

# **Polityka ochrony danych osobowych**

**Fundacji Edukacji i Rozwoju Centrum Wszechświata**

Czarnków, ..... 2018 r.



## Spis treści

1. Zakres i podstawa stosowania	3
2. Zawartość	3
3. Odpowiedzialność	3
4. Skróty i definicje	4
5. Ochrona danych osobowych – zasady ogólne	5
6. Inwentaryzacja	7
7. Rejestr czynności przetwarzania danych osobowych	8
8. Podstawy przetwarzania	9
9. Sposób obsługi praw jednostki i obowiązków informacyjnych	9
10. Obowiązki informacyjne	10
11. Żądania osób	11
12. Minimalizacja	14
13. Bezpieczeństwo	15
14. Przetwarzający	18
15. Eksport danych	19
16. Projektowanie prywatności	19
17. Załączniki	20

## **1. Zakres i podstawa stosowania**

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych Fundacji Edukacji i Rozwoju Centrum Wszechświata ” (dalej: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Fundacji Edukacji i Rozwoju Centrum Wszechświata (dalej: Fundacja).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (EU) 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 uszczegółwiających.

## **3. Odpowiedzialność**

3.1 Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Administrator, tj. Prezes Zarządu Fundacji Edukacji i Rozwoju Centrum Wszechświata.

3.2 Odpowiedzialnym za nadzór i monitorowanie przestrzegania Polityki jest Inspektor Ochrony Danych (dalej: IOD).

3.3 Odpowiedzialnymi za stosowanie niniejszej Polityki są wszyscy pracownicy Fundacji oraz zarząd Fundacji w zakresie powierzonych im obowiązków, uprawnień, odpowiedzialności, upoważnień i pełnomocnictw.

3.4 Fundacja zapewnia zgodność postępowania kontrahentów Fundacji z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Fundację. Zasady powierzenia procesu przetwarzania danych osobowych opisuje Rozdział 14 niniejszej Polityki.



#### 4. Skróty i definicje

**Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

**RODO** oznacza rozporządzenia Parlamentu Europejskiego i Rady (EU) 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).

**Dane** oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

**Dane szczególne** 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.

**Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

**Dane dzieci** oznaczają dane osób poniżej 16 roku życia.

**Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

**Administrator** oznacza osobę Prezesa Zarządu Fundacji Edukacji i Rozwoju Centrum Wszechświata, który samodzielnie lub wspólnie z innymi administratorami ustala cele i sposoby przetwarzania danych osobowych.

**Podmiot przetwarzający** oznacza organizację lub osobę, której Fundacja powierzyła przetwarzanie danych osobowych (np. zewnętrzna obsługa BHP, usługodawca IT).

**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.

**Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

**IOD lub Inspektor** oznacza Inspektora Danych Osobowych.

**RDCP lub Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

**Fundacja** oznacza Fundację Edukacji i Rozwoju Centrum Wszechświata.

## 5. Ochrona danych osobowych – zasady ogólne

### 5.1 Filary ochrony danych:

- (1) **Legalność** – Fundacja dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
- (2) **Bezpieczeństwo** – Fundacja zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
- (3) **Prawa jednostki** – Fundacja umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
- (4) **Rozliczalność** – Fundacja dokumentuje to, w jaki sposób spełnia obowiązek, aby w każdej chwili móc wykazać zgodność.

### 5.2 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).

### 5.3 System ochrony danych

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

- (1) **Inwentaryzacja danych.** Fundacja dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym:

- a) przypadków przetwarzania danych szczególnych i danych karnych;
  - 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 (Rejestr). Rejestr jest narzędziem rozliczania zgodności ochrony 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 Administratora lub osoby, której dane osobowe dotyczą.
- (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;
  - c) **obsługa żądań.** Fundacja zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i udokumentowane;
  - d) **zawiadamianie o naruszeniach.** Fundacja stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych oraz Prezesa Urzędu Ochrony Danych Osobowych.
- (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) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych w ramach zarządzania 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 Unię Europejską, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.
- (9) **Privacy by design.** Fundacja zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Fundacji uwzględniają konieczność oceny wpływu zmian na ochronę danych osobowych, analizę ryzyka, 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.

## 6. Inwentaryzacja

### 6.1 Dane szczególne i dane karne

Fundacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególne lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W chwili zidentyfikowania przypadku przetwarzania danych szczególnych lub danych karnych Fundacja postępuje zgodnie z przyjętymi przepisami prawa, zasadami w tym zakresie lub w szczególnych przypadkach w oparciu o zgodę osoby na przetwarzanie takich danych. Całość procesu przetwarzania opiera się o przesłanki określone w art. 9 ust. 2 i art. 10 RODO.

