|  |
| --- |
| Fundacja Po DRUGIE**POLITYKA**  **ochrony danych osobowych**  **FUNDACJI PO DRUGIE** |

**HISTORIA DOKUMENTU**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L.p. | Wersja i data utworzenia | Podmiot odpowiedzialny | Opis zmian | Data zatwierdzenia i wejścia w życie | Osoba zatwierdzająca |
| 1. | V.1.0 [•].07.2018 | IOD | Nowy dokument | Nowy dokument |  |
|  |  |  |  |  |  |

Spis treści:

[**1. Wprowadzenie** 1](#_Toc520838562)

[**1.1. Kontekst** 1](#_Toc520838563)

[**1.2. Czemu służy niniejszy dokument?** 2](#_Toc520838564)

[**1.3. Zakres stosowania** 3](#_Toc520838565)

[**1.3.1. Do czego stosuje się zasady określone w niniejszym dokumencie?** 3](#_Toc520838566)

[**1.3.1.1. Dane osobowe** 3](#_Toc520838567)

[**1.3.1.2. Przetwarzanie danych osobowych** 3](#_Toc520838568)

[**1.3.1.3. Automatyzacja przetwarzania danych** 4](#_Toc520838569)

[**1.3.1.4. Zbiory danych** 4](#_Toc520838570)

[**1.3.2. Kogo obowiązują zasady określone w niniejszym dokumencie?** 5](#_Toc520838571)

[**1.3.3. Gdzie obowiązują zasady określone w niniejszym dokumencie?** 5](#_Toc520838572)

[**2. Podstawowe zasady przetwarzania danych osobowych** 6](#_Toc520838573)

[**3. System ochrony danych** 7](#_Toc520838574)

[**3.1. Elementy systemu** 7](#_Toc520838575)

[**3.1.1. Inwentaryzacja danych.** 7](#_Toc520838576)

[**3.1.2. Rejestr**. 7](#_Toc520838577)

[**3.1.3. Kontrola dostępu**. 7](#_Toc520838578)

[**3.1.4. Podstawy prawne.** 8](#_Toc520838579)

[**3.1.5. Prawa jednostek i obowiązki informacyjne.** 8](#_Toc520838580)

[**3.1.6. Zawiadamianie o naruszeniach.** 8](#_Toc520838581)

[**3.1.7. Minimalizacja.** 8](#_Toc520838582)

[**3.1.8. Bezpieczeństwo**. 9](#_Toc520838583)

[**3.1.9. Przetwarzający**. 9](#_Toc520838584)

[**3.1.10. Eksport** **danych**. 9](#_Toc520838585)

[**3.1.11. Domyślna ochrona danych oraz ochrona danych już na etapie projektowania.** 9](#_Toc520838586)

[**4. Praca w systemach IT** 9](#_Toc520838587)

[**4.1.1. Użytkownicy.** 9](#_Toc520838588)

[**4.1.2. Nadawanie uprawnień.** 9](#_Toc520838589)

[**4.1.3. Warunki korzystania z systemów IT.** 10](#_Toc520838590)

[**4.1.4. Uwierzytelnianie** 10](#_Toc520838591)

[**4.1.5. Rozpoczęcie, zawieszenie i zakończenie pracy** 10](#_Toc520838592)

[**4.1.6. Kopie zapasowe.** 11](#_Toc520838593)

[**4.1.7. Przechowywanie nośników.** 11](#_Toc520838594)

[**4.1.8. Zapobieganie działaniu szkodliwego oprogramowania.** 11](#_Toc520838595)

[**4.1.9. Korzystanie z urządzeń przenośnych.** 11](#_Toc520838596)

[**4.1.10. Stosowanie wytycznych obowiązujących w Fundacji.** 12](#_Toc520838597)

[**5. Upowszechnianie wiedzy i budowanie kompetencji** 12](#_Toc520838598)

[**6. Kontrola wewnętrzna, nadzór i interpretacja** 12](#_Toc520838599)

[**7. Postanowienia końcowe** 13](#_Toc520838600)

[**Załącznik nr 1 – instrukcja postępowania w razie wystąpienia zdarzeń z zakresu ochrony danych osobowych** 14](#_Toc520838601)

[**Załącznik nr 2 – polityka czystego biurka i czystego ekranu** 1](#_Toc520838602)

[**Załącznik nr 3 – upoważnienie do przetwarzania danych osobowych** 1](#_Toc520838603)

[**Załącznik nr 4 – zobowiązanie do zachowania poufności** 1](#_Toc520838604)

[**Załącznik nr 5 – wzór umowy powierzenia przetwarzania danych osobowych** 1](#_Toc520838605)

[**Załącznik nr 6 – kryteria oceny podmiotu przetwarzającego** 1](#_Toc520838606)

[**Załącznik nr 7 – wzór tabeli rejestru czynności przetwarzania** 1](#_Toc520838607)

[**Załącznik nr 8 – wzór tabeli oceny skutków przetwarzania dla ochrony danych** 1](#_Toc520838608)

[**Załącznik nr 9 – szablon arkusza rejestru zdarzeń bezpieczeństwa z zakresu ochrony danych osobowych** 1](#_Toc520838609)

[**Załącznik nr 10 – szablon arkusza rejestru zdarzeń prawnych z zakresu ochrony danych osobowych** 1](#_Toc520838610)

1. **Wprowadzenie**
   1. **Kontekst**

FUNDACJA PO DRUGIE z siedzibą w Warszawie, adres: ul. Wiązana 22B, 04-680 Warszawa, wpisana do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej oraz do rejestu przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000385460, NIP 9522107635 („**Fundacja**”), prowadzi działalność społecznie użyteczną w sferze zadań publicznych w rozumieniu ustawy o działalności pożytku publicznego i wolontariacie na rzecz ogółu społeczności.

Do celów Fundacji należą m.in.:

* poprawa zdolności adaptacyjnych w środowisku i wsparcie w procesie usamodzielniania i readaptacji społecznej wychowanków i byłych wychowanków placówek resocjalizacyjnych dla nieletnich,
* zapobieganie wykluczeniu i wykolejeniu społecznemu,
* zapobieganie tworzeniu się patologii społecznej,
* podnoszenie poziomu aktywności zawodowej grup zagrożonych wykluczeniem i wykolejeniem społecznym, w szczególności wychowanków i byłych wychowanków placówek resocjalizacyjnych dla nieletnich oraz ich rodzin,
* wyrównywanie szans wychowanków po opuszczeniu placówek resocjalizacyjnych dla nieletnich.

W toku działalności i realizacji swoich celów Fundacja przetwarza dane osobowe, w tym przede wszystkim dane osobowe beneficjentów projektów prowadzonych przez Fundację. Wśród tych danych mogą znaleźć się także dane należące do szczególnych kategorii danych, jak choćby dane dotyczące zdrowia tych osób.

Poza wymogami wynikającymi z dobrych praktyk i odpowiedzialności wobec tych osób, działalność Fundacji musi w tym zakresie odpowiadać przepisom obowiązującego prawa – niezależnie od ram prawnych, w które ujęte są pozostałe obszary i aspekty funkcjonowania Fundacji.

Fundacja podlega zatem szczególnie istotnym obowiązkom na styku następujących płaszczyzn:

* dobrych praktyk, transparentności i rzetelności w stosunku do osób współpracujących z Fundacją oraz, osób, wobec których Fundacja prowadzi działania,
* regulacji wewnętrznych Fundacji, w tym jej Statutu,
* regulacji prawnych w obszarze prowadzonej działalności, w tym ustawy o fundacjach, ustawy o działalności pożytku publicznego i wolontariacie oraz ram prawnych dotyczących poszczególnych obszarów działalności,
* regulacji szczególnych odnoszących się do ochrony danych osobowych.

**FUNDACJA**

W odniesieniu do danych osobowych zestawienie tych sfer zakreśla spektrum danych, które Fundacja może, a niekiedy obowiązana jest pozyskać i przetwarzać, oraz określa cele i warunki ich dopuszczalnego wykorzystania.

Fundacja musi zapewnić należyty poziom ochrony praw i wolności tych osób w związku z przetwarzaniem tych danych, uwzględniając charakter, zakres, kontekst i cele takiego przetwarzania oraz ryzyko naruszenia praw lub wolności o różnym prawdopodobieństwie i wadze zagrożenia, a także wykazać zgodność przetwarzania z prawem.

* 1. **Czemu służy niniejszy dokument?**

Zapewnienie należytego poziomu ochrony praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych oraz wykazanie zgodności przetwarzania z prawem wymaga wdrożenia przez Fundację odpowiednich środków technicznych i organizacyjnych, tworzących system skutecznej ochrony danych osobowych. Środki te obejmują m.in. odpowiednie polityki ochrony danych.

Polityka Ochrony Danych Osobowych Fundacji PO DRUGIE („**Polityka Ochrony Danych**”) służy zapewnieniu zgodności przetwarzania z wymogami prawa oraz dobrymi praktykami, wskazaniu zasad przetwarzania danych osobowych w działalności Fundacji w ramach tego systemu, usystematyzowaniu tego przetwarzania i nadaniu mu stosownych ram, stanowiących wiążące wytyczne i instrukcje postępowania w Fundacji.

Polityka Ochrony Danych służy w szczególności opisowi realizacji i wykazaniu wdrożenia w Fundacji odpowiednich środków technicznych i organizacyjnych zgodnie z Rozporządzeniem 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 (ogólnego rozporządzenia o ochronie danych) („**RODO**”).

Niniejszy dokument ma charakter wewnętrzny i poufny, a jego treść oraz poszczególne opisane w nim rozwiązania techniczne i organizacyjne stanowią informacje chronione Fundacji – za wyjątkiem rozwiązań, które w wymaganym prawem zakresie zostały w uprawniony sposób podane do wiadomości osób, których dane osobowe mogą być w ramach działalności Fundacji przetwarzane (np. w ramach odpowiednich not informacyjnych).

* 1. **Zakres stosowania**
     1. **Do czego stosuje się zasady określone w niniejszym dokumencie?**

Polityka Ochrony Danych ma zastosowanie do przetwarzania przez Fundację danych osobowych w sposób całkowicie lub częściowo zautomatyzowany lub danych osobowych stanowiących lub mających stanowić część zbioru danych. Nie uchybia to pozostałym obowiązującym w Fundacji zasadom ochrony informacji poufnych, o ile zostały przyjęte i wdrożone.

* + - 1. **Dane osobowe**

1. **Dane osobowe** to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej – niezależnie od tego, czy osoba ta jest współpracownikiem Fundacji, czy np. beneficjentem korzystającym z prowadzonych przez Fundację działań.
2. **Osoba możliwa do zidentyfikowania** 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 tożsamość osoby fizycznej.

|  |
| --- |
| **Ważne!**  Dane osobowe to nie tylko dane identyfikujące imię, nazwisko czy nr PESEL osoby fizycznej. Mogą to być także takie informacje jak np. dane o okolicznościach z życiorysu, szczególnych cechach, preferencjach i potrzebach osoby objętej wsparciem Fundacji.  **To, czy uzyskana informacja stanowi dane osobowe, może zależeć od dostępności innych informacji, i w różnych okolicznościach dawać różne wyniki.** |

Do tej samej kategorii (np. adresów e-mail) mogą należeć informacje stanowiące dane osobowe (np. e‑mail w formacie „imię.nazwisko@domena.com”) oraz informacje, które bez dalszych danych takiego waloru będą pozbawione (np. e-mail w formacie „kontakt@domena.com”). Dlatego **informacje, które z dużą dozą prawdopodobieństwa mogą zyskać przymiot danych osobowych, należy traktować tak samo, jak dane osobowe.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Przykłady danych osobowych w Fundacji:**   |  | | --- | | * loginy do systemów informatycznych Fundacji | | * życiorysy osób korzystających ze wsparcia Fundacji | | * dane współpracowników Fundacji w ewidencji udzielanych im upoważnień | |

