

# **POLITYKA OCHRONY DANYCH OSOBOWYCH**

**FUNDACJI WYCHOWANKÓW HALINY I JANA MACHULSKICH z siedzibą w Warszawie**

Warszawa, dnia 02 stycznia 2022 roku

## I. ZAGADNIENIA WSTĘPNE

1. Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w **Fundacji Wychowanków Haliny i Jana Machulskich** (dalej jako „**Fundacja**”).
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).
3. Polityka zawiera:
  - 1) opis zasad ochrony danych obowiązujących w Fundacji;
  - 2) odwołania do załączników uszczegółwiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);
4. Skróty i definicje:
  - 1) **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
  - 2) **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).
  - 3) **Dane** oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
  - 4) **Dane wrażliwe** oznaczają dane specjalne i dane karne.
  - 5) **Dane specjalne** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
  - 6) **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
  - 7) **Dane dzieci** oznaczają dane osób poniżej 16. roku życia.
  - 8) **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
  - 9) **Podmiot przetwarzający** oznacza organizację lub osobę, której Fundacja powierzyła przetwarzanie danych osobowych (np. usługodawca IT, wykładowca).
  - 10) **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
  - 11) **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
  - 12) **IOD lub Inspektor** oznacza Inspektora Ochrony Danych Osobowych

- 13) **RCPD lub Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
- 14) **Fundacja** oznacza Fundację Wychowanków Haliny i Jana Machulskich z siedzibą w Warszawie.

## II. PODMIOTY ODPOWIEDZIALNE ZA WDROŻENIE I PRZESTRZEGANIE POSTANOWIEŃ POLITYKI

1. Odpowiedzialny za **wdrożenie** i **rozwijanie** niniejszej Polityki jest:
  - 1) Zarząd Fundacji.
2. Odpowiedzialny za **nadzór** i **monitorowanie** przestrzegania niniejszej Polityki jest:
  - 1) Inspektor Ochrony Danych.
3. Podmiotami odpowiedzialnymi za **stosowanie się do** niniejszej Polityki są:
  - 1) Fundacja;
  - 2) wszyscy członkowie personelu organizacyjnego Fundacji i jej komórek;
  - 3) kontrahenci i współpracownicy Fundacji w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Fundację.

## III. OCHRONA DANYCH OSOBOWYCH W FUNDACJI – ZASADY OGÓLNE

1. **Filary ochrony danych osobowych w Fundacji:**
  - 1) **Legalność podstaw przetwarzania danych osobowych** – Fundacja dba o ochronę prywatności i przetwarza dane osobowe zgodnie z powszechnie obowiązującym prawem. W szczególności Fundacja nie dokonuje czynności przetwarzania danych osobowych, gdy dane te zostały uzyskane bez właściwej podstawy prawnej;
  - 2) **Bezpieczeństwo** – Fundacja dąży do zapewnienia odpowiedniego poziomu bezpieczeństwa danych osobowych, podejmując stale działania w tym zakresie;
  - 3) **Ochrona wolności i praw osoby której dane dotyczą** – Fundacja umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
  - 4) **Rozliczalność** – Fundacja dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność przetwarzania danych z powszechnie obowiązującym prawem.

### 2. Zasady ochrony danych

Fundacja przetwarza dane osobowe z poszanowaniem następujących zasad:

- 1) w oparciu o podstawę prawną i zgodnie z prawem (**legalizm**);
- 2) rzetelnie i uczciwie (**rzetelność**);
- 3) w sposób przejrzysty dla osoby, której dane dotyczą (**transparentność**);
- 4) w konkretnych celach i nie „na zapas” (**minimalizacja**);
- 5) nie więcej niż potrzeba (**adekwatność**);
- 6) z dbałością o prawidłowość danych (**prawidłowość**);
- 7) nie dłużej niż potrzeba (**czasowość**);
- 8) zapewniając odpowiednie bezpieczeństwo danych (**bezpieczeństwo**).