## **6.2 Dane niezidentyfikowane**

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

## **6.3 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. Profilowanie odbywa się wyłącznie po wyczerpaniu przynajmniej jednej z przesłanek art. 22 ust. 2 RODO.

## **6.4 Współadministrowanie**

Fundacja identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami. Administrator przy wsparciu IOD w porozumieniu z współadministratorem ustala podział obowiązków ze szczególnym uwzględnieniem realizacji praw przysługujących osobie, której dane dotyczą w tym obowiązku informacyjnego wg założeń art. 13 RODO oraz wskazuje się punkt kontaktowy dla osób, których dane dotyczą. Ustalenia powyższe każdorazowo mają postać zindywidualizowanej umowy w formie porozumienia pisemnego.

## **7. Rejestr czynności przetwarzania danych osobowych**

7.1 RCPD 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 RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane.

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 uzna za odrębną dla potrzeb Rejestru, odnotowuje się co najmniej:

- (1) nazwę czynności;
- (2) cel przetwarzania;

- (3) opis kategorii osób;
- (4) opis kategorii danych;
- (5) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Fundacji, jeśli podstawą jest uzasadniony interes,
- (6) sposób zbierania danych;
- (7) informację o przekazaniu poza EU/EOG;
- (8) ogólny opis technicznych i organizacyjnych środków ochrony danych.

7.5 Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”**. Rejestr ma formę pisemną, w tym formę elektroniczną. 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. Prowadzenie Rejestru powierza się Prezesowi Zarządu Fundacji, który w porozumieniu z IDO dokonuje wpisów aktualizacyjnych. Zmiany takie mogą być wymuszone w szczególności nowymi aktami prawa pociągającymi za sobą konieczność realizacji nowych zadań w tym związanych z przetwarzaniem danych.

## 8. Podstawy przetwarzania

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

8.2 Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, uzasadniony cel Fundacji), Fundacja dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody – wskazując jej zakres, gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując konkretny cel, np. marketing własny, dochodzenie roszczeń.

8.3 Fundacja wdraża metody zarządzania zgodami umożliwiając rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS, itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

8.4 Zgody stanowią część akt spraw i jako takie podlegają nadzorowi. **Załącznik nr 4 do Polityki – „Wzór zgody na przetwarzanie danych”** określa treść zgody na

przetwarzanie, co pozwala na uzyskanie zgody od osoby, której dane dotyczą z zachowaniem jej obowiązkowych wg RODO cech, tj. dobrowolności, konkretności, świadomego i jednoznacznego określenia woli osoby.

8.5 Każdy pracownik Fundacji przetwarzając dane osobowe ma obowiązek znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Fundacji, pracownik ma obowiązek znać konkretny realizowany przetwarzaniem interes Fundacji.

## **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 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 dotrzymanie prawnych terminów realizacji obowiązków względem osób.

9.4 Fundacja wprowadza adekwatne metody identyfikacji i uwierzytelnienia osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych. Podstawowym narzędziem identyfikacji i uwierzytelnienia jest wgląd do dokumentu tożsamości osoby, której dane dotyczą, a na rzecz której to osoby ma nastąpić realizacja jej praw i obowiązków informacyjnych.

9.5 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. Mechanizmy te w szczególności określa dokumentacja techniczna czy podręcznik użytkownika każdego z systemów elektronicznego przetwarzania danych.

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

## **10. Obowiązki informacyjne**

- 10.1 Fundacja określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
- 10.2 Fundacja informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
- 1.1 Fundacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby. Udostępnia się osobie treść klauzuli informacyjnej m.in. bezpośrednio w miejscu uzyskania danych od osoby (biuro Fundacji), drogą komunikacji na odległość (e-mail, telefon) i na stronie internetowej Fundacji. **Załącznik nr 6 do Polityki – „Wzór klauzuli informacyjnej”** określa zawartość merytoryczną dostępną dla osoby, do której bezpośrednio zbiera się dane osobowe.
- 1.2 Fundacja nie informuje osoby o przetwarzaniu jej danych, przy pozyskaniu danych o tej osobie niebezpośrednio od niej, jeśli pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą lub dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie, w tym ustawowym obowiązkiem zachowania tajemnicy.
- 1.3 Fundacja określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka informująca o objęciu obszaru monitoringiem wizyjnym).
- 1.4 Fundacja informuje osobę o planowanej zmianie celu przetwarzania danych.
- 1.5 Fundacja informuje osobę przed uchyleniem ograniczenia przetwarzania danych.
- 1.6 Fundacja informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- 1.7 Fundacja bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko praw lub wolności tej osoby.

