POLITYKA OCHRONY DANYCH OSOBOWYCH

1. Postanowienia ogólne

Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**" (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w FUNDACJA PHARMAHELP z siedzibą w Toruniu (dalej jako **Fundacja**).

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).

2. Zawartość

Polityka zawiera:

a) opis zasad ochrony danych obowiązujących w Fundacji
b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

3. Zasady odpowiedzialności

Generalnie odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Fundacji, a w ramach Zarządu **za wdrożenie i utrzymanie niniejszej Polityki odpowiedzialny jest:**

- Członek Zarządu, któremu powierzono nadzór nad obszarem ochrony danych osobowych
- osoba wyznaczona przez Zarząd do zapewnienia zgodności z ochroną danych osobowych

Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:

- Inspektor Ochrony Danych, który został powołany w Fundacji
- komórka audytu wewnętrznego, jeżeli funkcjonuje w Fundacji

Za stosowanie niniejszej Polityki odpowiedzialna jest:

a) fundacja

Fundacja dokłada wszelkich starań aby zapewnić zgodność postępowania kontrahentów Fundacji z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Fundację.

4. Skróty i definicje:

a) **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
b) **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).
c) **Dane** oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
d) **Dane wrażliwe** oznaczają dane specjalne i dane karne.
e) **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.

f) **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
g) **Dane dzieci** oznaczają dane osób poniżej 16. roku życia.
h) **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
i) **Podmiot przetwarzający** oznacza organizację lub osobę, której Fundacja powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna Księgowość).
j) **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do automatycznej 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.
k) **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
l) **IOD lub Inspektor** oznacza Inspektora Ochrony Danych Osobowych.
m) **Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
n) **Fundacja** oznacza Fundację PHARMAHELP z siedzibą w Toruniu.

5. Ochrona danych osobowych w Fundacji - zasady ogólne

5.1 Filary ochrony danych osobowych w Fundacji:

a) **Legalność** – Fundacja dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
b) **Bezpieczeństwo** – Fundacja zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
c) **Prawa Jednostki** – Fundacja umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
d) **Rozliczalność** – Fundacja dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5.2 Zasady ochrony danych

Fundacja przetwarza dane osobowe z poszanowaniem następujących zasad:

a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
b) rzetelnie i uczciwie (rzetelność);
c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
d) w konkretnych celach i nie „na zapas" (minimalizacja);
e) nie więcej niż potrzeba (adekwatność);
f) z dbałością o prawidłowość danych (prawidłowość);
g) nie dłużej niż potrzeba (czasowość);
h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

5.3 System ochrony danych

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

A. 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**/UFO)
c) przypadków przetwarzania danych dzieci
d) profilowania
e) współadministrowania danymi

B. Rejestr.

Fundacja opracowuje, prowadzi i utrzymuje **Rejestr Czynności Danych Osobowych** w Fundacji (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Fundacji.

C. Podstawy prawne.

Fundacja zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

- utrzymuje system zarządzania **zgodami na przetwarzanie danych** i komunikację na odległość
- inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Fundacja przetwarza dane na podstawie prawnie uzasadnionego interesu Fundacji.

D. 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:

- **Obowiązki informacyjne.** Fundacja przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
- **Możliwość wykonania żądań.** Fundacja weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
- **Obsługa żądań.** Fundacja zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
- **Zawiadamianie o naruszeniach.** Fundacja stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych

E. 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;

F. 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.

G. Przetwarzający.
Fundacja posiada zasady doboru przetwarzających dane na rzecz Fundacji, wymogów co do warunków przetwarzania **(umowa powierzenia**), zasad weryfikacji wykonywania umów powierzenia.

H. 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.

a.*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.

b. Przetwarzanie transgraniczne.
Fundacja w razie zaistnienia potrzeby weryfikuje czy zachodzą przypadki przetwarzania transgranicznego oraz ustala wiodący organ nadzorczy i główną jednostkę organizacyjną w rozumieniu RODO.

6. Inwentaryzacja

A. 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.

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

C. 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.

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

7. Rejestr czynności przetwarzania danych

7.1 Fundacja stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

7.2 Fundacja prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

7.3 Rejestr jest jednym z podstawowych narzędzi umożliwiających Fundacji rozliczanie większości obowiązków ochrony danych.

7.4 W Rejestrze, dla każdej czynności przetwarzania danych, którą Fundacja uznała za odrębną dla potrzeb Rejestru, Fundacja odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Fundacji, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG;
(ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.

Wzór Rejestru stanowi **Załącznik nr 1 do Polityki - „Wzór Rejestru Czynności Przetwarzania Danych".** Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Fundacja rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

8. Podstawy przetwarzania

8.1 Fundacja dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

8.2 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.

8.3 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.).

9. Sposób obsługi praw jednostki i obowiązków informacyjnych

9.1 Fundacja dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

9.2 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 z Fundacją w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

9.3 Fundacja dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

9.4 Fundacja wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

9.5 W celu realizacji praw jednostki Fundacji zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Fundację, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

9.6 Fundacja dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

10. Obowiązki informacyjne

Fundacja:

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

11. Żądania osób

11.1 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.

11.2 Nieprzetwarzanie.

Fundacja informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

11.3 Odmowa.

Fundacja informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

11.4 Dostęp do danych.
Na żądanie osoby dotyczące dostępu do jej danych, Fundacji 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.

11.5 Kopie danych.
Na żądanie Fundacja wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

11.6 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.

11.7 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.

11.8 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).

11.9 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.

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

11.11 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 Fundacja, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Fundacji.

11.12 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.

11.13 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.

11. 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.

12. Minimalizacja

12.1 Fundacja dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu **przetwarzania**), (ii) dostępu do danych, (iii) czasu przechowywania danych.

12.2 Minimalizacja zakresu

Fundacja zweryfikowała 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*).

12.3 Minimalizacja dostępu

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.

12.4 Minimalizacja czasu

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.

13. Bezpieczeństwo

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

13.2 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 − wewnętrznie 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:
    - pseudonimizacja
    - szyfrowanie danych osobowych
    - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
    - 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.

13.3 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. Fundacja stosuje metodykę oceny skutków przyjętą w Fundacji.

13.4 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.

13.5 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.

14. Postanowienia Końcowe

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy 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). oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000) i przepisy wykonawcze do tej Ustawy.

Członkowie Zarządu Fundacji PHARMAHELP z siedzibą w Toruniu zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Fundacji PHARMAHELP z siedzibą w Toruniu, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

……..…..

pieczęć firmowa

Rejestr czynności przetwarzania

Nazwa czynności przetwarzania	Jednostka organizacyjna	Cel przetwarzania	Kategorie osób	Kategorie danych	Planowany termin usunięcia kategorii danych	Nazwa współadministratora i dane kontaktowe	Nazwa podmiotu przetwarzającego i dane kontaktowe	Kategorie odbiorców	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Transfer do kraju trzeciego lub organizacji międzynarodowej
1.										
2.										
3.										
4.										
5.										
6.										
7.										
8.										
9.										
10.										
11.										