczony termin odpowiedzi	Decyzja (realizacja / odmowa; uzasadnienie)	Data odpowiedzi	Osoba prowadząca sprawę
1.									
2.									
3.									
4.									
5.									

ZAŁĄCZNIK NR 8 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

KARTA OCENY NOWEGO DZIAŁANIA LUB PROCESU PRZETWARZANIA DANYCH OSOBOWYCH

Fundacja [nazwa Fundacji]

Narzędzie wstępnej preselekcji – nie jest Oceną Skutków dla Ochrony Danych (DPIA). Wypełnij kartę przed uruchomieniem nowego działania lub istotną zmianą działania już prowadzonego.

3. SEKCJA A – INFORMACJE PODSTAWOWE

Pole	Odpowiedź
Nazwa działania / projektu / procesu	[do uzupełnienia]
Osoba odpowiedzialna za działanie	[do uzupełnienia]
Planowana data uruchomienia	[do uzupełnienia]
Status karty	☐ Nowe działanie ☐ Istotna zmiana działania już prowadzonego ☐ Przegląd działania
Data wypełnienia karty	[do uzupełnienia]

4. SEKCJA B – OPIS DZIAŁANIA

1. Na czym polega planowane działanie i jaki jest jego cel?

……
……

2. Czy działanie wiąże się z przetwarzaniem danych osobowych?

☐ Tak – przejdź do sekcji C ☐ Nie – uzasadnij poniżej i zakończ wypełnianie karty

Uzasadnienie (jeżeli nie): ……

5. SEKCJA C – DANE OSOBOWE I PODSTAWY PRZETWARZANIA

3. Jakie kategorie osób będą dotyczyły dane?

☐ Uczestnicy projektu / beneficjenci

☐ Wolontariusze

☐ Eksperci / konsultanci

☐ Pracownicy / współpracownicy

☐ Darczyńcy

☐ Kontrahenci / partnerzy

☐ Inne: ……

4. Jakie kategorie danych będą przetwarzane?

☐ Imię i nazwisko, dane kontaktowe (e-mail, telefon, adres)

☐ Dane finansowe (nr rachunku, wynagrodzenie, darowizna)

☐ Wizerunek (zdjęcia, nagrania wideo)

☐ Dane o kwalifikacjach / wykształceniu / doświadczeniu

☐ Dane szczególnej kategorii (patrz sekcja D pkt 9)

☐ Dane dzieci / osób małoletnich

☐ Inne: ……

5. Jaki jest cel przetwarzania tych danych?

……

6. Jaka jest podstawa prawna przetwarzania?

☐ Zgoda osoby (art. 6 ust. 1 lit. a RODO) – czy zgoda jest dobrowolna, konkretna i odwoływalna?

☐ Wykonanie umowy lub działania na żądanie przed zawarciem umowy (art. 6 ust. 1 lit. b RODO)

☐ Obowiązek prawny ciążący na Fundacji (art. 6 ust. 1 lit. c RODO)

☐ Prawnie uzasadniony interes Fundacji (art. 6 ust. 1 lit. f RODO) – czy interes ten nie jest nadrzędny wobec praw i wolności osób?

☐ Inna: ……

7. Czy zakres zbieranych danych jest ograniczony do minimum niezbędnego do realizacji celu?

☐ Tak – uzasadnienie: ……

☐ Nie – jakie dane można wyeliminować? ……

6. SEKCJA D – SZCZEGÓŁY PRZETWARZANIA

8. Skąd pozyskuje się dane?

☐ Bezpośrednio od osób, których dane dotyczą ☐ Od innych podmiotów / źródeł (jakich?): ……

9. Czy przetwarzane będą dane szczególnej kategorii lub dane dzieci?

☐ Nie

☐ Tak – jakie: ……
→ UWAGA: wymagana szczególna ocena ryzyka i konsultacja z [IOD / koordynatorem / zarządem]. Rozważ konieczność DPIA.

10. Gdzie będą przechowywane dane?

☐ Wewnętrzne systemy / dyski Fundacji

☐ Chmura – dostawca: ……..

☐ Dokumenty papierowe

☐ Narzędzie zewnętrzne – dostawca: …….. ☐ Inne: ……..

11. Kto będzie miał dostęp do danych?

……

12. Czy dane będą przekazywane podmiotom zewnętrznym?

☐ Nie

☐ Tak – jakiemu podmiotowi / jakim podmiotom: …… Rola podmiotu zewnętrznego:

☐ Podmiot przetwarzający

☐ Inny administrator

☐ Współadministrator

Czy zawarto lub zostanie zawarta umowa powierzenia?

☐ Tak ☐ Nie ☐ W trakcie

13. Czy dane będą przekazywane poza EOG?

☐ Nie ☐ Tak / prawdopodobnie tak – dostawca / kraj: ……..