## IV. PRZYJĘTY PRZEZ FUNDACJĘ SYSTEM OCHRONY DANYCH

1. System ochrony danych osobowych w Fundacji składa się z następujących elementów:

- 1) **Inwentaryzacja danych.** Fundacja dokonuje identyfikacji zasobów danych osobowych w Fundacji, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:
  - a) przypadków przetwarzania danych specjalnych i danych „kryminalnych” (**dane wrażliwe**);
  - b) przypadków przetwarzania danych osób, których Fundacja nie identyfikuje (**dane niezidentyfikowane**);
  - c) przypadków przetwarzania danych dzieci;
  - d) profilowania;
  - e) współadministrowania danymi.
- 2) **Rejestr.** Fundacja opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Fundacji (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Fundacji.
- 3) **Podstawy prawne.** Fundacja zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
  - a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
  - b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Fundacja przetwarza dane na podstawie prawnie uzasadnionego interesu Fundacji.
- 4) **Obsługa praw jednostki.** Fundacja spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
  - a) **Obowiązki informacyjne.** Fundacja przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
  - b) **Możliwość wykonania żądań.** Fundacja weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających. Fundacja zapewnia odpowiednie procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO.
  - c) **Zawiadomianie o naruszeniach.** Fundacja stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
- 5) **Minimalizacja.** Fundacja posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
  - a) zasady zarządzania **adekwatnością** danych;
  - b) zasady reglamentacji i zarządzania **dostępem** do danych;
  - c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;
- 6) **Bezpieczeństwo.** Fundacja zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
  - a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
  - b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
  - c) dostosowuje środki ochrony danych do ustalonego ryzyka;
  - d) posiada system zarządzania bezpieczeństwem informacji;

- e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.
- 7) **Przetwarzający.** Fundacja posiada zasady doboru przetwarzających dane na rzecz Fundacji, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
- 8) **Eksport danych.** Fundacja posiada zasady weryfikacji, czy Fundacja nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.
- 9) **Privacy by design.** Fundacja zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Fundacji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
- 10) **Przetwarzanie transgraniczne.** Fundacja posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

## 2. Inwentaryzacja danych osobowych

### 1) Dane wrażliwe

Fundacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe (dane specjalne i dane karne) oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Fundacja postępuje zgodnie z przyjętymi zasadami w tym zakresie.

### 2) Dane niezidentyfikowane

Fundacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

### 3) Profilowanie

Fundacja identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, Fundacja postępuje zgodnie z przyjętymi zasadami w tym zakresie.

### 4) Współadministrowanie

Fundacja identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

## 3. Podstawy przetwarzania

- 1) Fundacja dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
- 2) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Fundacji) Fundacja dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

- 3) Fundacja wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
- 4) Kierownik komórki organizacyjnej Fundacji ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Fundacji, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes Fundacji.

#### 4. Sposób obsługi praw jednostki i obowiązków informacyjnych

- 1) Fundacja dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
- 2) Fundacja ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Fundacji informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Fundacji, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Fundacją w tym celu, ewentualnym cenniku żądań „dodatkových” itp.
- 3) Fundacja dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
- 4) Fundacja wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
- 5) W celu realizacji praw jednostki Fundacja zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Fundację, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
- 6) Fundacja dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

#### 9. Obowiązki informacyjne

- 1) Fundacja określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
- 2) Fundacja informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
- 3) Fundacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
- 4) Fundacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
- 5) Fundacja określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
- 6) Fundacja informuje osobę o planowanej zmianie celu przetwarzania danych.
- 7) Fundacja informuje osobę przed uchycieniem ograniczenia przetwarzania.
- 8) Fundacja informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
- 9) Fundacja informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- 10) Fundacja bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

#### 10. Procedury postępowania przy otrzymaniu żądań od osób których dane dotyczą

- 1) **Prawa osób trzecich.** Realizując prawa osób, których dane dotyczą, Fundacja wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej,

tajemnicę handlową, dobra osobiste itp.), Fundacja może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

- 2) **Nieprzetwarzanie.** Fundacja informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
- 3) **Odmowa.** Fundacja informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
- 4) **Dostęp do danych.** Na żądanie osoby dotyczące dostępu do jej danych, Fundacja informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Fundacja nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
- 5) **Kopie danych.** Na żądanie Fundacja wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Fundacja wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.
- 6) **Sprostowanie danych.** Fundacja dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Fundacja ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Fundacja informuje osobę o odbiorcach danych, na żądanie tej osoby.
- 7) **Uzupełnienie danych.** Fundacja uzupełnia i aktualizuje dane na żądanie osoby. Fundacja ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Fundacja nie musi przetwarzać danych, które są Fundacji zbędne). Fundacja może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Fundację procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
- 8) **Usunięcie danych.** Na żądanie osoby, Fundacja usuwa dane, gdy:
  - a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
  - b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
  - c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
  - d) dane były przetwarzane niezgodnie z prawem,
  - e) konieczność usunięcia wynika z obowiązku prawnego,
  - f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Fundacja określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Fundację, Fundacja podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych Fundacja informuje osobę o odbiorcach danych, na żądanie tej osoby.