* + - 1. **Przetwarzanie danych osobowych**

1. **Przetwarzanie danych osobowych** to dowolna operacja lub zestaw operacji wykonywanych na takich danych lub ich zestawach, w sposób zautomatyzowany lub niezautomatyzowany.
2. Przetwarzaniem danych osobowych jest m.in. ich 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, itd.
3. Ocena, czy Fundacja przetwarza dane osobowe, nie zależy od tego, czy operacji przetwarzania Fundacja miałaby dokonywać samodzielnie, czy korzystając z usług podmiotów trzecich (lub na ich zlecenie, np. podmiotu koordynującego prowadzony projekt). Bieżący dostęp do przetwarzanych danych nie jest zatem kryterium decydującym.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ważne!**  Nie istnieje wyczerpujący katalog operacji stanowiących przetwarzanie danych osobowych. Przetwarzaniem jest każda czynność wykonywana na takich danych, czyli każdy dający się wskazać i nazwać odcinek procesu, w którym są wykorzystywane, nawet o niewielkim stopniu zaawansowania.  **Przetwarzaniem danych osobowych są wobec tego także:**   |  |  |  | | --- | --- | --- | | * **przechowywanie danych** | * **przeglądanie danych** | * **usuwanie danych** | |

* + - 1. **Automatyzacja przetwarzania danych**

1. Przetwarzania danych osobowych **w sposób całkowicie lub częściowo zautomatyzowany** to przede wszystkim przetwarzanie takich danych z wykorzystaniem systemów informatycznych, w tym elektronicznych baz danych.
2. Przetwarzaniem danych osobowych w sposób zautomatyzowany będzie **przede wszystkim wykonywanie operacji na takich danych w ramach korzystania z systemów informatycznych Fundacji**.
3. Z takim przetwarzaniem wiążą się jednak także np. takie czynności jak korzystanie z poczty elektronicznej czy sporządzanie zestawień w arkuszach Excel – ogółem: korzystanie z rozwiązań technicznych pozwalających na jakąkolwiek automatyzację, posiadających funkcjonalności wykraczające poza podstawowe operacje na danych.
   * + 1. **Zbiory danych**
4. **Zbiór danych osobowych** to uporządkowany zestaw takich danych, dostępnych według określonych kryteriów. Zestaw może być zbiorem niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub przestrzennie.
5. **Zbiorami danych osobowych Fundacji będą przede wszystkim zestawienia danych osobowych zarządzane i wykorzystywane przez Fundację**, w tym także te o charakterze wewnętrznym, takie jak akta osobowe, ewidencje upoważnień oraz wszystkie inne zestawienia i listy, tak w formie elektronicznej, jak i papierowej, o ile zawierają dane pozwalające na identyfikację osoby fizycznej (patrz pkt 1.3.1.1 powyżej), jeśli wykazują uporządkowanie i pozwalają na udostępnienie danych według określonych kryteriów.

|  |
| --- |
| **Ważne!**  Szczególne zasady ochrony danych osobowych określone w Polityce Ochrony Danych odnoszą się do wszystkich takich danych przetwarzanych w systemach informatycznych Fundacji, w szczególności za pomocą szczególnych narzędzi do obsługi danego procesu, ale także do danych przetwarzanych w postaci papierowej, jeśli będą one zorganizowane według ustalonych kryteriów w ramach uporządkowanej struktury (ewidencje, listy, zestawienia).  Szczególne zasady ochrony danych osobowych nie będą wprawdzie dotyczyć np. pojedynczej, przechowywanej luzem w biurku wizytówki czy notatki z rozmowy z kandydatem, ale pozyskanych z tej wizytówki czy notatki danych, wprowadzonych do systemu IT – już tak. |

* + 1. **Kogo obowiązują zasady określone w niniejszym dokumencie?**

Zasady określone w niniejszym dokumencie obowiązują wszystkie osoby uczestniczące w przetwarzaniu danych w związku z działalnością Fundacji, niezależnie od tego, czy współpraca z nimi opiera się o stosunek pracy, czy o inną odpowiednią podstawę.

W przypadku, w którym Fundacja miałaby współpracować z podmiotami trzecimi – takimi jak dostawcy usług – należy zbadać, czy zapewniają one wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie przez nie danych spełniało obowiązujące wymogi i chroniło prawa osób, których dane dotyczą, np. poprzez realizację procedury opisanej w Załączniku nr 6. Należy ponadto zagwarantować realizację przez te podmioty adekwatnych zasad ochrony danych osobowych i rozliczalności prawidłowego przetwarzania za pomocą odpowiednich środków prawnych, np. poprzez zawarcie umowy, której wzór stanowi Załącznik nr 5.

* + 1. **Gdzie obowiązują zasady określone w niniejszym dokumencie?**

Zasady określone w Polityce Ochrony Danych obowiązują we wszystkich lokalizacjach, budynkach, pomieszczeniach i innych miejscach, w których w Fundacji przetwarzane są dane osobowe.

Przy przetwarzaniu danych osobowych poza siedzibą Fundacji (w szczególności z wykorzystaniem urządzeń mobilnych) środki ochrony danych i urządzeń stosuje się szczególnie rygorystycznie.

|  |
| --- |
| **PODSUMOWANIE**   * Obowiązek ochrony danych osobowych w Fundacji wynika wprost z przepisów obowiązującego prawa, regulujących działalność Fundacji. * Danymi osobowymi mogą stać się dowolne informacje, jeśli tylko umożliwiają identyfikację określonej osoby fizycznej. Nie musi to być jednoznaczne z wskazaniem jej z imienia i nazwiska. * Podlegają one ochronie nawet wówczas, gdy są wyłącznie przechowywane i nie wykorzystuje ich się w żaden inny szczególny sposób. * Dotyczy to nie tylko danych osób trzecich, z którymi Fundacja utrzymuje kontakt, ale w ogóle wszystkich danych osobowych w systemach IT Fundacji, a ponadto danych utrwalonych na papierze, zebranych w zbiory. * Zasady ochrony danych osobowych obowiązują wszystkie osoby działające na polecenie Fundacji, niezależnie od miejsca, gdzie się znajdują, i urządzeń, z jakich korzystają. |

1. **Podstawowe zasady przetwarzania danych osobowych**

Środki przewidziane w niniejszej Polityce Ochrony Danych stanowią konkretyzację podstawowych zasad przetwarzania danych osobowych:

|  |  |
| --- | --- |
|  | 1. Zasada legalności, rzetelności i przejrzystości Dane muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. 2. Zasada ograniczenia celu Dane osobowe mogą być zbierane wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach, oraz nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami. 3. Zasada minimalizacji danych Przetwarzane dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. 4. Zasada prawidłowości - Przetwarzane dane muszą być prawidłowe i w razie potrzeby uaktualniane (dane nieprawidłowe w świetle celów ich przetwarzania należy niezwłocznie usuwać lub prostować). 5. Zasada ograniczenia przechowywania Dane nie mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres dłuższy, niż jest to niezbędne do celów, w których są przetwarzane. 6. Zasada integralności i poufności Dane przetwarza się w sposób zapewniający odpowiednie bezpieczeństwo tych danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. 7. Zasada rozliczalności Należy być w stanie wykazać przestrzeganie w/w zasad. |

**Powyższe zasady stanowią podstawowe dyrektywy, w świetle których należy rozumieć wszystkie wytyczne i zalecenia dotyczące przetwarzania danych w Fundacji, wynikające tak z niniejszej Polityki, jak i poszczególnych procedur szczegółowych.**

1. **System ochrony danych**
   1. **Elementy systemu**

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

* + 1. **Inwentaryzacja danych.**

Fundacja dokonuje identyfikacji zasobów przetwarzanych danych osobowych, kategorii tych danych, podmiotowych i przedmiotowych zależności między tymi zasobami oraz sposobów wykorzystywania posiadanych danych, w tym:

1. przypadków przetwarzania danych należących do szczególnych kategorii danych (tzw. danych wrażliwych, w tym w szczególności danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, a także danych dotyczących zdrowia, seksualności lub orientacji seksualnej) oraz danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;
2. przypadków przetwarzania danych osób, których się nie identyfikuje, lub których identyfikacja jest do celów przetwarzania zbędna;
3. przypadków przetwarzania danych dzieci;
4. profilowania;
5. współadministrowania danymi, powierzania danych Fundacji do przetwarzania przez inne podmioty oraz przez Fundację innym podmiotom przetwarzającym.
   * 1. **Rejestr**.

Fundacja opracowuje, prowadzi i utrzymuje rejestr czynności przetwarzania danych osobowych w Fundacji. Rejestr czynności przetwarzania stanowi „mapę drogową” oraz narzędzie rozliczania i wykazywania zgodności przetwarzania z zasadami ochrony danych. Wzór rejestru stanowi załącznik nr 7 do niniejszej Polityki.

* + 1. **Kontrola dostępu**.

1. Do przetwarzania danych osobowych dopuszczane są jedynie osoby, które zgodnie z przyjętą w Fundacja procedurą nadawania uprawnień zostały upoważnione do przetwarzania danych. Wzór nadawanego upoważnienia stanowi załącznik nr 3.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się z zasadami przetwarzania danych osobowych w Fundacji oraz zachowania poufności. Wzór oświadczenia w powyższym zakresie stanowi załącznik nr 4.
3. Oryginały upoważnień i oświadczeń, o których mowa powyżej, przechowywane są przez Fundację. Osoby posiadające upoważnienie do przetwarzania danych osobowych zostają wpisane do ewidencji osób upoważnionych.
   * 1. **Podstawy prawne.**

Fundacja identyfikuje i weryfikuje podstawy prawne przetwarzania danych administrowanych przez Fundację, zapewniając ich udokumentowanie, w tym:

1. utrzymuje system zarządzania zgodami na przetwarzanie danych (w tym zgodami na szczególne formy tego przetwarzania);
2. inwentaryzuje i odnotowuje uzasadnienie przypadków, gdy Fundacja przetwarza dane na podstawie prawnie uzasadnionego interesu Fundacji.
   * 1. **Prawa jednostek i obowiązki informacyjne.**

Fundacja spełnia obowiązki informacyjne względem osób, których danymi administruje, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

1. **Obowiązki informacyjne.**

Fundacja przekazuje osobom, których dane są przetwarzanie, pełne wymagane prawem informacje, przy zbieraniu danych oraz podczas ich przetwarzania, a także organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

1. **Możliwość realizacji żądań.**

Fundacja weryfikuje i zapewnia możliwość efektywnego wykonania zgłaszanych żądań, zgłoszeń i zapytań.

1. **Obsługa żądań.**

Fundacja zapewnia odpowiednie środki techniczne i organizacyjne, w tym proceduralne, w szczególności procedury opisane w załączniku nr 1, aby żądania osób je zgłaszających były realizowane w terminach i w sposób wymagany przepisami obowiązującego prawa, oraz by podlegały należytemu udokumentowaniu, w szczególności z zastosowaniem procedury opisanej w załączniku nr 10.

* + 1. **Zawiadamianie o naruszeniach.**

Fundacja stosuje procedury pozwalające na ustalenie konieczności zawiadomienia organu nadzoru oraz osób dotkniętych zidentyfikowanym naruszeniem ochrony danych, w szczególności procedury opisane w załączniku nr 1.

* + 1. **Minimalizacja.**

Fundacja stosuje zasady i metody zarządzania minimalizacją przetwarzania danych zgodnie z zasadami domyślnej ochrony danych oraz ochrony danych już na etapie projektowania, w tym:

1. zasady zarządzania adekwatnością danych;
2. zasady reglamentacji i zarządzania dostępem do danych;
3. ocenę okresu przechowywania danych i weryfikację ich dalszej przydatności w toku przetwarzania.
   * 1. **Bezpieczeństwo**.

Fundacja zapewnia poziom bezpieczeństwa danych odpowiadający ryzykom dla praw i wolności osób, których dotyczą, w tym:

1. dokonuje oceny ryzyka dla poszczególnych czynności przetwarzania danych lub ich kategorii;
2. przeprowadza i dokumentuje oceny skutków przetwarzania dla ochrony danych osobowych tam, gdzie ryzyko naruszenia praw i wolności tych osób jest wysokie, zgodnie z załącznikiem nr 8;
3. dostosowuje środki ochrony danych do ustalonego poziomu ryzyka;
4. prawidłowo zarządza incydentami z obszaru bezpieczeństwa danych osobowych, a w szczególności stosuje procedury pozwalające w przypadkach określonych prawem na identyfikację, ocenę, udokumentowanie i zgłoszenie zidentyfikowanego naruszenia ochrony danych organom nadzoru oraz osobom, których prawa i wolności zostały naruszeniem dotknięte, zgodnie z załącznikami nr 1 i 9.
   * 1. **Przetwarzający**.

