FUNDACJA im. LESŁAWA A. PAGI

POLITYKA OCHRONY DANYCH OSOBOWYCH

W
Fundacji im. Lesława A. Pagi
ul. Książęca 4, 00-498 Warszwa

Data wprowadzenia:	20.05.2018
Wersja:	2
Opracował:	Marta Płowiec, Członkini Zarządu ds. Operacyjnych
Zatwierdził:	Ewa Paga, Prezes Zarządu
Inspektor Danych Osobowych(IOD):	

SPIS TREŚCI

A. INFORMACJE OGÓLNE

1. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. TERMINOLOGIA

Administrator Danych (ADO) – Fundacja im. Lesława A. Pagi z siedzibą w Warszawie, ul. Książęca 4, 00-498 Warszawa, NIP: 701-017-05-17.

1. **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych,
2. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
3. **DPIA** – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*),
4. **Inspektor Ochrony Danych (IOD) –** osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
5. **organ nadzorczy** – niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,
6. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
7. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
8. **podmiot przetwarzający** –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych,
9. **Polityka** – niniejsza Polityka ochrony danych osobowych,
10. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej,
11. **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
12. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
13. **Unia** – Unia Europejska,
14. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.),
15.

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka ochrony danych osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Administratora Danych. Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.

B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

A.1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych,
2. Inspektor Ochrony Danych,
3. Administrator Systemów Informatycznych,
4. Osoby upoważnione do przetwarzania danych osobowych.

1.1. ADMINISTRATOR DANYCH

1. Administrator Danych wyznacza:
   - 1.1. IOD,
   - 1.2. Administratora Systemów Informatycznych.
2. Administrator Danych jest odpowiedzialny za:
   - 2.1. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
   - 2.2. wdrożenie odpowiednich procedur ochrony danych osobowych,
   - 2.3. jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora Danych ciążących na nim obowiązków,
   - 2.4. zapewnienie środków umożliwiających prawidłowa realizację praw osób, których dane dotyczą,
   - 2.5. prowadzenie rejestru czynności przetwarzania danych osobowych,
   - 2.6. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
   - 2.7. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
   - 2.8. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
   - 2.9. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
   - 2.10. dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
   - 2.11. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,
   - 2.12. nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

2.13. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,

2.14. w stosunku do IOD:

2.14.1. zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,

2.14.2. wspieranie IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,

2.14.3. zagwarantowanie by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,

2.14.4. publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

3. Administrator Danych nadzoruje działania IOD oraz ASI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.

4. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania IOD oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

5.

1.2. INSPEKTOR OCHRONY DANYCH

1. Funkcję IDO pełni osoba wyznaczona przez Administratora Danych.
2. Wzory dokumentów wyznaczenia oraz odwołania IOD znajdują się w Załączniku nr 11 do Polityki.
3. IOD jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.
4. Do zadań IOD należy:
   - 4.1. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
   - 4.2. monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
   - 4.3. monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
   - 4.4. doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem Danych a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora Danych),
   - 4.5. działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
   - 4.6. szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych,
   - 4.7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
   - 4.8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
   - 4.9. współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,
   - 4.10. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

1.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję ASI pełni osoba wyznaczona przez Administratora Danych.
2. Wzory dokumentów wyznaczenia oraz odwołania ASI znajdują się w Załączniku nr 12 do Polityki.
3. Do zadań ASI należy:
   - 3.1. prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
   - 3.2. opracowywanie oraz aktualizacja Załącznika nr 10 do Polityki, który stanowi ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych,
   - 3.3. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   - 3.4. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   - 3.5. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
   - 3.6. sprawowanie nadzoru nad kopiami zapasowymi;
   - 3.7. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
   - 3.8. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
   - 3.9. dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów.
   - 3.10. ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 2 do Polityki.
3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

A.I.1.A.I.1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:

   1.1 zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),

   1.2 w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),

   1.3 w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),

   1.4 w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),

   1.5 w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),

   1.6 przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),

   1.7 przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),

   1.8 w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).

2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1.i.1.a.i.1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.