## **2. Żądania osób**

- 2.1 **Prawa osób trzecich.** Realizując prawa osób, której 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, tajemnica handlową, dobra osobiste), Fundacja może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

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

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

**2.4 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.

**2.5 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 skalkulowania jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych. Cennik wprowadza się osobnym zarządzeniem Administratora i udostępnia na stronie internetowej Fundacji.

**2.6 Sprostowanie danych.** Fundacja dokonuje sprostowania danych na żądanie osoby. Fundacja ma prawo odmówić sprostowania, 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 osoby biorąc pod uwagę, że organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem, nie są uznawane za odbiorców.

**2.7 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 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.

**2.8 Usunięcie danych.** Na żądanie osoby Fundacja usuwa dane, gdy:

- (1) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
- (2) zgoda na ich przetwarzanie została cofnięta a nie ma innej podstawy prawnej przetwarzania,
- (3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
- (4) dane były przetwarzane niezgodnie z prawem,
- (5) konieczność usunięcia wynika z obowiązku prawnego,
- (6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. 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 poniższe wyjątki:

- a) jeżeli przetwarzanie danych jest konieczne do korzystania z prawa do wolności wypowiedzi i informacji;
- b) jeżeli przetwarzanie danych jest konieczne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa;
- c) jeżeli przetwarzanie danych jest konieczne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- d) jeżeli przetwarzanie danych jest istotne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- e) jeżeli przetwarzanie danych jest konieczne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
- f) jeżeli przetwarzanie danych jest konieczne do ustalenia, dochodzenia lub obrony roszczeń.

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

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

**2.9 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 stosowania,
- 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 uchyleniem ograniczenia przetwarzania.

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

**2.10 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.

**2.11 Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane są przetwarzane 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.

**2.12 Sprzeciw przy celach statystycznych.** Jeżeli Fundacja 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.

**2.13 Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Fundację na potrzeby marketingu



bezpośredniego (w tym ewentualnie profilowania), Fundacja uwzględni taki sprzeciw i zaprzestanie takiego przetwarzania.

**2.14 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:

- (1) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Fundacją,
- (2) jest wprost dozwolona przepisami prawa,
- (3) opiera się na wyraźnej zgodzie osoby odwołującej się.

### **3. Minimalizacja**

Fundacja dba o minimalizację przetwarzania danych pod kątem:

- (1) adekwatności danych do celów (ilość danych i zakresu przetwarzania),
- (2) dostępu do danych,
- (3) czasu przechowywania danych.

#### **3.1 Minimalizacja zakresu.**

Fundacja zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach 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*).

#### **3.2 Minimalizacja dostępu**

Fundacja stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresu upoważnień), fizyczne (strefy dostęp, zamykanie pomieszczeń) i logiczne ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których znajdują się dane osobowe.

Fundacja stosuje kontrolę dostępu fizycznego, m.in. poprzez ograniczenie dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe.

Fundacja dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających w oparciu o wydane upoważnienia do przetwarzania danych oraz ewidencję osób upoważnionych do przetwarzania danych.

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 **Załączniku nr 6 do Polityki – „Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji”**.

### **3.3 Minimalizacja czasu**

Fundacja wdraża mechanizmy kontroli cyklu życia danych osobowych w Fundacji, w tym weryfikacji dalszej przydatności danych pod względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów informatycznych Fundacji, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się w kopiach zapasowych systemów i informacji przetwarzanych przez Fundację. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystywania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogu usuwania danych.

## **4. Bezpieczeństwo**

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

### **4.1 Analiza ryzyka i adekwatność 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. Analiza ryzyka jest wykonywana przy udziale Administratora, IOD, oraz osoby dokonującej czynności przetwarzania danych. Analiza ryzyka dla czynności przetwarzania danych lub ich kategorii jest dokumentowana w **Załączniku nr 11 do Polityki – „Wzór protokołu analizy ryzyka”**. W zakresie oceny wagi zagrożenia ustala się skalę, gdzie 1 oznacza brak przetwarzania danych osobowych, 2 przetwarzanie danych zwykłych, 3 oznacza przetwarzanie danych szczególnych i/lub karnych. W zakresie prawdopodobieństwa wystąpienia zagrożenia ustala się skalę, gdzie 1 oznacza sporadyczne przetwarzanie (do 100 rekordów miesięcznie), 2 oznacza częste przetwarzanie (do 500 rekordów miesięcznie), 3 oznacza bardzo częste przetwarzanie (powyżej 500 rekordów miesięcznie). Mnożnik wagi ryzyka i prawdopodobieństwa jego wystąpienia daje przedziały ryzyka, gdzie wynik od 1 do 2 zwalnia z konieczności prowadzenia oceny skutków przetwarzania danych (DPIA). Wynik od 3 do 4 z udziałem danych szczególnych i/lub karnych skłania do prowadzenia DPIA. Wynik od 6 do 9 bezwzględnie nakazuje przeprowadzenie DPIA. Wynik analizy widnieje w Rejestrze Czynności Przetwarzania Danych w części DPIA, gdzie stwierdza się konieczność przeprowadzenia oceny skutków przetwarzania danych lub brak takiej konieczności.
- (4) Fundacja ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym celu 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.