Fundacja posiada sformułowane zasady doboru podmiotów przetwarzających dane na rzecz Fundacji, zgodnie z załącznikiem nr 6, oraz ustaliła wymogi minimalne co do warunków powierzenia im takiego przetwarzania, zgodnie z załącznikiem nr 5. Fundacja weryfikuje wykonywanie zawartych w tym przedmiocie umów.

* + 1. **Eksport** **danych**.

Fundacja weryfikuje, czy dane nie są przekazywane do państw trzecich (poza terytorium Europejskiego Obszaru Gospodarczego) lub do organizacji międzynarodowych, oraz zapewnia zgodność z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

* + 1. **Domyślna ochrona danych oraz ochrona danych już na etapie projektowania.**

Fundacja zarządza zmianami mającymi wpływ na prywatność. W tym celu opracowując i wdrażając nowe projekty i inwestycje w Fundacji ocenia się wpływ projektowanych zmian na ochronę danych oraz zapewnia się minimalizację przetwarzania, bezpieczeństwo danych i ochronę prywatności.

1. **Praca w systemach IT**
   * 1. **Użytkownicy.**

Użytkownikami systemów IT Fundacji są wyłącznie osoby posiadające stosowne upoważnienie („**Użytkownicy**”).

* + 1. **Nadawanie uprawnień.**

Służby informatyczne Fundacji wprowadzają do systemu dane Użytkowników i nadają odpowiednie uprawnienia. W momencie wygaśnięcia lub ograniczenia upoważnienia użytkownika do przetwarzania danych osobowych służby informatyczne Fundacji odpowiednio usuwają lub ograniczają uprawnienia dostępowe użytkownika do systemu.

* + 1. **Warunki korzystania z systemów IT.**

1. Każdy Użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

* Rozdziałami I do V oraz rozdziałem VIII RODO;
* Niniejszą Polityką Ochrony Danych wraz z załącznikami;
* Dalszymi wytycznymi w zakresie ochrony danych osobowych i korzystania z technologii informacyjnej obowiązującymi w Fundacji, o ile zostały przyjęte.

1. Zapoznanie się z powyższymi informacjami Użytkownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 4.
2. Użytkownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
3. Użytkownik uniemożliwia zarówno w trakcie pracy w systemie, jak i po jej zakończeniu, przetwarzanie danych przez osoby nieuprawnione.
   * 1. **Uwierzytelnianie**
4. Systemy, w którym przetwarzane są dane osobowe, wyposaża się w mechanizmy uwierzytelniania Użytkownika i kontroli dostępu do systemu.
5. Użytkownik w momencie zarejestrowania w systemie otrzymuje od służb informatycznych Fundacji hasło dostępu, oraz instrukcję zmiany swojego hasła. Użytkownik przed przystąpieniem po raz pierwszy do pracy zmienia swoje hasło. Od tego momentu Użytkownik jest jedyną osobą znającą hasło. Ta zasada jest przestrzegana do momentu wyrejestrowania użytkownika z systemu.
6. Użytkownik zobowiązany jest do regularnej zmiany swojego hasła. W razie potrzeby wprowadza się mechanizmy automatycznego wymuszania hasła przez systemy informatyczne. Hasło musi być ponadto zmieniane dodatkowo w każdym momencie, kiedy zachodzi podejrzenie, że hasło przestało być wiadome tylko i wyłącznie Użytkownikowi.
7. W przypadku utraty hasła, służby informatyczne Fundacji nadają nowe hasło. W takim przypadku stosuje się odpowiednio zasady wskazane powyżej.
   * 1. **Rozpoczęcie, zawieszenie i zakończenie pracy**
8. Użytkownik rozpoczynając pracę w systemie informatycznym po ukazaniu się okna logowania proszony jest o podanie hasła.
9. Użytkownik zawieszając pracę w systemie informatycznym zabezpiecza dostęp do systemu za pomocą stosownej funkcjonalności systemu (np. wylogowania się, blokady hasłem, wyłączenia urządzenia, przez które uzyskuje się dostęp do systemu, itp.). Blokada winna następować automatycznie także po okresie bezczynności Użytkownika.
10. Przed opuszczeniem stanowiska pracy, oraz każdorazowo kończąc pracę w systemie IT, Użytkownik obowiązany jest zabezpieczyć dostęp do systemu na zasadach określonych powyżej, a ponadto zabezpieczyć i uporządkować stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, na których znajdują się dane osobowe, w taki sposób, by osoby nieupoważnione nie uzyskały dostępu do danych. Zasady obowiązujące w tym zakresie określa załącznik nr 2.
    * 1. **Kopie zapasowe.**
11. Kopie zapasowe tworzą i przechowują służby informatyczne Fundacji.
12. Kopie zapasowe nie mogą znajdować się w tym samym pomieszczeniu, w którym przechowywane są dane główne.
13. Kopie zapasowe zabezpiecza się przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem poprzez odpowiednie środki ochrony, w tym kryptograficznej i fizycznej.
14. Kopie zapasowe przechowywane są przez okres ich użyteczności.
15. Zdezaktualizowane i uszkodzone kopie zapasowe niszczone są w sposób uniemożliwiający ich ponowne użycie.
16. Szczegółowe zasady w zakresie tworzenia i zarządzania kopiami zapasowymi mogą zostać określone w odrębnych dokumentach.
    * 1. **Przechowywanie nośników.**
17. Elektroniczne nośniki informacji przechowuje się w siedzibie Fundacji w wyznaczonych pomieszczeniach, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
18. Okresowe przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych wykonują służby informatyczne Fundacji.
19. Przeznaczone do likwidacji urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające zapis danych osobowych, należy pozbawić zapisu w sposób uniemożliwiający ich odzyskanie. Służby informatyczne Fundacji zapewniają środki techniczne służące do bezpiecznego usuwania danych.
    * 1. **Zapobieganie działaniu szkodliwego oprogramowania.**
20. System informatyczny zabezpiecza się przed działalnością wirusów i innego szkodliwego oprogramowania za pomocą programu antywirusowego i innych odpowiednich narzędzi.
21. Aktualizacja programu antywirusowego winna następować automatycznie.
22. Po każdorazowym wykryciu szkodliwego oprogramowania użytkownik zobowiązany jest niezwłocznie powiadomić służby informatyczne Fundacji. Służby informatyczne Fundacji po usunięciu szkodliwego oprogramowania sprawdzają system i przywracają go do pełnej funkcjonalności.
    * 1. **Korzystanie z urządzeń przenośnych.**
23. W przypadku przetwarzania danych osobowych przy wykorzystaniu komputerów przenośnych i innych przenośnych urządzeń elektronicznych, oprócz stosowania odpowiednio środków wskazanych powyżej, użytkownik takiego urządzenia zobowiązany jest do:

* transportu urządzenia w sposób minimalizujący ryzyko kradzieży lub zniszczenia, m.in. poprzez przenoszenie urządzenia w torbie/futerale do tego celu specjalnie przeznaczonym oraz zachowanie szczególnej pieczy nad urządzeniem, a zwłaszcza niepozostawianie go w miejscach publicznych;
* nieprzetwarzania danych osobowych w miejscach publicznych lub środkach transportu publicznego;
* wykorzystywania urządzeń, na których przetwarzane są dane osobowe, tylko zgodnie z ich służbowym przeznaczeniem;
* umożliwienia wykonywania kopii zapasowych i aktualizacji oprogramowania.

1. Fundacja prowadzi ewidencję wykorzystywanych urządzeń przenośnych, obejmującą:

* typ i numer seryjny urządzenia;
* imię i nazwisko użytkownika;
* datę przekazania urządzenia użytkownikowi.
  + 1. **Stosowanie wytycznych obowiązujących w Fundacji.**

1. Szczegółowe warunki odnoszące się do zachowania bezpieczeństwa przy korzystaniu z systemów informatycznych, w tym m.in.: korzystania z sieci Fundacji, służbowej poczty elektronicznej, urządzeń przenośnych, dokumentacji zawierającej istotne dane (przez co należy rozumieć także dokumenty zawierające dane osobowe), publicznego dostępu do Internetu, tworzenia kopii zapasowych, ustawień bezpieczeństwa oraz drukowania, kopiowania i wysyłania faksem informacji itp. mogą zostać uregulowane w szczegółowych wytycznych w zakresie ochrony danych osobowych i korzystania z technologii informacyjnej obowiązujących w Fundacji, o ile wytyczne takie zostaną przyjęte.
2. W przypadku rozbieżności w/w zasad z obowiązującymi przepisami prawa należy stosować wymogi określone obowiązującym prawem.
3. W razie rozbieżności w/w zasad z wytycznymi w zakresie ochrony danych osobowych i korzystania z technologii informacyjnej obowiązujących w Fundacji, o ile wytyczne takie zostaną przyjęte, należy stosować postanowienia bardziej rygorystycznie odnoszące się do bezpieczeństwa danych, przy poszanowaniu obowiązujących przepisów prawa.
4. **Upowszechnianie wiedzy i budowanie kompetencji**
5. Fundacja zapewnia upowszechnienie wiedzy i budowanie kompetencji w obszarze objętym Polityką Ochrony Danych.
6. Pracownicy Fundacja uczestniczący w realizacji zadań i czynności określonych Polityką Ochrony Danych odbywają szkolenia przekazujące wiedzę i budujące umiejętności w zakresie bezpieczeństwa i zgodności z prawem przetwarzania danych osobowych. Odbycie przez tych pracowników szkoleń jest obowiązkowe i podlega udokumentowaniu. Warunkiem uznania szkolenia za odbyte może być w szczególności pozytywne zaliczenie przez pracownika testu podsumowującego szkolenie.
7. **Kontrola wewnętrzna, nadzór i interpretacja**
8. Nadzoru nad przestrzeganiem postanowień Polityki Ochrony Danych dokonuje Inspektor Ochrony Danych.
9. Inspektor Ochrony Danych prowadzi okresowe kontrole zgodnie z przyjętym harmonogramem.
10. Inspektor Ochrony Danych ma także kompetencje do wydawania wiążących interpretacji postanowień Polityki Ochrony Danych, a w przypadkach wymagających wzmożenia stosowanych środków w sposób nią nieprzewidziany – zezwalania i nakazywania odstępstw na rzecz środków bardziej restrykcyjnych.
11. **Postanowienia końcowe**

Pracownicy i współpracownicy Fundacji, uczestniczący w realizacji zadań i czynności określonych Polityką Ochrony Danych, przed udzieleniem im upoważnienia do przetwarzania danych osobowych potwierdzają zapoznanie się z przepisami Polityki Ochrony Danych na piśmie oraz zobowiązują się do utrzymania w tajemnicy danych osobowych, informacji dotyczących ich przetwarzania, a także sposobów ich zabezpieczenia.

|  |  |
| --- | --- |
|  | Dn. [•] 2018 r. zatwierdził:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ za FUNDACJA PO DRUGIE [imię, nazwisko, funkcja] |

