**Fundacja "PROMETEUSZ DLA SENIORÓW" IMIENIA KSIĄŻĄT MARII I WŁODZIMIERZA CZETWERTYŃSKICH**

Stan: wrzesień 2022r.

**POLITYKA OCHRONY DANYCH OSOBOWYCH**

**I Cel**

Niniejszy dokument ma służyć zapewnieniu bezpieczeństwa danych osobowych przetwarzanych przez Fundację „PROMETEUSZ DLA SENIORÓW” IMIENIA KSIĄŻĄT MARII I WŁODZIMIERZA CZETWERTYŃSKICH (KRS: 0000377508) (dalej: „Fundacja”) i innych danych mogących mieć wartość dla Fundacji oraz jej podopiecznych, darczyńców i kontrahentów. Wszyscy pracownicy oraz osoby współpracujące z Fundacją zobowiązani są do zapoznania się z niniejszym dokumentem oraz przestrzegania jego postanowień.

Dane osobowe mogą być przetwarzane w sposób tradycyjny dokumentowy oraz przy użyciu systemów informatycznych. Niniejszy dokument dotyczy głównie przetwarzania danych osobowych w sposób tradycyjny, tj. w dokumentach papierowych, kartotekach, skorowidzach wykazach i innych zbiorach; zawiera również postanowienia ogólne dotyczące polityki ochrony danych w Fundacji.

**II Definicje**

(alfabetycznie]

**„Administrator danych”** oznacza Fundację „PROMETEUSZ DLA SENIORÓW” IMIENIA KSIĄŻĄT MARII I WŁODZIMIERZA CZETWERTYŃSKICH (KRS: 0000377508), dalej jako „Fundacja”;

**„Dane osobowe”** oznaczają dane osobowe zgodnie z RODO, tzn. informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

**„Dane wrażliwe”** oznaczają dane osobowe szczególnej kategorii tzn. pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przekonania światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, zdrowie, seksualność i orientacja seksualna.

**„Naruszenie”** albo **„naruszenie ochrony danych osobowych”** oznacza 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;

**„Przetwarzanie danych osobowych”** oznacza przetwarzanie danych osobowych zgodnie z RODO, tzn. operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie,

ograniczanie, usuwanie lub niszczenie;

**„RODO”** oznacza 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) (Tekst mający znaczenie dla EOG);

**„Podopieczny”** oznacza osobę fizyczną, która udostępnia dane osobowe i wrażliwe Administratorowi i wyraża zgodę na przetwarzanie tych danych.

**III Administrator i podmiot przetwarzający**

1. Fundacja jest administratorem danych osobowych otrzymanych od osób fizycznych, których dane dotyczą tzn. odpowiada za zgodność przetwarzania tych danych osobowych z obowiązującymi przepisami. Dotyczy to danych osobowych otrzymanych od Podopiecznych (np. dane osobowe kontaktowe i dane osobowe dotyczące stanu zdrowia) jak również Profesjonalistów (np. dane osobowe kontaktowe).

**IV Zasady ogólne**

1. Fundacja dokłada wszelkich starań i zobowiązuje swoich pracowników oraz współpracowników, aby dane osobowe były:
2. przetwarzane zgodnie z zasadami zgodności z prawem, rzetelności i przejrzystości;
3. zbierane wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami, z zastrzeżeniem sytuacji dozwolonych przez prawo („ograniczenie celu”);
4. prawidłowe i miarę potrzeby uaktualniane („prawidłowość”);
5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

**V Dostęp do pomieszczeń, w których przetrzymywane są dane osobowe**

1. Administrator danych zapewnia, by dostęp do pomieszczeń, w których przechowywane są dokumenty zawierające dane osobowe miały wyłącznie osoby upoważnione i zobowiązane do zachowanie w tajemnicy danych, do których mają dostęp.
2. Dokumenty, które zawierają dane osobowe albo inne informacje chronione powinny być zamykane na klucz, dostęp do nich mają jedynie osoby o odpowiednim upoważnieniu.
3. Pracownicy i współpracownicy zobowiązani są do chronienia dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych, w tym usuwania z biurek dokumentów zawierających dane osobowe po zakończonej pracy lub w czasie jakiejkolwiek nieobecności przy swoim stanowisku pracy (clear desk policy).
4. Zakazuje się wynoszenia jakichkolwiek dokumentów zawierających dane osobowe z biura bez uprzedniej zgody Administratora danych stwierdzonej pismem (np. e-mail).