- 9) **Ograniczenie przetwarzania.** Fundacja dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
- a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
  - b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
  - c) Fundacja nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
  - d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Fundacji zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Fundacja przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Fundacja informuje osobę przed uchynieniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Fundacja informuje osobę o odbiorcach danych, na żądanie tej osoby.

- 10) **Przenoszenie danych.** Na żądanie osoby Fundacja 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 Fundacji, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Fundacji.
- 11) **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Fundację w oparciu o uzasadniony interes Fundacji lub o powierzone Fundacji zadanie w interesie publicznym, Fundacja **uwzględni** sprzeciw, o ile nie zachodzą po stronie Fundacji ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
- 12) **Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych.** Jeżeli Fundacja prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Fundacja uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
- 13) **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Fundacja na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Fundacja uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
- 14) **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Fundacja przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na **osobę**, Fundacja zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Fundacji, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Fundacją; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

## 11. Minimalizacja danych

Fundacja dba o minimalizację przetwarzania danych pod kątem:

- 1) **Adekwatności danych do celów (ilości danych i zakresu przetwarzania)**
- Fundacja zweryfikowało zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.



- Fundacja dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
- Fundacja przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

## 2) Minimalizacja dostępu do danych

- Fundacja stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
- Fundacja stosuje kontrolę dostępu fizycznego.
- Fundacja dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
- Fundacja dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
- Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Fundacji.

## 3) Minimalizacja czasu przetwarzania danych

- Fundacja wdraża mechanizmy kontroli cyklu życia danych osobowych w Fundacji, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
- Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Fundacji, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Fundację. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

## 12. Bezpieczeństwo danych

Fundacja zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Fundację.

### 1) Analizy ryzyka i adekwatności środków bezpieczeństwa

Fundacja przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

- (1) Fundacja zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnątrz lub ze wsparciem podmiotów wyspecjalizowanych.
- (2) Fundacja kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
- (3) Fundacja przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Fundacja analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
- (4) Fundacja ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Fundacja ustala przydatność i stosuje takie środki i podejście jak:
  - (i) pseudonimizacja,

- (ii) szyfrowanie danych osobowych,
- (iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- (iv) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

#### **2) Oceny skutków dla ochrony danych**

Fundacja dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

#### **3) Środki bezpieczeństwa**

Fundacja stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Fundacji i są bliżej opisane w procedurach przyjętych przez Fundację dla tych obszarów.

#### **4) Zgłaszanie naruszeń**

Fundacja stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

### **13. Podmioty przetwarzające dane osobowe**

Fundacja posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Fundacji opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Fundacji.

Fundacja przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 1 do Polityki – „Wzór umowy powierzenia przetwarzania danych”**.

Fundacja rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

### **14. Eksport danych osobowych**

Fundacja rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).

### **15. Projektowanie prywatności**

Fundacja zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

W tym celu zasady prowadzenia projektów i inwestycji przez Fundację odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

## **V. POSTANOWIENIA KOŃCOWE**

- 1) Polityka Ochrony Danych Osobowych wchodzi w życie z dniem podjęcia uchwały o przyjęciu niniejszej Polityki przez Zarząd Fundacji.
- 2) W żadnym wypadku celem niniejszej Polityki nie jest ograniczenie, wyłączenie lub obejście obowiązujących bezwzględnie obowiązujących przepisów. W sprawach nieuregulowanych niniejszą Polityką mają zastosowanie powszechnie obowiązujące przepisy, w tym przede wszystkim

RODO. W razie sprzeczności ewentualnych wątpliwości co do zgodności z przepisami powszechnie obowiązującymi lub niezupełności regulacji niniejszej Polityki zastosowanie będą mieć przepisy powszechnie obowiązujące.