**Załącznik nr 1 – instrukcja postępowania w razie wystąpienia zdarzeń z zakresu ochrony danych osobowych**

|  |
| --- |
| **INSTRUKCJA POSTĘPOWANIA W RAZIE WYSTĄPIENIA ZDARZEŃ Z ZAKRESU OCHRONY DANYCH OSOBOWYCH**   1. **Wprowadzenie i określenie celu.**   Ze względu na wymogi prawne, w szczególności obowiązki określone w Rozporządzeniu 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 (ogólnego rozporządzenia o ochronie danych), oraz dobre praktyki i odpowiedzialność przed interesariuszami, w tym podmiotami danych, w Fundacji PO DRUGIE przyjmuje się instrukcję postępowania w razie wystąpienia zdarzeń z zakresu ochrony danych osobowych („**Instrukcja**”).  Celem wdrożenia Instrukcji jest zapewnienie:   1. faktycznej realizacji uprawnień podmiotów danych, oraz 2. poprawnej identyfikacji zagrożeń i zdarzeń z zakresu ochrony danych osobowych, prawidłowej reakcji na incydenty, skutecznego minimalizowania naruszeń poprzez sprawne podejmowanie skutecznych działań naprawczych oraz ograniczania ryzyka wystąpienia naruszeń w przyszłości poprzez poparte rzetelną analizą działania prewencyjne. 3. **Zakres obowiązywania.**   Instrukcja obowiązuje wszystkich pracowników i współpracowników Fundacji, niezależnie od zajmowanego przez nich stanowiska oraz charakteru pracy, jak również miejsca jej wykonywania.  Instrukcja uzupełnia pozostałe polityki przyjęte w Fundacji, w szczególności Politykę Ochrony Danych. Jeżeli jednak z przepisów prawa oraz postanowień pozostałych polityk, procedur i instrukcji wiążących Fundację wynikają wymogi bardziej rygorystyczne niż stwierdzone w Instrukcji, stosować się należy do wymogów bardziej rygorystycznych.   1. **Definicje.** 2. **Incydent**: niepożądane lub niespodziewane zdarzenie bezpieczeństwa skutkujące naruszeniem. 3. **Naruszenie**: przypadkowe lub niezgodne z prawem zniszczenie, utrata, modyfikacja, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych osobowych. 4. **Zdarzenie**: 5. **zdarzenie prawne**: otrzymanie przez Fundację żądania, zgłoszenia, zapytania lub podobnego środka kierowanego przez osobę, której dane dotyczą, zmierzającego do realizacji uprawnienia przysługującemu temu podmiotowi (**zgłoszenie**), lub 6. **zdarzenie bezpieczeństwa**: wystąpienie stanu wskazującego na potencjalne naruszenie ochrony danych osobowych lub realną możliwość jego wystąpienia, tak w obrębie systemu IT, jak i poza takim systemem, np. poprzez zaistnienie uprzednio nieznanej sytuacji lub ich serii, które mogą być istotne z perspektywy ochrony danych osobowych. 7. **Zasady ogólne – kolejność działań.** 8. W razie stwierdzenia bądź podejrzenia wystąpienia zdarzenia, podstawową kolejność działań wyznacza następujący schemat: 9. **Identyfikacja** Obejmuje działania od powzięcia wiadomości o zdarzeniu bądź podejrzeniu jego wystąpienia (otrzymaniu zgłoszenia, zapoznania się ze stanem systemu, dokonania obserwacji), dokonania wstępnych ustaleń i zebrania podstawowych informacji zgodnie z przyjętymi metodami do przekazania i przejęcia sprawy przez osoby kompetentne.   Każda osoba, która powzięła wiadomość o zdarzeniu bądź podejrzewa jego wystąpienie, zbiera podstawowe informacje i przystępuje do dalszych czynności, a jeśli ze względu na zakres obowiązków nie jest właściwa do zajęcia się sprawą – przekazuje ją osobom kompetentnym zgodnie z zakresem odpowiedzialności w zarządzaniu danym obszarem.  W przypadku zdarzeń bezpieczeństwa w obrębie systemów IT należy bezzwłocznie zawiadomić służby informatyczne Fundacji.  Obowiązek zawiadomienia służb informatycznych Fundacji obowiązuje w szczególności wówczas, jeśli wystąpiły: (a) modyfikacja danych przez osobę nieupoważnioną, w tym osobę, która dostęp do danych uzyskała korzystając z systemu IT Fundacja za pomocą uwierzytelniania lub dostępu nadanego innemu użytkownikowi, w tym poprzez zalogowanie za pomocą hasła dostępu innego użytkownika; (b) błąd w programie, który zniszczył lub uszkodził dane; (c) awaria urządzenia, która zniszczyła lub uszkodziła dane; (d) działanie wirusów i innego szkodliwego oprogramowania, które zniszczyło lub uszkodziło dane; (e) zagubienie lub kradzież elektronicznego nośnika informacji, na którym przechowywane były dane.  Należy ponadto bezzwłocznie powiadomić bezpośredniego przełożonego oraz Inspektora Ochrony Danych. W przypadku braku możliwości samodzielnego ustalenia osób kompetentnych, osoba, która powzięła wiadomość o zdarzeniu, przekazuje sprawę wzwyż ścieżki raportowania – aż do ustalenia tych osób.   1. **Rejestrowanie** Obejmuje działania w zakresie odnotowania i utrwalenia informacji o zdarzeniu bądź podejrzeniu jego wystąpienia po przejęciu sprawy przez osoby odpowiedzialne za jej prowadzenie w ramach identyfikacji, aż do zamknięcia sprawy, w tym także gromadzenie i zabezpieczanie dowodów związanych ze zdarzeniami, które mogłyby zostać wykorzystane w ewentualnych postępowaniach sądowych.   Po przejęciu sprawy osoba odpowiedzialna w toku czynności utrwala otrzymane i wytworzone informacje oraz dokumentuje okoliczności ich otrzymania. **W zakresie, w jakim informacje nie są automatycznie utrwalane za pomocą odpowiednich środków technicznych, dla zdarzenia zakłada się arkusz zdarzenia zgodnie z załącznikiem nr 9 lub 10 do niniejszej Polityki, włączany odpowiednio do rejestru zdarzeń bezpieczeństwa lub rejestru zdarzeń prawnych z zakresu ochrony danych osobowych**; arkusz ten należy odpowiednio uzupełniać w toku czynności.     1. **Analiza** Obejmuje dokonanie ustaleń co do faktów oraz ich ocenę w świetle zasad ochrony danych, w sposób pozwalający potwierdzić albo wykluczyć wystąpienie zdarzenia, względnie ustalić prawdopodobieństwo jego wystąpienia, określić kategorię zdarzenia oraz zebrać informacje niezbędne do dokonywania dalszych czynności.   Osoba odpowiedzialna dokonuje w toku czynności ustaleń i ocen:  • w ramach zdarzenia prawnego – co do prawidłowości wystąpienia przez podmiot danych ze środkiem prawnym, a następnie co do zasadności, możliwości i warunków jego realizacji przez Fundację, lub  • co do stwierdzenia wystąpienia zdarzenia bezpieczeństwa, a następnie co do rodzaju działań, jakie należy podjąć w celu usunięcia lub ograniczenia skutków zdarzenia oraz ograniczenia ryzyka występowania tego rodzaju zdarzeń w przyszłości, w szczególności poprzez: (a) zapoznanie się z zaistniałą sytuacją i dokonanie określenia sposobu dalszego postępowania; (b) żądanie wyjaśnień dotyczących zdarzenia od osoby powiadamiającej o zdarzeniu oraz od każdej innej osoby, która może posiadać informacje związane ze zdarzeniem; (c) dokonanie zabezpieczenia systemu IT lub urządzenia przed rozprzestrzenianiem się skutków zaistniałego naruszenia lub powstałego zagrożenia, w tym poprzez ograniczenie dostępu do systemu i danych osobom niepowołanym; (d) zabezpieczenie śladów zdarzenia przed usunięciem; (e) przekazanie informacji o zdarzeniu i dokonanych ustaleniach do przełożonego lub Inspektora Ochrony Danych.   1. **Priorytetyzacja** Obejmuje określenie pilności sprawy w ramach działalności Fundacji, tak bezpośrednio w odniesieniu do zasad ochrony danych, jak i w porównaniu z równolegle obsługiwanymi zdarzeniami, w sposób pozwalający na ustalenie właściwej kolejności czynności, a także w razie potrzeby na eskalację wzwyż ścieżki raportowania, zaś jeśli to niezbędne – także bezpośrednio do centrum decyzyjnego Fundacji (zarządu), umożliwiając właściwym osobom prawidłową koordynację i komunikację tak wewnątrz Fundacji, jak i w razie potrzeby z innymi podmiotami.   Na podstawie ustaleń zebranych w ramach analizy, osoba odpowiedzialna ustala wagę zdarzenia, w razie potrzeby konsultując się z innymi osobami, w tym z przełożonymi, nadaje sprawie należyty priorytet i w razie potrzeby eskaluje ją w drodze służbowej, a w przypadkach uzasadnionych pilnością i wagą sprawy – także z pominięciem tej drogi, przekazując niezbędne informacje bezpośrednio do kierownictwa Fundacji.   1. **Określenie powiązań** Obejmuje wykrycie zależności pomiędzy zdarzeniem a innymi zdarzeniami, także hipotetycznymi, które mogą wiązać się z wystąpieniem badanego zdarzenia.   Osoba odpowiedzialna weryfikuje, czy zdarzenie ma wpływ na identyfikację innych zdarzeń, ich analizę lub usunięcie ich przyczyn, a w szczególności czy zgłoszone jednorazowo zdarzenie nie ma szerszego wymiaru i czy nie dotyczy innych danych, innych rodzajów i warunków ich przetwarzania lub też innych podmiotów danych, np. czy utrudnienie lub uniemożliwienie dostępu do systemu IT, choćby samo nie skutkowało naruszeniem, nie wynika z czynników zewnętrznych, służących do zamaskowania właściwego zagrożenia naruszeniem, oraz czy wątpliwości podniesione w ramach obsługi zdarzenia prawnego nie odnoszą się także do innych osób fizycznych w porównywalnej sytuacji.   1. **Podjęcie działań** obejmujewdrożenie, ocenę i monitorowanie środków naprawczych i zapobiegawczych, których adekwatność wynika z wcześniejszych ustaleń i czynności dokonanych w toku sprawy.   Osoba odpowiedzialna dokonuje niezbędnych i adekwatnych czynności w celu jak najszybszej realizacji środka skierowanego wobec Fundacji w ramach zdarzenia prawnego, względnie w celu jak najszybszego zabezpieczenia zdarzenia bezpieczeństwa, w szczególności usunięcia ewentualnych naruszeń i uchylenia ich skutków, a także zapobieżenia wystąpieniu podobnych zdarzeń w przyszłości.  W związku ze zdarzeniem bezpieczeństwa osoba odpowiedzialna realizuje w szczególności wytyczne wydane jej przez przełożonego, służby informatyczne Fundacji lub Inspektora Ochrony Danych.  Do momentu otrzymania takich wytycznych, a także równolegle z ich realizacją, o ile otrzymane wytyczne temu się nie sprzeciwiają, osoba odpowiedzialna powinna zabezpieczyć dostęp do pomieszczenia lub urządzenia, w którym nastąpiło zdarzenie. Osoba powiadamiająca o zdarzeniu powinna w szczególności: (a) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zdarzenia oraz działania mające na celu ustalenie jego przyczyn lub sprawców; (b) rozważyć wstrzymanie bieżącej pracy z wykorzystaniem danego urządzenia, celem zabezpieczenia miejsca i warunków zdarzenia; (c) zaniechać – o ile to możliwe – dalszych planowanych czynności, które mogą wiązać się z lub wpływać na zdarzenie, i które mogą utrudnić późniejsze udokumentowanie oraz analizę zdarzenia; (d) wstępnie udokumentować zdarzenie; (e) w miarę możliwości nie pozostawiać miejsca zdarzenia bez nadzoru.   1. **Ocena w razie podejrzenia incydentu i stwierdzenia naruszenia**   https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png**W myśl obowiązujących przepisów prawa, naruszenia ochrony danych osobowych nie zawsze mogą pozostać wewnętrzną sprawą Fundacji.**  **Przepisy przewidują konieczność dokonania oceny ryzyka wystąpienia negatywnych skutków takich naruszeń** na płaszczyźnie praw i wolności osób, których objęte naruszeniem dane dotyczą. **Dalsze kroki uzależniane są od wyniku tej oceny.**  W niektórych przypadkach przepisy przewidują konieczność powiadomienia organu nadzoru lub osób, których dane dotyczą.  