## 4.2 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.

Fundacja przeprowadza ocenę skutków planowanych operacji przetwarzania niezależnie od wyników analizy ryzyka jeśli:

- proces przetwarzania danych opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej;
- proces przetwarzania danych odnosi się do przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych karnych;
- proces przetwarzania danych odbywa się z wykorzystaniem systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Fundacja stosuje metodykę oceny skutków przyjętą w **Załączniku nr 12 do Polityki – „Ocena skutków przetwarzania danych”** i z wykorzystaniem tego załącznika dokumentuje przeprowadzenie oceny skutków. Ocena skutków przetwarzania danych jest wykonywana przy udziale Administratora, IOD oraz osoby zaangażowanej w ocenianie czynności przetwarzania danych przed podjęciem przetwarzania danych, które tworzą zespół oceniający. Ocena uwzględnia kryteria bezpieczeństwa, których nieosiągnięcie może spowodować naruszenie praw i wolności osoby, której dane są przetwarzane. Do tych kryteriów należą: poufność (P), integralność (I) i rozliczalność (R) przetwarzania danych. Wskazanie przez zespół oceniający skutki przetwarzania danych w każdym z kryteriów konkretnych zagrożeń w liczbie od 0 do 4 daje poziom szacowany na wartość 1, kolejno w liczbie od 5 do 8 daje wartość 2 i w liczbie od 9 do 12 daje wartość 3. Po oszacowaniu wartości (P), (I), (R) zespół mnożące je przez siebie otrzymuje skalę powagi ryzyka, gdzie:

- wartość od 1 do 3 oznacza niską powagę,
- wartość od 4 do 8 oznacza średnią powagę,
- wartość od 9 do 18 oznacza wysoką powagę.

Stwierdzenie niskiej powagi umożliwia zespołowi oceniającemu skutki przetwarzania wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka.

Stwierdzenie średniej powagi umożliwia zespołowi oceniającemu skutki przetwarzania wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka oraz działanie obniżające przynajmniej jedną z maksymalnych wartości (P), (I), (R).

Stwierdzenie wysokiej powagi umożliwia zespołowi oceniającemu skutki przetwarzania wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka,

ewentualnie jeśli to możliwe zaniechanie przetwarzania danych i/lub delegację skutków ryzyka na stronę trzecią (np. ubezpieczenie) oraz działania obniżające maksymalne wartości (P), (I), (R).

Zespół oceniający po ustaleniu planu reakcji na ryzyko wyznacza metodę monitorowania bieżącego poziomu ryzyka, np. poprzez przegląd zdarzeń o charakterze incydentów bezpieczeństwa.

Jeżeli ocena skutków wskaże, że przetwarzanie powodowałoby wysokie ryzyko (powaga ryzyka liczona w wartości 27), gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka (ryzyko szcątkowe), to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym na zasadach określonych w art. 36 RODO.

### 4.3 Środki bezpieczeństwa

Fundacja stosuje środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz oceny 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.

### 4.4 Zgłaszanie naruszeń

Fundacja stosuje zapisy art. 33 i 34 RODO w identyfikacji, ocenie i zgłoszeniu zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia oraz powiadomienia osób, których dotyczyło naruszenie ochrony danych. W celu udokumentowania nadzoru nad zgłaszaniem naruszeń ochrony danych w Fundacji stosuje się **Załącznik nr 13 do Polityki – „Wzór rejestru naruszeń bezpieczeństwa”**.

## 5. Przetwarzający

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 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”**, a każda umowa jest odnotowana w **Załączniku nr 3 do Polityki – „Wzór ewidencji umów powierzenia przetwarzania danych osobowych”**. Proces do realizacji i nadzoru powierzono Prezesowi Zarządu Fundacji, a każdy pracownik Fundacji, który zamierza zawrzeć z podmiotem zewnętrznym umowę skutkującą powierzeniem danych powinien powiadomić o tym fakcie Prezesa Zarządu Fundacji, który konsultując się z IOD przygotowuje treść umowy powierzenia przetwarzania danych, a po jej podpisaniu odnotowuje ją w ewidencji umów powierzenia. Administrator może zlecić IOD przeprowadzenie weryfikacji wykonywania umowy powierzenia przez podmiot przetwarzający.

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

## **6. Eksport danych**

Fundacja rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.

Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Fundacja okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodnie z prawem ochrony danych rozwiązania równoważne.

## **7. Projektowanie prywatności**

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

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



## **8. Załączniki**

Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”

Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”

Załącznik nr 3 do Polityki – „Wzór ewidencji umów powierzenia przetwarzania danych osobowych”

Załącznik nr 4 do Polityki – „Wzór zgody na przetwarzanie danych”

Załącznik nr 5 do Polityki – „Wzór klauzuli informacyjnej”

Załącznik nr 6 do Polityki – „Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji”

Załącznik nr 7 do Polityki – „Ewidencja osób upoważnionych do przetwarzania danych osobowych”

Załącznik nr 8 do Polityki – „Wzór upoważnienia do przetwarzania danych osobowych”

Załącznik nr 9 do Polityki – „Wniosek o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym”

Załącznik nr 10 do Polityki – „Wzór klauzuli poufności”

Załącznik nr 11 do Polityki – „Wzór protokołu analizy ryzyka”

Załącznik nr 12 do Polityki – „Ocena skutków przetwarzania danych”

Załącznik nr 13 do Polityki – „Wzór rejestru naruszeń bezpieczeństwa”.



### Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”

LP.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych <i>(jeżeli jest to możliwe)</i>	Nazwa współadministratora i dane kontaktowe <i>(jeżeli dotyczy)</i>	Nazwa podmiotu przetwarzającego i dane kontaktowe <i>(jeżeli dotyczy)</i>	Kategorie odbiorców <i>(innych niż podmiot przetwarzający)</i>	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 <i>(jeżeli jest to możliwe)</i>	DPIA (TAK/NIE)	Transfer do kraju trzeciego lub org. międzynarodowej	
														Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń

## Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych”

### Umowa Nr .....

Zawarta w dniu ..... r. w..... pomiędzy:

.....zwanym w dalszej części niniejszej umowy „Zleceniodawcą” reprezentowanym przez:

.....

a

.....

zwanym w dalszej części niniejszej umowy „Wykonawcą” reprezentowanym przez:

.....

o następującej treści:

### § 1

#### Powierzenie przetwarzania danych osobowych

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy (.....) a (.....), o ..... Zleceniodawca powierza Wykonawcy trybie art. 28 ust.3 rozporządzenia Parlamentu Europejskiego i Rady (EU) 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). zwanego dalej RODO przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
3. Powierzone dane zawierają informacje o osobach fizycznych będących osobami fizycznymi.
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

### § 2

#### Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych:  
.....  
.....
2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie , o której mowa w § 1 ust. 1 i w sposób zgodny z niniejszą Umową.

### § 3

#### Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 28 RODO.
2. Wykonawca oświadcza, że:
  - 1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
  - 2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają właściwy do zagrożeń poziom bezpieczeństwa,
  - 3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.
3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
  - 1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
  - 2) każdym nieupoważnionym dostępem do danych osobowych,
  - 3) każdym żądaniem otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.
6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
9. Wykonawca może „podpowierzyć” usługi objęte umową, o której mowa w § 1 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą Zleceniodawcy.

## **Odpowiedzialność Wykonawcy**

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów RODO lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

### **§5**

#### **Czas obowiązywania Umowy powierzenia**

Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia .....

### **§ 6**

#### **Warunki wypowiedzenia Umowy**

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
  - 1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
  - 2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
  - 3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
  - 4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

### **§ 7**

#### **Rozwiązanie Umowy**

Wykonawca, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 i niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

### **§8**

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

### **§9**

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego.

**§10**

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

**§ 11**

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....  
za Zleceniodawcę

.....  
za Wykonawcę

**Załącznik nr 3 do Polityki – „Wzór ewidencji umów powierzenia przetwarzania danych osobowych”**

<b>Lp.</b>	<b>Nazwa podmiotu przetwarzającego</b>	<b>Data podpisania umowy</b>	<b>Data zakończenia umowy</b>	<b>Zakres i kategoria powierzonych danych</b>	<b>Nazwa strony trzeciej jeśli taką wskazano</b>

## Załącznik nr 4 do Polityki – „Wzór zgody na przetwarzanie danych”

### Zgoda na przetwarzanie danych osobowych

Poinformowano mnie o przysługującym mi prawie cofnięcia niniejszej zgody w dowolnym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Aby wycofanie zgody było tak łatwe jak jej wyrażenie Administrator zapewnia mi dostęp w swojej siedzibie do niniejszego formularza i umożliwia złożenie podpisu pod klauzulą „Cofam zgodę na przetwarzanie danych”.