1.i.1.a.i.2. Wykaz zbiorów danych osobowych, których administratorem jest Administrator Danych oraz procesów przetwarzania zachodzących w tych zbiorach stanowi Załącznik nr 1 do Polityki.

1.i.1.a.i.3. Administrator Danych prowadzi:

3.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,

3.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.

4. Rejestr, o którym mowa w pkt 3.1. zawiera co najmniej następujące informacje:

4.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,

4.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,

4.3. imię i nazwisko oraz dane kontaktowe IOD,

4.4. cele przetwarzania,

4.5. opis kategorii osób, których dane dotyczą,

4.6. opis kategorii danych osobowych,

4.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

4.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

4.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

4.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

5. Rejestr, o którym mowa w pkt 3.2. zawiera co najmniej następujące informacje:

5.1. nazwę oraz dane kontaktowe Administratora Danych,

5.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,

5.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,

5.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,

5.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

5.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

5.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

6. Administrator Danych prowadzi rejestry, o których mowa w pkt 3 w formie elektornicznej.
7. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

a.i.1.a.i.1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.

a.i.1.a.i.2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.

a.i.1.a.i.3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.

a.i.1.a.i.4. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi Załącznik nr 4 do Polityki.

a.i.1.a.i.5. Szczegółowa Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych stanowi Załącznik nr 3 do Polityki.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
   3.1. przedmiot powierzenia,
   3.2. czas trwania powierzenia,
   3.3. charakter i cel przetwarzania,
   3.4. rodzaj powierzanych danych osobowych,
   3.5. kategorie osób, których dane dotyczą,
   3.6. warunki podpowierzenia przetwarzania danych
   3.7. obowiązki i prawa Administratora Danych,
   3.8. obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiadają osoby wymienione przed Administratora jako osoby upoważnione do przetwarzania danych osobowych.
7. Osoby upoważnione do przetwarzania danych osobowych przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, są zobowiązane poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.
8. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.
9. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.
10. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.
11. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.

2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.

3. Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

4. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 3, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy Administrator Danych samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia Administrator Danych może zapewnić za pomocą:

   4.1. prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,

   4.2. wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,

   4.3. standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,

   4.4. standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,

   4.5. zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub

   4.6. zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

5. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w pkt 4 Administrator Danych może zapewnić w szczególności za pomocą:

   5.1. klauzul umownych między Administratorem Danych lub podmiotem przetwarzającym a Administratorem Danych, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub

   5.2. postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

6. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora Danych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 3 oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 4 i 5. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:

   6.1. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,

   6.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,

6.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,

6.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

6.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,

6.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub

6.7. przekazanie nastąpi z publicznego rejestru.

7. Podmiot upoważniony do przetwarzania danych osobowych przed planowanym przekazaniem danych do państwa trzeciego, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim warunki przekazania tych danych. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez IOD.

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
   2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,
   2.2. muszą wspólnie ustalić cele przetwarzania danych,
   2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora Danych procesów przetwarzania danych osobowych pojawią się procesy wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, podmiot upoważniony do przetwarzania danych informuje o tym fakcie IOD.
6. IOD dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
7. W przypadku, kiedy wynik oceny, o której mowa w pkt 6 wskazuje na współadministrowanie danymi osobowymi, IOD, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 4.

8. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1.i.1.a.i.1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IOD.

1.i.1.a.i.2. IOD przeprowadza audyt według opracowanego planu audytów.

2. IOD przygotowuje plan audytów na okres nie krótszy niż kwartał i nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt.

3. Plan audytów IOD przygotowuje w formie elektornicznej i przedstawia Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.

4. W planie audytów IOD uwzględnia, w szczególności:

   4.1. przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,

   4.2. procesy przetwarzania danych osobowych objęte audytem,

   4.3. konieczność weryfikacji zgodności przetwarzania danych osobowych z:

      4.3.1. zasadami przetwarzania danych osobowych,

      4.3.2. zasadami dotyczącymi zabezpieczenia danych osobowych,

      4.3.3. zasadami przekazywania danych osobowych.