Niezależnie od wystąpienia samego naruszenia, jego błędna identyfikacja i ocena związanych z nim ryzyk może stanowić samodzielną podstawę do odpowiedzialności cywilnej i administracyjnej, także finansowej, oraz wiązać się z szeregiem dalszych ryzyk dla działalności Fundacji. Z tego względu właściwe działanie od momentu powzięcia podejrzenia o naruszeniu jest niezwykle istotne, tak samo jak należyte udokumentowanie tego działania.  Prawa i wolności, które mogą zostać zagrożone uszczerbkiem, to przede wszystkim samo prawo do ochrony danych osobowych i prawo do prywatności, ale nie tylko. Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do jakiegokolwiek uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla tych osób.  Ma to miejsce np. wówczas, jeżeli przetwarzanie może poskutkować kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych szczególną tajemnicą, lub wszelką inną szkodą gospodarczą lub społeczną, a w szczególności jeżeli objęte naruszeniem zostały dane wrażliwe, należące do szczególnych kategorii danych (np. dane dotyczące zdrowia) lub dane dotyczące wyroków skazujących, ale także jeżeli objęte naruszeniem dane wiążą się z dokonywaniem w toku przetwarzania oceny czynników osobowych, w szczególności analizy lub prognozy aspektów dotyczących m.in. sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się w celu tworzenia lub wykorzystywania profili osobistych.  Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której określa się poziom ryzyka związany z operacjami przetwarzania danych.   1. **Obowiązek notyfikacyjny wobec organu nadzoru**   https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png**Jeśli prawdopodobieństwo, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, jest większe niż małe, zachodzi obowiązek poinformowania organu nadzoru:**   1. W razie powzięcia informacji o naruszeniu ochrony danych osobowych, powzięcia podejrzenia jego wystąpienia lub w razie stwierdzenia takiego naruszenia, osoba odpowiedzialna natychmiast powiadamia Inspektora Ochrony Danych, odnotowując godzinę stwierdzenia naruszenia, oraz eskaluje sprawę wzwyż ścieżki raportowania. 2. W ciągu maksymalnie 48 godzin od stwierdzenia naruszenia, osoba odpowiedzialna w konsultacji z Inspektorem Ochrony Danych oraz innymi osobami właściwymi w zakresie zarządzania danym obszarem dokonuje oceny ryzyka, analizując zaistniałe i możliwe skutki naruszenia na płaszczyźnie praw i wolności osób, których objęte naruszeniem dane dotyczą. 3. Jeśli nie wykluczono zaistnienia ryzyka naruszenia praw i wolności podmiotów danych w stopniu większym niż mały, osoba odpowiedzialna eskaluje sprawę bezpośrednio do ścisłego centrum decyzyjnego Fundacji (zarządu), które w uzgodnieniu z Inspektorem Ochrony Danych zapewnia koordynację podejmowanych działań. 4. Inspektor Ochrony Danych lub inna osoba właściwa w ciągu maksymalnie 24 godzin od dokonania oceny, nie przekraczając 72 godzin od stwierdzenia naruszenia, powiadamia organ nadzoru (Prezesa Urzędu Ochrony Danych Osobowych). Powiadomienie powinno nastąpić bez zbędnej zwłoki, w miarę możliwości z wykorzystaniem zapewnianego przez organ nadzoru systemu teleinformatycznego umożliwiającego administratorom danych dokonywanie zgłoszenia naruszenia ochrony danych osobowych. Do powiadomienia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. 5. Jeżeli mimo grożącego upływu terminu 72 godzin nie ustalono jeszcze wszystkich okoliczności incydentu, nie przeprowadzono całościowej oceny oraz nie określono i nie podjęto działań naprawczych i zapobiegawczych w sposób wyczerpujący, powiadomienia należy dokonać z uwzględnieniem aktualnego stanu wiedzy i działań. Dalsze informacje należy przekazywać sukcesywnie w drodze powiadomień następczych, bez zbędnej zwłoki. 6. Osoba dokonująca powiadomienia dokumentuje godzinę jego dokonania. 7. Osoba dokonująca powiadomienia zamieszcza w nim następujące elementy: 8. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; 9. opis charakteru naruszenia ochrony danych osobowych, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; 10. opis możliwych konsekwencji naruszenia ochrony danych osobowych; 11. opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych oraz w celu zminimalizowania jego ewentualnych negatywnych skutków. 12. Jeśli objęte naruszeniem dane przetwarzane są przez Fundację w imieniu innego podmiotu, który powierzył ich przetwarzanie, po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza się je administratorowi. 13. **Obowiązek notyfikacyjny wobec osoby, której dane dotyczą**   https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png**Jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, może zachodzić ponadto obowiązek poinformowania tych osób:**   1. Jeśli nie wykluczono zaistnienia ryzyka naruszenia praw i wolności podmiotu danych w stopniu wysokim, osoba odpowiedzialna w konsultacji z Inspektorem Ochrony Danych dokonuje oceny skuteczności technicznych i organizacyjnych środków ochrony, które miały zastosowanie do danych osobowych, których dotyczy naruszenie, w szczególności pod kątem uniemożliwienia osobom nieuprawnionym dostępu i odczytu, i bada, czy wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, może zostać wyeliminowane przed ziszczeniem się jego skutków, a jeśli tak – niezwłocznie podejmuje stosowne czynności. 2. Jeśli wysokie ryzyko nie może zostać wyeliminowane, Inspektor Ochrony Danych lub inna osoba właściwa bez zbędnej zwłoki powiadamiają o naruszeniu ochrony danych osobowych osoby, której dane dotyczą. 3. Do komunikacji z osobami, których dane dotyczą, stosuje się wymogi w zakresie przejrzystości przekazu jak przy obsłudze zdarzeń prawnych: 4. Informacji udziela się w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny, jasnym i prostym językiem. 5. W celu weryfikacji przystępności komunikatu można posłużyć się narzędziami analitycznymi do oceny przejrzystości tekstu (np. <http://jasnopis.pl/aplikacja>), zgodnie z warunkami ich wykorzystania, na potrzeby weryfikacji uprzednio usuwając z weryfikowanego komunikatu wszelkie dane osobowe. 6. Osoba dokonująca powiadomienia zamieszcza w nim następujące elementy: 7. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; 8. opis charakteru naruszenia ochrony danych osobowych; 9. opis możliwych konsekwencji naruszenia ochrony danych osobowych; 10. opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych oraz w celu zminimalizowania jego ewentualnych negatywnych skutków. 11. Jeśli powiadamianie w sposób indywidualny wymagałoby niewspółmiernie dużego wysiłku, osoba, która miałaby dokonywać powiadomień, o stwierdzonych przeszkodach informuje centrum decyzyjne Fundacji (zarząd), które wyjątkowo może zdecydować o zastąpieniu powiadomień indywidualnych wydaniem publicznego komunikatu lub zastosowaniem podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. 12. **Zasady obsługi zdarzeń prawnych.** 13. **Weryfikacja:** 14. Realizacja żądania w ramach zdarzenia prawnego wymaga potwierdzenia przez osobę odpowiedzialną, że podmiot kierujący zgłoszenie jest tożsamy z podmiotem danych, których dotyczy zgłoszenie (**weryfikacja**). 15. Weryfikacja może opierać się w szczególności o treść danych przetwarzanych przez Fundację (np. poprzez historię wcześniejszych kontaktów z Fundacją). 16. Jeśli osoba odpowiedzialna poweźmie uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie w ramach zdarzenia prawnego, powinna zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości tej osoby w zakresie wymaganym do dokonania weryfikacji. 17. **Komunikacja:** 18. Osoba odpowiedzialna po dokonaniu weryfikacji, analizie treści żądania i określeniu niezbędnych kroków udziela żądanych informacji w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny, jasnym i prostym językiem. 19. Osoba odpowiedzialna w celu weryfikacji przystępności komunikatu może posłużyć się narzędziami analitycznymi do oceny przejrzystości tekstu (np. <http://jasnopis.pl/aplikacja>), zgodnie z warunkami ich wykorzystania, na potrzeby weryfikacji uprzednio usuwając z weryfikowanego komunikatu wszelkie dane osobowe. 20. Informacji należy udzielać w formie zgodnej z życzeniem osoby kierującej zgłoszenie, a jeśli nie wyraziła takiego życzenia – w formie odpowiadającej formie, w której przekazała zgłoszenie, w udokumentowany sposób. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie. 21. Ustna forma komunikacji dopuszczalna jest wówczas, jeśli tożsamość rozmówcy zostanie zweryfikowana innymi sposobami. 22. **Termin:** 23. Osoba odpowiedzialna zapewnia realizację kierowanego wobec Fundacji środka bez zbędnej zwłoki po otrzymaniu zgłoszenia, a w każdym przypadku przed upływem miesiąca od tej daty. 24. W przypadku skomplikowanego charakteru lub liczby żądań termin może zostać wyjątkowo przedłużony o kolejne dwa miesiące. O przedłużeniu terminu decyduje się po uzgodnieniu z Inspektorem Ochrony Danych, o ile dla danego rodzaju zdarzeń prawnych nie zostały ustalone inne zasady postępowania. W każdym wypadku o przedłużeniu terminu osobę kierującą żądanie należy powiadomić w przeciągu miesiąca od otrzymania zgłoszenia. 25. Miesięczny termin na powiadomienie obowiązuje także w przypadku odmowy, jeśli zawarte w zgłoszeniu żądanie miałoby nie podlegać uwzględnieniu (np. ze względu na bezzasadność żądania), co nie zwalnia z obowiązku poinformowania podmiotu danych o odmowie i jej przyczynach. 26. **Odpłatność:** 27. Realizacja kierowanego wobec Fundacji środka jest wolna od opłat. 28. Opłatę można pobrać jedynie w wyjątkowych wypadkach, jeśli żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. O pobraniu opłaty decyduje osoba odpowiedzialna w porozumieniu ze swoim przełożonym i Inspektorem Ochrony Danych, o ile dla danego rodzaju zdarzeń prawnych nie zostały ustalone inne zasady postępowania. Opłata musi wówczas odpowiadać kosztom udzielenia informacji, prowadzenia komunikacji i podjęcia żądanych działań. 29. **Nieuwzględnienie żądania:** 30. Osoba odpowiedzialna może odmówić uwzględnienia żądania kierowanego w ramach środka prawnego tylko wówczas, jeżeli żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, lub jeśli stwierdziła, że nie jest w stanie zidentyfikować występującej z takim żądaniem osoby (po rozważeniu okoliczności może jednak zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą). 31. W razie nieuwzględnienia żądania osobę kierującą żądanie należy pouczyć o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem. 32. **Zasady obsługi zdarzeń bezpieczeństwa.**   Fundacja może przyjmować i wdrażać szczegółowe zasady obsługi zdarzeń bezpieczeństwa w poszczególnych obszarach – w szczególności w obszarze bezpieczeństwa środowiska teleinformatycznego i fizycznego, obszarze technologii informacyjnej oraz w obszarze organizacyjnym. Zastosowanie znajdują dalsze obowiązujące w Fundacji wytyczne w zakresie ochrony danych i korzystania z technologii informacyjnej, o ile zostały przyjęte. |