Wyrażam dobrowolnie i świadomie zgodę na przetwarzanie przez Administratora

...**nazwa**

...z siedzibą...**adres,**

w celu

.....  
.....  
.....

poniżej wymienionych moich danych osobowych

.....  
.....  
.....

i poświadczam ten fakt własnoręcznym podpisem pod klauzulą „Wyrażam zgodę na przetwarzanie danych”.

Wyrażam zgodę na przetwarzanie danych

.....

Data i własnoręczny podpis

Cofam zgodę na przetwarzanie danych

.....  
Data i własnoręczny podpis

## Załącznik nr 5 do Polityki – „Wzór klauzuli informacyjnej”

### KLAUZULA INFORMACYJNA – wzór ogólny

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. administratorem Pani/Pana danych osobowych jest ... (*\*nazwa*) z siedzibą w ... (*\*adres*);
2. inspektorem ochrony danych w ... (*\*nazwa*) jest Pan (*\*imię i nazwisko inspektora*) ... (*\*e-mail*) ... ;
3. Pani/Pana dane osobowe przetwarzane będą w celu ... (*\*należy podać cel przetwarzania*) na podstawie ... (*\*należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f. \*Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej*);
4. odbiorcą Pani/Pana danych osobowych będą ... (*\*można wymienić kategorię odbiorców o ile istnieją*);
5. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.
6. Pani/Pana dane osobowe będą przechowywane przez okres ... (*\*jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.*);
7. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;
8. ma Pan/Pani prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;
9. podanie przez Pana/Panią danych osobowych jest ... (*\*wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy*). Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych będzie ... (*\*jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych*);



## Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji

### I

#### **Procedura nadawania upoważnień do przetwarzania danych i uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.**

Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków związanych z przetwarzaniem danych osobowych. Prezes Zarządu Fundacji przygotowuje treść upoważnienia zgodnie ze wzorem określonym w **Załączniku nr 8 do Polityki – „Wzór upoważnienia do przetwarzania danych osobowych”** w dwóch egzemplarzach. Jeden egzemplarz upoważnienia wpina się do teczki z upoważnieniami z podpisem pracownika potwierdzającym odbiór upoważnienia. Drugi egzemplarz otrzymuje osoba upoważniona. Fakt wydania upoważnienia odnotowuje się w Ewidencji osób upoważnionych, którego wzór stanowi **Załącznik nr 7 do Polityki – „Ewidencja osób upoważnionych do przetwarzania danych osobowych”**.

Na zasadach powyżej opisanych następuje cofnięcie upoważnienia czy jego rozszerzenie.

Uprawnienia w systemie informatycznym, w którym przetwarza się dane osobowe nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków związanych z przetwarzaniem danych osobowych z wykorzystaniem systemów informatycznych. Wniosek o wydanie uprawnienia jest kierowany do Administratora przez osobę, która powinna uzyskać uprawnienie pracy w systemie informatycznym. W przypadku akceptacji wniosku, Administrator powiadamia ustnie zainteresowanego o nadaniu uprawnień w systemie informatycznym. Na zasadach powyżej opisanych następuje cofnięcie uprawnienia czy jego rozszerzenie. Druk wzoru wniosku o wydanie uprawnienia określa **Załącznik nr 9 do Polityki – „Wniosek o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym”**.

Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zostaje zapoznany przez Administratora z zasadami ochrony danych osobowych opisanych w Polityce ochrony danych osobowych. Pracownik po zapoznaniu z wspomnianymi zasadami podpisuje klauzulę poufności, której wzór stanowi **Załącznik nr 10 do Polityki – „Wzór klauzuli poufności”**. Każdy z pracowników jest przeszkolony z zakresu tematyki ochrony danych osobowych przez IOD po podjęciu zatrudnienia oraz w razie zmiany istotnych warunków zewnętrznych (np. zmiany przepisów) lub wewnętrznych (np. zmiana stanowiska pracy).

## II

### **Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem**

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem.

1. Hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
  - hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
  - hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
  - hasło nie może być jednakowe z identyfikatorem użytkownika,
  - hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.
2. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
3. Hasło powinno być zmieniane nie rzadziej niż co 30 dni.
4. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie Administratora.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

## III

### **Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych**

Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora.

Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.

Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem do dodatkowych nośników danych, np. płyty CD, pendrive i inne, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następuje poprzez wylogowanie się z tego systemu.

#### IV

#### **Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania**

Kopie zapasowe powinny być kontrolowane przez administratora danych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

#### V

#### **Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych**

Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem. W przypadku uszkodzenia lub zużycia nośnika informacji zawierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

## VI

### **Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych**

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

- poprzez zainstalowanie programu antywirusowego
- poprzez zainstalowanie firewall (zapora sieciowa).
- poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

Kopie zapasowe:

- a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem,

- modyfikacją, uszkodzeniem lub zniszczeniem
- b) usuwa się niezwłocznie po ustaniu ich użyteczności.