**VI Prawa osób, których dane dotyczą**

1. Administrator danych zapewnia i zobowiązuje swoich pracowników oraz współpracowników do respektowania praw osób, których dane dotyczą, w szczególności do:
2. przejrzystej komunikacji (art. 12 ust.1 RODO);
3. informacji (art. 13 i 14 RODO);
4. dostępu do danych (art. 15);
5. sprostowania danych (art.16);
6. usunięcia danych, czyli prawo do bycia zapomnianym (art.17 RODO);
7. ograniczenia przetwarzania (art. 18 RODO);
8. przenoszenia danych (art.20 RODO);
9. sprzeciwu (art.21 RODO);
10. niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu (art.22 RODO).
11. Przed zrealizowaniem prawa osoby, której dane dotyczą należy upewnić się, że osoba, która zwraca się do Administratora faktycznie jest tym, za kogo się podaje.
12. Administrator danych niezwłocznie realizuje uprawnione żądanie osoby, w stosunku do jej danych osobowych.

**VII Przetwarzanie danych w charakterze podmiotu przetwarzającego**

W przypadku przetwarzania przez Fundację danych osobowych i wrażliwych w imieniu innych podmiotów, tj. administratorów danych, obowiązują wszystkie standardy Administratora chyba, że z umowy o powierzeniu przetwarzania danych osobowych wynikają wyższe standardy- wówczas Administrator stosuje standardy z uwzględnieniem postanowień umowy powierzenia przetwarzania danych osobowych.

**VIII Lista podmiotów podprzetwarzających**

1. Biura rachunkowe, oraz świadczące obsługę kadrowo-płacową;
2. Osoby fizyczne i prawne udzielające wsparcia prawnego;
3. Podmioty będące darczyńcami Fundacji;
4. Dostawcy usług informatycznych.

Dane osobowe przekazywane przez Fundację podmiotom podprzetwarzającym, są ograniczone do danych niezbędnych i ściśle związanych z działalnością statutową Fundacji.

**IX Zasady zgłaszania incydentów i naruszeń**

1. Pracownicy oraz współpracownicy Fundacji zobowiązani są do zgłaszania osobom reprezentującym Fundację wszelkich Naruszeń oraz podejrzeń Naruszeń (incydentów) ochrony danych osobowych.

|  |
| --- |
| Zgodnie z art. 4 pkt 12 RODO oznacza:  Naruszenie danych osobowych oznacza 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  Zgodnie z wytycznymi grupy roboczej art. 29 można mówić o naruszenia *sensu stricto*, jeśli nastąpi przynajmniej jedno z poniższych:   * naruszenie poufności- niedozwolone lub przypadkowe ujawnienie lub dostęp do danych osobowych; * naruszenie dostępności- niedozwolona lub przypadkowa utrata dostępu do danych osobowych lub ich zniszczenie; * naruszenie integralności- niedozwolona lub przypadkowa zmiana danych osobowych |

1. W przypadku naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych Administrator danych w porozumieniu z dostawcą systemów informatycznych przeprowadza postępowanie wyjaśniające. W przypadku stwierdzenia naruszenia w rozumieniu RODO dostawca systemów informatycznych niezwłocznie przygotowuje pełny opis naruszenia systemów informatycznych i przekazuje opis Administratorowi danych.
2. W przypadku naruszenia danych osobowych przetwarzanych tradycyjnie Administrator danych sam przeprowadza postępowanie wyjaśniające.
3. Administrator danych odnotowuje incydenty. Administrator danych prowadzi Rejestr Naruszeń, w którym dokumentuje lub naruszenie i, jeśli to ma zastosowanie, przekazuje pełną informację o naruszeniu odpowiednim organom.

**X Postanowienia końcowe**

1. W sprawach nieuregulowanych niniejszym dokumentem należy stosować obowiązujące przepisy prawa, w szczególności RODO, a także instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń.
2. Pracownicy i współpracownicy Fundacji zobowiązują się do przestrzegania niniejszego dokumentu oraz w miarę możliwości stosowania wytycznych obowiązujących przy przetwarzaniu danych osobowych również do innych danych mogących mieć wartość dla Fundacji lub Podopiecznych Fundacji. W szczególności zobowiązują się zachować poufność powierzanych im informacji dotyczących danych wrażliwych, w szczególności dotyczących zdrowia Podopiecznych.
3. Naruszenie obowiązków wynikających z niniejszego dokumentu może być uznane za ciężkie naruszenie obowiązków pracowniczych.