**Załącznik nr 2 – polityka czystego biurka i czystego ekranu**

|  |
| --- |
| **ZASADY BEZPIECZNEJ I POUFNEJ PRACY Z DOKUMENTACJĄ PAPIEROWĄ I ELEKTRONICZNĄ: POLITYKA CZYSTEGO BIURKA I CZYSTEGO EKRANU**   1. **Wprowadzenie i określenie celu.**   W Fundacji obowiązuje polityka czystego biurka i czystego ekranu („**Polityka CBE**”).  Jej zasady wynikają nie tylko z potrzeb zachowania ładu odpowiadającego wymogom wysokiej wydajności, higieny i ergonomii, ale także ze względów bezpieczeństwa informacji i ochrony poufności danych, w tym w szczególności ochrony danych osobowych zawartych w papierowych i elektronicznych dokumentach wykorzystywanych w bieżącej, codziennej pracy.  Celem wdrożenia Polityki CBE jest uwrażliwienie pracowników i współpracowników Fundacji, niezależnie od ich funkcji i stanowiska, na problematykę bezpieczeństwa informacji i ochrony danych, a przez to stworzenie środowiska, w którym dbałość o te wartości należy do swoistego kodu kulturowego organizacji, i w którym każdy świadomie przyczynia się do ograniczania ryzyk i zagrożeń w tym zakresie.   1. **Zakres obowiązywania.**   Polityka CBE obowiązuje wszystkich pracowników i współpracowników Fundacji, niezależnie od zajmowanego przez nich stanowiska oraz charakteru pracy, jak również miejsca jej wykonywania.  Polityka CBE uzupełnia pozostałe polityki przyjęte w Fundacji, w szczególności Politykę Ochrony Danych. Jeżeli jednak z przepisów prawa oraz postanowień pozostałych polityk, procedur i instrukcji wiążących Fundację wynikają wymogi bardziej rygorystyczne niż stwierdzone w Polityce CBE, stosować się należy do wymogów bardziej rygorystycznych.   1. **Zalecenia ogólne. Zasady 5-S:**   Model postępowania zgodnie z Polityką CBE wyznacza hasłowo **5 zasad „S”**, odnoszonych do bezpieczeństwa informacji i ochrony danych:   1. **Sortowanie**   Wyeliminowanie ze środowiska pracy zbędnych elementów, takich jak dokumenty, materiały, notatki i nośniki danych, które nie są konieczne do wykonywania bieżących zadań.  Pozostawia się tylko dane przydatne, tylko w niezbędnej ilości, i tylko na czas, w którym istnieje potrzeba ich wykorzystania. Dane zbędne niszczy się w należyty sposób, natomiast dane, które na dany moment nie są przydatne, zabezpiecza się i umieszcza w miejscu ich przechowywania.   1. **Systematyka**   Organizacja elementów środowiska pracy oraz ich oznaczenie w sposób umożliwiający łatwość ich identyfikacji, odnalezienia, użycia i odłożenia na miejsce, czytelne także dla innych osób mających uprawniony interes w dostępie do nich. Umożliwienie wizualnej kontroli danych, ich statusu, sposobu wykorzystania oraz stanu prowadzonych z ich użyciem prac.   1. **Sprzątanie**   Stałe i rutynowe porządkowanie środowiska pracy, umożliwiające bieżące identyfikowanie źródeł potencjalnych problemów i anomalii.   1. **Standaryzacja**   Wypracowanie ustalonych sposobów i modeli wykonywania czynności w zakresie pozostałych kroków, utrwalanie dobrych praktyk.  Wkomponowanie dbałości o jednolitość czynności przetwarzanych danych, sposobów ich wykorzystywania i zabezpieczenia w rutynę bieżących czynności operacyjnych.   1. **Samodyscyplina**   Wyrobienie potrzeby wewnętrznej dbałości o bezpieczeństwo informacji, a także utrzymanie nawyków i przyzwyczajeń ułatwiających pracę zgodnie z przyjętymi standardami.  Osiągnięcie efektu w postaci utrzymywania „czystego biurka” oraz utrzymywania wypracowanego efektywnego systemu pracy z danymi i dokumentami zgodnie z wymogami ochrony danych i dobrymi praktykami w tym zakresie.   1. **Zalecenia szczegółowe:** 2. **Dokumenty, pisma, wydruki**   Na koniec dnia pracy, a także na czas nieobecności, wszystkie dokumenty w formie papierowej zabezpiecza się poprzez umieszczenie w przeznaczonych na nie miejscach (teczki, segregatory, szuflady, szafki, organizatory).  Unika się pozostawiania dokumentów widocznych na stanowisku pracy. Informacje o charakterze wrażliwym i poufnym przechowuje się w zamknięciu.   1. **Ekrany**   Monitory ekranowe na czas nieobecności użytkownika przy stanowisku zabezpiecza się blokadą.   1. **Stanowiska komputerowe**   Unika się pozostawiania stacji roboczych i systemów w trybach oszczędzania energii, wstrzymania, uśpienia itp. na koniec dnia pracy. Preferowanym sposobem zakończenia pracy jest ich pełne zamknięcie. Laptopy i inne urządzenia przenośne fizycznie zabezpiecza się przed niepowołanym dostępem.   1. **Środki dostępu**   Fizycznych i logicznych środków dostępu (hasła komputerowe, klucze, karty elektroniczne) nie przechowuje się w miejscach publicznie dostępnych, jak blaty biurek czy zasobniki na przybory biurowe i nie pozostawia bez nadzoru.  Haseł nie przechowuje się w systemach teleinformatycznych w formie niezabezpieczonej kryptograficznie. Nie udostępnia się ich innym osobom i nie zapisuje w formie papierowej w sposób dostępny dla osób trzecich – w szczególności nie zapisuje się ich na kartach post-it i nie umieszcza na elementach stacji roboczych.   1. **Drukowanie**   Wydruki podejmuje się z drukarek bezpośrednio po ich wydrukowaniu. Wydruków nie pozostawia się na drukarce.   1. **Nośniki danych**   Elektroniczne nośniki danych, jak pamięci SD, nośniki optyczne, urządzenia typu pendrive itp., traktuje się jako wrażliwe i przechowuje w zamknięciu.   1. **Niszczenie**   Przedarcie i wyrzucenie wydruku do kosza na odpadki nie stanowi bezpiecznego niszczenia dokumentu. Preferowaną metodą usuwania dokumentacji papierowej jest niszczarka bądź umieszczenie w bezpiecznym pojemniku na dokumentację do zniszczenia. |

**Załącznik nr 3 – upoważnienie do przetwarzania danych osobowych**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Upoważnienie nr \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (numer porządkowy)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (miejscowość, data)  **UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH**  Działając w imieniu Fundacji PO DRUGIE z siedzibą w Warszawie, adres: ul. Wiązana 22B, 04-680 Warszawa, wpisanej do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej oraz do rejestu przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000385460, NIP 9522107635 („**Fundacja**”), na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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 (ogólnego rozporządzenia o ochronie danych) („**RODO**”),  udzielam Pani/Panu:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (imię i nazwisko)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (stanowisko)  [bezterminowo / do dn. [•]] upoważnienia do przetwarzania danych osobowych w zakresie pełnionych obowiązków na zajmowanym stanowisku, tj. [w szczególności]:   |  |  | | --- | --- | | **Czynności przetwarzania:** | **Zakres upoważnienia / opis autoryzowanych czynności:** | |  |  | |  |  |   a ponadto w zakresie wynikającym z poleceń kierowanych przez przełożonego.  Upoważnienie niniejsze uchyla i zastępuje wszystkie upoważnienia do przetwarzania danych osobowych udzielone uprzednio. Upoważnienie może zostać w każdej chwili odwołane. Upoważnienie w każdym przypadku traci ważność z chwilą ustania stosunku pracy/zakończenia współpracy z Fundacja.  Jednocześnie zobowiązuję Panią/Pana do stosowania się przy przetwarzaniu danych do przepisów RODO oraz wszystkich odnośnych aktów prawnych je uzupełniających i zastępujących, jak również do przyjętej w Fundacja polityki ochrony danych, instrukcji i procedur w tym zakresie, a także do zachowania w tajemnicy danych osobowych, informacji dotyczących ich przetwarzania, a także sposobów ich zabezpieczenia.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (podpis uprawnionej osoby nadającej upoważnienie) |

**Załącznik nr 4 – zobowiązanie do zachowania poufności**

|  |
| --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (miejscowość, data)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (imię i nazwisko składającego oświadczenie)  **OŚWIADCZENIE OSOBY UPOWAŻNIONEJ W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH ORAZ DOSTĘPEM DO ŚRODOWISKA IT**  Oświadczam, że zapoznałam/łem się z przepisami oraz zasadami postępowania dotyczącymi ochrony danych osobowych w Fundacji PO DRUGIE z siedzibą w Warszawie, i zobowiązuję się do przestrzegania:   1. przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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 (ogólnego rozporządzenia o ochronie danych) wraz z dalszymi aktami prawnymi je uzupełniającymi; 2. polityki ochrony danych obowiązującej w Fundacji PO DRUGIE, wraz z procedurami i instrukcjami o charakterze szczegółowym, w szczególności z zasadami bezpieczeństwa IT.   Zobowiązuję się w szczególności do zachowania tajemnicy w stosunku do przetwarzanych danych osobowych, informacji dotyczących ich przetwarzania, a także sposobów ich zabezpieczenia. Zobowiązuję się w szczególności do nie sporządzania w sposób nieuprawniony kopii tych danych, w tym kopii w formie cyfrowej, a także kopii wykonywanych poprzez utrwalenie dowolną techniką obrazu ekranu urządzenia, na którym są przetwarzane, jak również kopii wykonywanych poprzez dokonanie wydruku z systemu informatycznego lub dowolne inne oddanie tych danych w formie papierowej.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (podpis) |

**Załącznik nr 5 – wzór umowy powierzenia przetwarzania danych osobowych**

|  |
| --- |
| **UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH**  zawarta w [•] dnia [•], pomiędzy:   1. Fundacją PO DRUGIE z siedzibą w Warszawie, adres: ul. Wiązana 22B, 04-680 Warszawa, wpisaną do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej oraz do rejestu przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000385460, NIP 9522107635 („**Administrator**”),   reprezentowaną przez [•];  oraz   1. **w przypadku spółek prawa handlowego:**   [•], spółką z siedzibą w [•], adres: [•], wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy [•], [•] Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr. KRS [•], NIP [•] („**Procesor**”),  reprezentowaną przez [•];  **w przypadku osoby fizycznej:**  [•] zamieszkałym/ą w [•], adres: [•], [*prowadzącym/ą działalność gospodarczą pod firmą:* [•]*, wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, adres głównego miejsca wykonywania działalności:* [•]], NIP [•], PESEL [•] („**Procesor**”);  Administrator i Procesor są zwani dalej łącznie „Stronami”, a każdy z nich z osobna „Stroną”.   1. **PRZEDMIOT UMOWY** 2. Umowa powierzenia zostaje zawarta w związku i w celu wykonywania umowy [●] z dnia [●] („**Umowa główna**”). Przetwarzanie danych osobowych w związku z wykonywaniem Umowy głównej podlega przepisom Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych iw sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („**RODO**”). 3. Na podstawie Umowy powierzenia Administrator powierza Procesorowi do przetwarzania dane osobowe określone w Załączniku A do Umowy powierzenia („**Dane osobowe**”). 4. Procesor przetwarza Dane osobowe wyłącznie w celu realizacji Umowy głównej i w zakresie niezbędnym do jej wykonania oraz jedynie w czasie jej obowiązywania.   Procesor zobowiązany jest przetwarzać Dane osobowe zgodnie z Rozporządzaniem, innymi obowiązującymi przepisami prawa oraz Umową.   1. **OBOWIĄZKI STRON** 2. Procesor zobowiązany jest do: 3. stosowania wszelkich adekwatnych do poziomu ryzyka środków technicznych i organizacyjnych zabezpieczających Dane osobowe na zasadach określonych w art. 32 RODO; 4. pomagania Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO, przy uwzględnieniu charakteru przetwarzania i informacji dostępnych dla Procesora; 5. przetwarzania Danych osobowych wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego obowiązujące prawo krajowe lub unijne; w takim przypadku przed rozpoczęciem przetwarzania Procesor informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny; 6. w miarę możliwości, pomagania Administratorowi poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO; 7. zapewnienia, by osoby upoważnione do przetwarzania Danych osobowych zobowiązywały się do zachowania tajemnicy, chyba że będą to osoby zobowiązane do zachowania tajemnicy na podstawie ustawy; 8. po zakończeniu Umowy, w zależności od żądania Administratora, usunięcia lub zwrotu Danych osobowych i usunięcia ich kopii, chyba że przepisy prawa bezwzględnie obowiązującego przewidują inaczej. 9. Procesor jest uprawniony do dalszego powierzenia przetwarzania Danych osobowych dalszym podmiotom przetwarzającym, których lista stanowi Załącznik B do Umowy. Procesor poinformuje Administratora o każdej zamierzonej zmianie na liście dalszych podmiotów przetwarzających w sposób przyjęty dla komunikacji zgodnie z Umową. Administrator ma możliwość sprzeciwienia się takiej zmianie w ciągu kolejnych 7 dni. Procesor zapewnia, że będzie korzystał wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO, a także chroniło prawa osób, których dane dotyczą. Procesor zobowiązany jest zapewnić, by na dalsze podmioty przetwarzające zostały nałożone co najmniej te same obowiązki co nałożone na Procesora w Umowie. Administrator przyjmuje do wiadomości, że brak zgody na zmianę na liście dalszych podmiotów przetwarzających może skutkować niemożliwością dalszego wykonywania Umowy przez Procesora, o czym Procesor poinformuje Administratora niezwłocznie. 10. Procesor udostępni Administratorowi informacje niezbędne do wykonywania jego obowiązków związanych z powierzeniem przetwarzania Danych osobowych. Procesor umożliwi Administratorowi przeprowadzenie audytów, w tym inspekcji, w zakresie dotyczącym powierzenia przetwarzania Danych osobowych i zapewni współpracę w tym zakresie. Koszty audytu ponosi każda ze Stron we własnym zakresie, niezależnie od jego wyniku. 11. **TRANSFER DANYCH**   Procesor nie będzie przekazywał Danych osobowych poza terytorium EOG, chyba że uzyska w tym zakresie odrębne zezwolenie Administratora, którego Administrator nie odmówi bez uzasadnionych przyczyn, a taki transfer będzie odbywać się w zgodzie z przepisami RODO. W każdym wypadku przekazanie odbywać się będzie wyłącznie w celu realizacji Umowy głównej.   1. **ODPOWIEDZIALNOŚĆ**   Niezależnie od postanowień Umowy głównej, odpowiedzialność Procesora w związku z przetwarzaniem Danych osobowych na podstawie Umowy ograniczona jest do kwoty [●], chyba że bezwzględnie obowiązujące przepisy prawa stanowią inaczej.   1. **POSTANOWIENIA KOŃCOWE** 2. Umowa zawarta jest na czas obowiązywania Umowy głównej. Umowa może zostać wypowiedziana przez Administratora ze skutkiem natychmiastowym w przypadku rażącego lub powtarzającego się naruszania Umowy, Rozporządzenia lub innych obowiązujących przepisów prawa z zakresu ochrony danych osobowych, przez Procesora, pod warunkiem uprzedniego wezwania Procesora do usunięcia naruszeń, wyznaczenia w tym celu dodatkowego terminu, nie krótszego niż 7 dni, oraz bezskutecznego upływu tego terminu. Wypowiedzenie Umowy wymaga formy pisemnej pod rygorem bezskuteczności. 3. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem bezskuteczności, z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian. 4. Każda ze Stron jest obowiązana do poinformowania na piśmie drugiej Strony o zmianie adresu dla doręczeń korespondencji. W przypadku braku poinformowania o zmianie adresu, uznaje się za aktualny adres ostatnio wskazany ze skutkiem doręczenia. 5. Wszelkie pojęcia pisane wielką literą, a niezdefiniowane w Umowie, mają znaczenie nadane im w Umowie głównej. 6. Wszelkie spory mające związek z Umową będą rozstrzygane przez sąd właściwy zgodnie z Umową główną. 7. Załączniki do Umowy stanowią jej integralną część. Lista załączników jest następująca: 8. Załącznik A – Zakres powierzenia danych osobowych 9. Załącznik B – Lista dalszych podmiotów przetwarzających   **ZAŁĄCZNIK A**  ZAKRES POWIERZENIA DANYCH OSOBOWYCH:   1. Charakter oraz cele przetwarzania: (…) 2. Kategorie osób, których dane dotyczą: (…) 3. Rodzaj danych osobowych: (…) 4. Terytorium, na którym przetwarzane będą dane osobowe: (…)   **ZAŁĄCZNIK B**  LISTA DALSZYCH PODMIOTÓW PRZETWARZAJĄCYCH |