## VII

### **Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych**

Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych przez firmy zewnętrzne na podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora.

Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.

Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator.



Załącznik nr 7 do Polityki –

„Ewidencja osób upoważnionych do przetwarzania danych osobowych”

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Czynność przetwarzania danych wg RCPD	Identyfikator <i>(Jeżeli dane są przetwarzane w systemie informatycznym)</i>





**Załącznik nr 8 do Polityki – „Wzór upoważnienia do przetwarzania danych osobowych”**

.....  
Miejscowość i data

**UPOWAŻNIENIE Nr .....  
do przetwarzania danych osobowych**

**I.**

Na podstawie art. 29 RODO z dniem ..... upoważniam Panią/Pana\*) .....

.....  
*(imię i nazwisko)*

zatrudnioną/zatrudnionego/pełniącego funkcję.....

w .....

*(nazwa organizacji)*

do przetwarzania danych osobowych, w celach związanych z :

.....  
*(cel przetwarzania)*

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej i elektronicznej\*)

**II.**

Upoważniam Panią/Pana\*) do przetwarzania danych osobowych w ramach czynności przetwarzania danych:

.....  
*(wpisać zgodnie z RCPD)*

**III.**

1. Upoważnienie wygasa z chwilą ustania Pana/Pani\*) zatrudnienia na stanowisku

..... w .....  
*(wskazać stanowisko pracy/funkcję)*

2. Jednocześnie informuję, że zobowiązany(a) jest Pan(i) do zachowania powyższych informacji w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia.

.....  
*Data i podpis Administratora*

**Uwaga:**

Niniejsze upoważnienie zostało sporządzone w dwóch jednobrzmiących egzemplarzach, które otrzymują:

Osoba upoważniona;

Administrator

\*) *niepotrzebne skreślić*

**Załącznik nr 9 do Polityki – „Wniosek o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym”.**

.....

Miejscowość i data

**Wniosek**

**o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym**

**Wnioskuje** o wydanie uprawnienia/ rozszerzenie/ cofnięcie uprawnienia\* z dnia .....

Pani /Panu\*

.....

(imię i nazwisko)

zatrudnionej/emu w

..... na

stanowisku

..... do

przetwarzania danych osobowych w poniższym systemie / systemach\*:

.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....

.....

Data i podpis

---

Akceptuję / nie akceptuję wniosku\*

.....

Data i podpis Administratora

---

\* niepotrzebne skreślić

**Załącznik nr 10 do Polityki – „Wzór klauzuli poufności”**

**KLAUZULA POUFNOŚCI**

**OŚWIADCZENIE**

Oświadczam, że zapoznano mnie z obowiązującymi w Czarnkowsko-Trzcianeckiej Lokalnej Grupy Działania zasadami ochrony danych osobowych oraz przepisami prawa i zobowiązuję się do ich stosowania.

Świadomy/a jestem obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub zakończeniu współpracy.

Pouczono mnie o konsekwencjach prawnych nieprzestrzegania obowiązujących w Czarnkowsko-Trzcianeckiej Lokalnej Grupy Działania zasad ochrony danych i / lub przepisów krajowych o ochronie danych osobowych.

.....

.....  
*(miejsowość, data)*

*(czytelny podpis)*

## Załączniku nr 11 do Polityki – „Wzór protokołu analizy ryzyka”

### Protokół analizy ryzyka

1. Nazwa analizowanej czynności przetwarzania danych lub ich kategorii  
.....  
.....
2. Data wykonania analizy  
.....  
.....
3. Skład zespołu analizującego ryzyko  
.....  
.....  
.....  
.....
4. Charakter przetwarzania  
.....  
.....
5. Zakres przetwarzania  
.....  
.....
6. Kontekst przetwarzania  
.....  
.....
7. Cel przetwarzania  
.....  
.....
8. Ryzyko naruszenia praw lub wolności osób fizycznych (prawdopodobieństwo i waga zagrożenia)  
Skutek - .....  
Prawdopodobieństwo - .....  
Poziom zagrożenia - .....
9. Rekomendacja do przeprowadzenia oceny skutków przetwarzania danych  
.....  
.....