Podstawa prawna transferu:

☐ Decyzja KE ☐ Standardowe klauzule umowne ☐ Inna ☐ Do ustalenia

14. Jaki jest planowany okres przechowywania danych?

……

Uzasadnienie: ……

7. SEKCJA E – RYZYKA I ŚRODKI OCHRONY

15. Jakie podstawowe środki ochrony będą zastosowane?

☐ Ograniczenie dostępu do danych (wyłącznie osoby upoważnione)

☐ Szyfrowanie danych lub zabezpieczenie hasłem

☐ MFA dla narzędzi / kont z danymi

☐ Umowa powierzenia z dostawcą

☐ Bezpieczne kanały komunikacji

☐ Inne: ……

16. LISTA CZERWONYCH FLAG – oceń, czy działanie obejmuje którykolwiek z poniższych elementów:

Element	Tak	Nie	Uwagi
dane szczególnej kategorii	☐	☐	
dane dzieci lub osób małoletnich	☐	☐	
dane osób w kryzysie lub wymagających szczególnego wsparcia	☐	☐	
przetwarzanie na szeroką skalę (wiele osób lub duże ilości danych)	☐	☐	
systematyczne monitorowanie osób	☐	☐	
profilowanie lub zautomatyzowane podejmowanie decyzji	☐	☐	
decyzje mogące znacząco wpływać na osoby	☐	☐	
łączenie danych z różnych źródeł	☐	☐	
nowa technologia lub narzędzie nieznane dotąd Fundacji	☐	☐	
transfer danych poza EOG	☐	☐	

Liczba zaznaczonych „Tak“: ……. **Jeżeli zaznaczono choć jedną flagę – wymagana konsultacja i pogłębiona ocena ryzyka. Przy wielu flagach rozważ DPIA.**

8. SEKCJA F – FORMALNOŚCI

17. Czy spełniono obowiązek informacyjny wobec osób, których dane będą dotyczą?

☐ Tak – klauzula informacyjna: ……..

☐ Nie – do przygotowania przed uruchomieniem ☐ Nie dotyczy (uzasadnienie): ……

18. Czy działanie zostanie wpisane do Rejestru Czynności Przetwarzania?

☐ Tak – data wpisu lub planowana data wpisu: …… ☐ Nie – uzasadnienie: ……..

9. SEKCJA G – DECYZJA I DALSZE KROKI

19. Decyzja końcowa:

☐ **Można rozpocząć** po wdrożeniu środków wskazanych poniżej

☐ **Wymaga zatwierdzenia** przez [IOD / koordynatora / zarząd] przed uruchomieniem

☐ **Wymaga pogłębionej analizy ryzyka** przed uruchomieniem

☐ **Należy rozważyć DPIA** – skonsultuj z [IOD / koordynatorem / zarządem]

☐ **Nie rozpoczynać działania w obecnej formie** – konieczna istotna modyfikacja

20. Lista działań wymaganych przed uruchomieniem:

1. ……
2. ……
3. ……

21. Osoba zatwierdzająca kartę:

Imię i nazwisko: ……

Funkcja: ……..

Podpis i data: ……

22. Termin ponownego przeglądu karty / działania:

[do uzupełnienia]

ZAŁĄCZNIK NR 9 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

WYKAZ PODMIOTÓW PRZETWARZAJĄCYCH

Fundacja: [nazwa Fundacji] **Prowadzony przez:** [IOD / koordynator ochrony danych – do uzupełnienia]

Podstawa: rozdział XI Polityki Ochrony Danych Osobowych **Data ostatniej aktualizacji:** [do uzupełnienia]

Instrukcja do szablonu, usunąć przed przyjęciem dokumentu: Do wykazu wpisuje się wyłącznie podmioty przetwarzające (procesory) – podmioty zewnętrzne przetwarzające dane w imieniu Fundacji na podstawie umowy powierzenia. Nie wpisuje się tutaj innych administratorów (np. organów publicznych) ani współadministratorów. Wykaz może być prowadzony w formie elektronicznej. Aktualizuj go niezwłocznie po każdej zmianie.

Lp.	Nazwa dostawcy	Świadczona usługa	Zakres powierzonych danych (kategorie)	Kategorie osób	Data zawarcia umowy powierzenia / inna podstawa	Podwykonawcy dostawcy (jeżeli znani)	Miejsce przetwarzania / Transfer poza EOG (tak/nie; kraj/podstawa)	Osoba odpowiedzialna po stronie Fundacji	Data ostatniego przeglądu
1.									
2.									
3.									
4.									
7.									

Dofinansowane przez Unię Europejską

sieć splot wartości

Lp.	Nazwa dostawcy	Świadczona usługa	Zakres powierzonych danych (kategorie)	Kategorie osób	Data zawarcia umowy powierzenia / inna podstawa	Podwykonawcy dostawcy (jeżeli znani)	Miejsce przetwarzania / Transfer poza EOG (tak/nie; kraj/podstawa)	Osoba odpowiedzialna po stronie Fundacji	Data ostatniego przeglądu
8.									