**Załącznik nr 6 – kryteria oceny podmiotu przetwarzającego**

|  |
| --- |
| **WERYFIKACJA PODMIOTU PRZETWARZAJĄCEGO**  **Wymogi prawne:**  W celu pozytywnej weryfikacji podmiotu przetwarzającego konieczne jest spełnienie przez ten podmiot wszystkich wymogów określonych w punktach 1-4:   1. **Czy podmiot prowadzi rejestr naruszeń?**   Rejestr naruszeń jest dokumentem, w którym powinny być ewidencjonowane wszelkie incydenty – naruszenia ochrony danych osobowych. W rejestrze opisuje się zdarzenie, które miało miejsce, skutki naruszenia oraz podjęte działania zaradcze, mające na celu usunięcie skutków naruszenia oraz zminimalizowanie prawdopodobieństwa powtórzenia się naruszenia w przyszłości.   1. **Czy pracownicy / współpracownicy podmiotu są upoważnieni do przetwarzania danych osobowych?**   Każda osoba mająca dostęp do danych osobowych powinna zostać upoważniona do ich przetwarzania przez administratora lub podmiot przetwarzający. Pytanie ma na celu zweryfikowanie, czy podmiot udzielił swoim pracownikom / współpracownikom wymaganych upoważnień.   1. **Czy osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?**   Wymóg zobowiązania do zachowania tajemnicy przez osoby przetwarzające dane z upoważnienia podmiotu przetwarzającego wynika z art. 28 RODO. Konieczne jest zatem, aby osoby upoważnione do przetwarzania danych zobowiązały się do zachowania poufności (w odrębnym dokumencie lub części umowy zawartej pomiędzy podmiotem a jego pracownikiem / współpracownikiem).   1. **Jeżeli podmiot dokonuje transferów danych do państw poza EOG, to czy zapewniony jest mechanizm legalizujący taki transfer?**   W przypadku transferów danych poza EOG należy zapewnić, aby taki transfer był legalny (przykładem mechanizmu legalizującego transfer jest zawarcie umowy w brzmieniu zgodnym ze standardowymi klauzulami umownymi przyjętymi przez Komisję Europejską). Przykładem, gdy dochodzi do transferu jest sytuacja, gdy wykonaniu podlega umowa na świadczenie usług hostingowych z usługodawcą, którego serwery znajdują się w USA.  **Kryteria dodatkowe:**  Kryteria oceny wiedzy fachowej oraz wiarygodności podmiotu (w przypadku niespełnienia co najmniej jednego z wymogów określonych w punktach 5-8, ankietę należy przekazać do oceny Inspektorowi Ochrony Danych lub innej właściwej osobie):   1. **Czy został powołany Inspektor Ochrony Danych (IOD) lub została wyznaczona osoba do wykonywania zadań związanych z zapewnieniem zgodności przetwarzania danych osobowych u dostawcy z obowiązującym prawem?**   IOD jest powoływany w przypadkach określonych w art. 37 RODO, a także gdy dany podmiot zdecyduje się na jego wyznaczenie w sytuacji, gdy przepisy nie narzucają takiego obowiązku. Jeżeli nie ma formalnie powołanego IOD, wówczas należy wskazać, czy została wyznaczona inna osoba, która jest odpowiedzialna za wykonywanie zadań w zakresie ochrony danych osobowych u dostawcy.   1. **Czy IOD lub inna osoba wyznaczona do wykonywania zadań związanych z ochroną danych osobowych posiada odpowiednie kwalifikacje, dające gwarancję zgodności przetwarzania danych osobowych zgodnie z przepisami prawa?**   Za osobę spełniającą wskazany wymóg uważa się w szczególności: osobę, która posiada udokumentowane i rzeczywiste doświadczenie w pełnieniu funkcji IOD (wcześniej: administratora bezpieczeństwa informacji), osobę, która ukończyła studia podyplomowe w dziedzinie ochrony danych osobowych lub bezpieczeństwa informacji na uczelni wyższej, radcę prawnego lub adwokata z co najmniej 2-letnim doświadczeniem w dziedzinie ochrony danych osobowych, itp.   1. **Czy podmiot posiada wdrożone mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony danych osobowych?**   Celem tego pytania jest zweryfikowanie, czy podmiot posiada dostateczną wiedzę i kompetencję, aby być w stanie zidentyfikować oraz ocenić naruszenia ochrony danych osobowych w jego organizacji.   1. **Czy podmiot posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzenia bezpieczeństwa informacji?**   W rachubę wchodzą m.in. certyfikat ISO 27001, CISA, CISSP itd. |

**Załącznik nr 7 – wzór tabeli rejestru czynności przetwarzania**

|  |  |
| --- | --- |
| **REJESTR CZYNNOŚCI PRZETWARZANIA – ADMINISTRATOR DANYCH OSOBOWYCH ARKUSZ NR A-[•]** | |
| 1. **Administrator danych osobowych [A]:** | [Wskazanie Fundacji jako administratora danych osobowych, dane kontaktowe administratora i wszelkich współadministratorów, a gdy ma to zastosowanie – także ich przedstawicieli.]   * Fundacja PO DRUGIE, ul. Wiązana 22B, 04-680 Warszawa [e-mail], [tel.] |
| 1. **Inspektor ochrony danych [A]:** | [Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych Fundacji.]   * [Imię, nazwisko; adres] [e-mail], [tel.] |
| 1. **Określenie czynności przetwarzania:** | [Czynność przetwarzania podlegająca rejestracji – zbiorcze oznaczenie operacji przetwarzania, które łączy realizacja wspólnego celu.] |
| 1. **Cele przetwarzania:** | [Cele przetwarzania danych osobowych przez Fundację w ramach danej czynności.] |
| 1. **Opis kategorii podmiotów danych:** | [Uogólniające wspólne wskazanie grup podmiotów danych (np. współpracownicy Fundacji, osoby objęte wsparciem w ramach danego programu itp.), przy uwzględnieniu cech i powiązań wspólnych dla członków tych grup.] |
| 1. **Opis kategorii danych osobowych:** | [Zakres przetwarzanych danych osobowych, z uwzględnieniem szczególnych kategorii danych.] |
| 1. **Kategorie odbiorców:** | [Kategorie odbiorców, którym dane zostały lub zostaną ujawnione, w tym odbiorców – podmiotów trzecich będących samodzielnymi administratorami ujawnionych im danych [O], oraz podmiotów przetwarzających dane działających na rzecz Fundacji [P].] |
| 1. **Przekazywanie poza EOG / do organizacji międzynarodowych:** | [Gdy ma to zastosowanie, informacje o przekazywaniu danych osobowych przez Fundację lub działające na rzecz Fundacji podmioty przetwarzające do państwa trzeciego lub organizacji międzynarodowej: nazwa państwa lub organizacji, a w przypadku przekazań na podstawie uzasadnionego interesu administratora w warunkach art. 49 ust. 1 II RODO, dokumentacja zabezpieczeń (jako załącznik).] |
| 1. **Terminy usunięcia poszczególnych kategorii danych:** | [Informacja o planowanych terminach usunięcia poszczególnych kategorii danych, o ile możliwe jest jej podanie.] |
| 1. **Ogólny opis środków bezpieczeństwa:** | [Ogólna informacja (opis) o technicznych i organizacyjnych środkach bezpieczeństwa, jeśli jest dostępna.] |
| 1. **Data aktualizacji / uwagi:** | [Data wypełnienia arkusza oraz ewentualne informacje dodatkowe, o ile są dostępne.] |
| **REJESTR CZYNNOŚCI PRZETWARZANIA – PODMIOT PRZETWARZAJĄCY ARKUSZ NR P-[•]** | |
| 1. **Podmiot przetwarzający [P]:** | [Nazwa oraz dane kontaktowe Fundacji jako podmiotu przetwarzającego.]   * Fundacja PO DRUGIE, ul. Wiązana 22B, 04-680 Warszawa [e-mail], [tel.] |
| 1. **Inspektor ochrony danych [P]:** | [Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych Fundacji.]   * [Imię, nazwisko; adres] [e-mail], [tel.] |
| 1. **Administrator danych osobowych [A]:** | [imię i nazwisko lub nazwa oraz dane kontaktowe administratora, w imieniu którego Fundacja działa jako podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela tego administratora.]   * [Np. podmiot prowadzący dany program (inna fundacja, organ administracji itp.)] |
| 1. **Inspektor ochrony danych [A]:** | [Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych administratora, j/w.]   * [John Doe, ul. Przykładowa, 00-001 Przykład, e-mail, tel.] |
| 1. **Kategorie przetwarzań:** | [Skategoryzowane określenie procesu przetwarzania.] |
| 1. **Przekazywanie poza EOG / do organizacji międzynarodowych:** | [Gdy ma to zastosowanie, informacje o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań na podstawie uzasadnionego interesu administratora w warunkach art. 49 ust. 1 II RODO, dokumentacja zabezpieczeń (jako załącznik).] |
| 1. **Ogólny opis środków bezpieczeństwa:** | [Ogólna informacja (opis) o technicznych i organizacyjnych środkach bezpieczeństwa, jeśli jest dostępna.] |
| 1. **Data aktualizacji / uwagi:** | [Data wypełnienia arkusza oraz ewentualne informacje dodatkowe, o ile są dostępne.] |