.....  
Data i podpis Administratora



Załącznik nr 12 do Polityki – „Ocena skutków przetwarzania danych”

<b>Ocena skutków przetwarzania danych</b>		
<b>Data wykonania oceny</b>		
<b>Czynność przetwarzania</b>		
<b>Osoby zaangażowane w przetwarzanie</b>		
<b>Kategoria przetwarzanych danych</b>		
<b>Cel przetwarzania danych – kontekst</b>		
<b>Podstawa przetwarzania danych</b>		
<b>Adekwatność przetwarzania danych</b>		
<b>Realizacja obsługi praw osób</b>		
<b>Stosowane środki ochronne</b>		
<b>Zagrożenia dla poufności (P)</b> Skala od 0 do 4 = 1 od 5 do 8 = 2 od 9 do 12 = 3	1. nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;	
	2. ujawnienie haseł dostępu do zasobów z danymi osobowymi;	
	3. nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;	
	4. utrata nośnika zawierającego dane osobowe;	
	5. klęska żywiołowa, w wyniku której utracono poufność danych osobowych;	
	6. nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym lub innym;	



	7. udostępnianie danych osobowych osobom nieupoważnionym;	
	8. wejście w posiadanie danych osobowych przez osobę nieuprawnioną;	
	9. pokonanie zabezpieczeń fizycznych lub programowych;	
	10. naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych;	
	11. podsłuch lub podgląd danych osobowych;	
	12. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy;	
	<b>Stwierdzony poziom zagrożenia dla poufności wg skali od 1 do 3</b>	
<b>Zagrożenia dla integralności (I)</b>  <b>Skala od 0 do 4 = 1</b> <b>od 5 do 8 = 2</b> <b>od 9 do 12 = 3</b>	1. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;	
	2. błędy, pomyłki;	
	3. awarie sprzętowe (serwer i inne komponenty);	
	4. awarie oprogramowania;	
	5. brak kopii bezpieczeństwa;	
	6. brak narzędzi, urządzeń i innych składników wspomagających integralność (np. brak archiwum)	
	7. zaniechania organizacyjne personelu;	
	8. uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;	
	9. celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych;	

	10. działanie złośliwego oprogramowania (wirusy);	
	11. pożar, zalanie, ekstremalna temperatura, itp.;	
	12. zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).	
	<b>Stwierdzony poziom zagrożenia dla integralności wg skali od 1 do 3</b>	
<b>Zagrożenia dla rozliczalności (R)</b> Skala od 0 do 4 = 1 od 5 do 8 = 2 od 9 do 12 = 3	1. brak kontroli nad dokumentami wykonywanymi na stanowisku w zakresie ich kopiowania i drukowania;	
	2. brak formalizacji zastępstw pracowniczych;	
	3. możliwość wprowadzenia zmian w treści dokumentu zawierającego dane osobowe;	
	4. błędy oprogramowania lub sprzętu;	
	5. nieprzydzielenie użytkownikom indywidualnych zasobów informacyjnych;	
	6. brak ciągłości w administracji systemem informatycznym;	
	7. brak mechanizmów okresowej kontroli zasad wspierających rozliczalność;	
	8. możliwość zniszczenia lub uszkodzenia danych w sposób zamierzony;	
	9. brak rejestracji udostępnienia danych osobowych;	
	10. możliwość wyłudzenia dostępu do danych (np. podszywanie się pod innego użytkownika);	
	11. przebywanie w strefach przetwarzania osób nieupoważnionych w trakcie lub po pracy;	
	12. wykonywanie pracy w sposób zdalny.	
	<b>Stwierdzony poziom zagrożenia dla rozliczalności wg skali od 1 do 3</b>	

Powaga ryzyka	Poufność (P)		Mnożnik (P) x (I) x (R)		Stwierdzona powaga ryzyka	
	Integralność (I)			Skala od 1 do 3 = niska od 4 do 8 = średnia od 9 do 18 = wysoka		
	Rozliczalność (R)					
Plan reakcji na ryzyko						
Ryzyko szacunkowe Jeśli mnożnik (P) x (I) x (R) równy 27						
Metoda monitorowania ryzyka						
Konsultacje z UODO						
Podpisy osób uczestniczących w ocenie skutków przetwarzania danych						

### Załącznik nr 13 do Polityki – „Wzór rejestru naruszeń bezpieczeństwa”.

Lp.	Naruszenie (stypizowany opis naruszenia)	Data i godzina zgłoszenia podejrzenia naruszenia	Data i godzina stwierdzenia naruszenia	Data naruszenia/o kres, którego dotyczy	Kategoria i liczba osób, których dotyczy naruszenie	Zakres danych i/lub kategorii danych, których dotyczy naruszenie	Osoba/źródło informacji o naruszeniu	Miejsce naruszenia	Okoliczności naruszenia – opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia	Opis skutków/konsekwencji	Ryzyko naruszenia praw i wolności	Opis możliwego naruszenia praw lub wolności	Osoba/jednostka odpowiedzialna za naruszenie	Podjęte działania-opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu	Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy zachodzi obowiązek poinformowania UODO	Czy poinformowano organa ścigania	Czy zachodzi obowiązek poinformowania osoby, których naruszenie dotyczy	Monitoring działań naprawczych