**Załącznik nr 8 – wzór tabeli oceny skutków przetwarzania dla ochrony danych**

|  |  |  |
| --- | --- | --- |
| Ocena skutków przetwarzania nr [•] z dn. [•] | | |
| Nazwa procesu: | [Np.:   * „Rekrutacja do programu XYZ”.] | |
| Nowy proces / / aktualizacja oceny: | [„Nowy proces” lub „aktualizacja oceny skutków przetwarzania nr [•] z dn. [•].”] | |
| Opis planowanych operacji przetwarzania: | [Np.:   * „zebranie i utrwalenie danych przekazywanych przez kandydata do programu prowadzonego przez Fundację (kwestionariuszy, innych dokumentów), przeglądanie i wykorzystanie tych danych przez osobę upoważnioną na potrzeby dokonania oceny kandydata, przechowywanie danych przez okres retencji zgodnie z wymogami programu”, itp.] | |
| Kategorie podmiotów danych: | [Np.:   * „kandydaci do programu XYZ”, * „osoby wchodzące i wychodzące z pomieszczeń biurowych wykorzystywanych na potrzeby siedziby Fundacji”, * „użytkownicy systemów IT Fundacji”, * „pracownicy i współpracownicy Fundacji”, itp.] | |
| Cel przetwarzania: | [Np.:   * „dokonanie oceny kwalifikacyjnej kandydata do programu XYZ”, * „ustalenie, dochodzenie i obrona roszczeń Fundacji”, itp.] | |
| Podstawa prawna: | [Podstawa prawna w rozumieniu art. 6 ust. 1 lub art. 9 ust. 2 RODO, np.:   * „zgoda podmiotu danych – art. 6 ust. 1 lit. a) RODO”, względnie „art. 9 ust. 2 lit. a) RODO”, * „wymóg prawny – art. 6 ust. 1 lit. c) RODO; obowiązek prawny ciążący na Fundacji na podst. [•]”, * „uzasadniony interes Fundacji – art. 6 ust. 1 lit. f) RODO; ustalanie, dochodzenie i obrona roszczeń (w sposób przeważający nad interesem podmiotu danych w ich nieprzetwarzaniu)”, itp.] | |
| Ocena niezbędności i proporcjonalności: | [Oceniając operacje przetwarzania, Fundacja musi zweryfikować, czy planowane czynności są adekwatne i stosowne względem wyznaczonych celów, oraz czy ich podjęcie nie jest nadmiarowe w relacji do tych celów.  Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne do celu przetwarzania, powinna zawierać:   1. ustalenie, jakie dane są niezbędne do realizacji celu, 2. wskazanie, jakie dane będą podlegać planowanym operacjom przetwarzania, 3. stwierdzenie, czy wszystkie dane, które mają podlegać planowanym operacjom przetwarzania, są do realizacji celu niezbędne (stwierdzenie, czy z procesu wyeliminowano dane zbędne i nadmiarowe), 4. ustalenie, jakie operacje przetwarzania są niezbędne do prawidłowego przetwarzania tych danych w świetle celu, 5. wskazanie, jakie operacje przetwarzania będą wykonywane (patrz opis powyżej), 6. stwierdzenie, czy wszystkie poszczególne operacje przetwarzania, które mają być wykonywane, są do realizacji celu niezbędne, i czy realizacji tego celu nie można osiągnąć za pomocą środków mniej ingerujących w prywatność jednostki.] | |
| Ocena ryzyka naruszenia praw i wolności podmiotu danych | [Oceniając ryzyko naruszenia praw i wolności osób, których dane dotyczą, Fundacja musi rozważyć możliwie pełne spektrum faktycznych oraz prawnych zagrożeń wynikających dla tych osób z przetwarzania ich danych, wybierając metodę top‑down/bottom-up lub ich kombinację wg. zasadności danej metodyki. Ocena powinna uwzględniać ryzyka nie tylko w toku prawidłowego, ale także nieprawidłowego przebiegu procesu przetwarzania, także z udziałem podmiotów trzecich (tak upoważnionych – np. powierzenie przetwarzania – jak i nieupoważnionych).  Ustalenia powinny móc sprowadzić się do jednej z następujących, wzajemnie się wykluczających konkluzji, stanowiącej punkt wyjścia do określenia środków zaradczych:   * nie zidentyfikowano ryzyka naruszenia praw lub wolności osób, których dane dotyczą, * zidentyfikowano ryzyko, które nie zostało jednak uznane za wysokie, * zidentyfikowano ryzyko, które uznano za wysokie.] | |
| Obowiązek uprzedniej konsultacji z PUODO: | https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png | [Jeśli ocena ryzyka wskaże, że przetwarzanie powodowałoby wysokie ryzyko (niezależnie od podjęcia środków w celu zminimalizowania tego ryzyka), przed rozpoczęciem przetwarzania Fundacja konsultuje się z organem nadzorczym.] |
| Planowane środki  zapobieżenia ryzyku oraz  wykazania zgodności: | [Określenie środków podejmowanych w celu zaradzenia ryzyku wiążącemu się z przetwarzaniem, w tym ryzykom wynikającym z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.  Wykazanie zastosowania zasady ochrony danych osobowych już w momencie projektowania procesu oraz zasady domyślnej ochrony danych osobowych.  Wyszczególnienie sposobu, w jaki środki te ukierunkowane są na respektowanie praw i wolności podmiotów danych, a także środków pozwalających udokumentować i wykazać zapewnioną zgodność, z uwzględnieniem:   * stanu wiedzy technicznej, * kosztu wdrożenia, * charakteru, zakresu, kontekstu i celów przetwarzania, * ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.   Do rozważenia przykładowe środki techniczne i organizacyjne:   * zabezpieczenia fizyczne i logiczne (ograniczenie i kontrola dostępu, CCTV), * środki ochrony kryptograficznej, szyfrowanie i pseudonimizacja, * środki ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, * wdrożenie procedur i instrukcji, szkolenia personelu, * bariery informacyjne („need-to-know-basis”, „Chinese wall”), itp.] | |
| Ocena ryzyka po zastosowaniu środków zapobieżenia ryzyku: | [Np.:  „Jak wykazały wyniki analiz, studium wykonalności oraz przeprowadzonych testów, planowane środki pozwolą na wyeliminowanie stwierdzonych ryzyk; należy zapewnić należytą kontrolę właściwego wdrożenia planowanych środków oraz dokonać audytu ich skuteczności po upływie miesiąca od wdrożenia, oraz dokonywać audytów okresowych w interwałach półrocznych.”, itp.] | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ za administratora danych osobowych Fundacja PO DRUGIE: [imię, nazwisko, funkcja]     \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Inspektor Ochrony Danych dla Fundacji PO DRUGIE: [imię, nazwisko] | | |

**Załącznik nr 9 – szablon arkusza rejestru zdarzeń bezpieczeństwa z zakresu ochrony danych osobowych**

|  |  |  |
| --- | --- | --- |
| Rejestr zdarzeń bezpieczeństwa z zakresu ochrony danych osobowych Arkusz zdarzenia nr [•] z dn. [•] | | |
| Opis zdarzenia (hasłowo): | [Stypizowany opis zdarzenia.] | | |
| Data uzyskania informacji: | [Data i godzina uzyskania informacji o zdarzeniu] | | |
| Źródło informacji: | [Osoba zgłaszająca lub inne źródła informacji o zdarzeniu] | | |
| Data / okres zdarzenia: | [Data i godzina zdarzenia; okres, którego zdarzenie dotyczy.] | | |
| Osoby dotknięte zdarzeniem: | [Kategorie i ilość podmiotów danych, których dotyczy zdarzenie.] | | |
| Dane dotknięte zdarzeniem: | [Zakres i kategorie danych, których dotyczy zdarzenie.] | | |
| Lokalizacja zdarzenia: | [Lokalizacja fizyczna lub element systemu IT, w którym nastąpiło zdarzenie.] | | |
| Analiza zdarzenia: | [Opis i ocena charakteru zdarzenia pod kątem okoliczności i przyczyn jego wystąpienia oraz zagrożeń dla ochrony danych osobowych oraz praw i wolności podmiotów danych.] | | |
| Stwierdzenie naruszenia: | [Ustalenie, czy nastąpiło zniszczenie, utrata, modyfikacja, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych osobowych – tj. czy zdarzenie miało charakter incydentu.] | | |
| Data i godzina stwierdzenia naruszenia (jeśli stwierdzono): | [Istotne ze względu na bieg terminów na dokonanie zgłoszeń.] | | |
| Opis skutków naruszenia: | https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png | [Określenie wagi, prawdopodobieństwa i stopnia ryzyka naruszenia praw lub wolności osób fizycznych poprzez zniszczenie, utratę, modyfikację, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych osobowych.  Jeśli prawdopodobieństwo, by naruszenie mogło powodować ryzyko naruszenia praw lub wolności tych osób, jest większe niż małe, zachodzi obowiązek poinformowania organu nadzoru. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności tych osób, zachodzi obowiązek poinformowania podmiotów danych.] | |
| Podmiot odpowiedzialny za naruszenie: | [Wskazanie osoby, podmiotu, jednostki organizacyjnej itp.] | | |
| Podmiot odpowiedzialny za wdrożenie działań: | [Wskazanie osoby, podmiotu, jednostki organizacyjnej itp., odpowiadającej za realizację środków zaradczych i naprawczych.] | | |
| Podjęte działania: | [Opis zastosowanych lub proponowanych środków zaradczych i naprawczych.] | | |
| Rezultat działań: | [Opis planowanych i stwierdzonych skutków podjętych działań.] | | |
| Obowiązek notyfikacyjny wobec PUODO: | https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png | [Jeśli prawdopodobieństwo, by naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, jest większe niż małe, zachodzi obowiązek poinformowania organu nadzoru. Jeśli zdarzenie nie kwalifikuje się do jednego z wyjątków od tego obowiązku: data, godzina i forma zgłoszenia, z kopią w załączniku; w przypadku wystąpienia opóźnienia w powiadomieniu – wyjaśnienie przyczyn.] | |
| Obowiązek notyfikacyjny wobec podmiotów danych: | https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/Znak_A-30.svg/80px-Znak_A-30.svg.png | [Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zachodzi obowiązek poinformowania podmiotów danych. Jeśli zdarzenie nie kwalifikuje się do jednego z wyjątków od tego obowiązku: data, godzina i forma przekazania informacji, z kopią w załączniku.] | |
| Zawiadomienie organów ścigania: | [Czy zachodzi obowiązek / stwierdzono potrzebę poinformowania organów ścigania, a jeśli tak: data, godzina i forma zawiadomienia.] | | |
| Monitoring działań i wytyczne dla administratora: | [Uwagi IOD.] | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ za administratora danych osobowych Fundacja PO DRUGIE: [imię, nazwisko, funkcja]   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Inspektor Ochrony Danych dla Fundacji PO DRUGIE: [imię, nazwisko] | | | |

**Załącznik nr 10 – szablon arkusza rejestru zdarzeń prawnych z zakresu ochrony danych osobowych**

|  |  |
| --- | --- |
| Rejestr zdarzeń prawnych z zakresu ochrony danych osobowych Arkusz zdarzenia nr [•] z dn. [•] | |
| Skierowany środek: | [Określenie uprawnienia, którego realizacji żąda podmiot kierujący środek:   * wycofania udzielonej zgody; * prawa potwierdzenia przetwarzania, uzyskania dostępu, realizacji obowiązku informacyjnego i uzyskania kopii danych – art. 15 RODO; * prawa do sprostowania danych – art. 16 RODO; * prawa do usunięcia danych – art. 17 RODO; * prawa do ograniczenia przetwarzania – art. 18 RODO; * prawa do przenoszenia danych – art. 20 RODO; * prawa do sprzeciwu z przyczyn szczególnych – art. 21 ust. 1 RODO; * prawa do sprzeciwu wobec przetwarzania do celów marketingowych – art. 21 ust. 2 RODO; * prawa do niepodlegania decyzji opartej wyłącznie o zautomatyzowane przetwarzanie – art. 22 RODO;.] | |
| Data i forma zgłoszenia: | [Data i godzina wpływu zgłoszenia oraz forma, w jakiej zostało dokonane.] | |
| Podmiot kierujący środek: | [Osoba dokonująca zgłoszenia.] | |
| Sposób, forma i data realizacji: | [Sposób i data załatwienia sprawy – art. 12 RODO.] | |
| Powiadomienie odbiorców danych: | [Adnotacja dot. realizacji obowiązku informacyjnego wobec odbiorców danych w razie sprostowania lub usunięcia danych oraz ograniczenia ich przetwarzania – art. 19 RODO.] | |
| Uwagi |  | |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
za administratora danych osobowych  
Fundacja PO DRUGIE:  
[imię, nazwisko, funkcja]**