5. W toku audytu IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

6. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.

7. IOD przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.

9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1.i.1.a.i.1. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:

1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),

1.2. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),

1.3. prawo do sprostowania danych (art. 16 RODO),

1.4. prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),

1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),

1.6. prawo do przenoszenia danych (art. 20 RODO),

1.7. prawo sprzeciwu (art. 21 RODO),

1.8. prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

1.i.1.a.i.2. Procedura realizacji praw osób, których dane dotyczą stanowi Załącznik nr 7 do Polityki.

10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
   2.1. stan wiedzy technicznej,
   2.2. koszt wdrażania,
   2.3. charakter, zakres, kontekst i cele przetwarzania danych,
   2.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Administrator Danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. W szczególności stosowane środki techniczne i organizacje muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6. Administrator Danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-5 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.
7. Ogólny opis organizacyjnych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 9 do Polityki.
8. Ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 10 do Polityki.

11. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (*DATA PROTECTION IMPACT ASSESSMENT*)

1.i.1.a.i.1. Administrator Danych dokonuje oceny skutków dla ochrony danych w celu opisania przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.

1.i.1.a.i.2. W strukturze Administratora Danych ocena skutków dla ochrony danych osobowych stanowi narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.

12. INCYDENTY OCHRONY DANYCH OSOBOWYCH

1.i.1.a.i.1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, jest: Administrator Danych, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).

1.i.1.a.i.2. Procedura postępowania z incydentami ochrony danych osobowych stanowi Załącznik nr 5 do Polityki.

13. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.

13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.

14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.

16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.

17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.

18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

14. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje Marta Płowiec, Członkini Zarządu ds. Operacyjnych w porozumieniu z Zarządem Fundacji i IOD.
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   3.1. procesów funkcjonujących w strukturach Administratora Danych,
   3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Inspektor Danych osobowych dokonuje aktualizacji Polityki w wymaganym zakresie.

15. ZAŁĄCZNIKI

Załącznik nr 1	Wykaz zbiorów danych osobowych wraz z procesami przetwarzania danych osobowych
Załącznik nr 2	Zasady retencji danych osobowych
Załącznik nr 3	Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych
Załącznik nr 4	Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 5	Procedura postępowania z incydentami ochrony danych osobowych
Załącznik nr 6	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 7	Procedura realizacji praw osób, których dane dotyczą
Załącznik nr 8	Ogólny opis organizacyjnych środków bezpieczeństwa
Załącznik nr 9	Wzory wyznaczenia oraz odwołania IOD.

<table>
<tr><td rowspan="2">Dokument sporządzono:

Data: 20.05.2018

Miejsce: Warszawa</td><td>Pełen podpis Administratora Danych:</td><td>Pieczęć</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td>Pełen Podpis IOD</td><td>Pieczęć</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

Załącznik nr. 1

Wykaz zbiorów danych osobowych wraz z procesami przetwarzania danych osobowych.

1. **Fundacja przetwarza następujące zakresy danych osobowych:**
   - 1.i) **Dane personalne**
   - 1.ii) **Dane kontaktowe**
   - 1.iii) **Dane dotyczące doświadczenia zawodowego**
   - 1.iv) **Dane dotyczące metryki urodzenia**
   - 1.v) **Dane dotyczące aktywności podejmowane w ramach Fundacji**
   - 1.vi) **Dane dotyczące zatrudnienia**
   - 1.vii) **Dane dotyczące osiągnięć.**
2. **Wszystkie ww. dokumenty są przechowywanie w formie elektronicznej i papierowej.**
3. **Przechowywanie i przetwarzanie danych osobowych odbywa się zgodnie z :**

3.i) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

3.ii) Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

4. Wszystkie dane są przechowywane i przetwarzane przez programy zgromadzenia danych zgodne z zasadami RODO.

5. Lokalizacja bazy danych to siedziba główna Fundacji w Warszawie oraz Biuro Rachunkowe Fundacji, z którym Fundacja ma podpisane odpowiednie umowy dot. RODO.

6. Miejscem przetwarzania danych osobowych jest siedziba Fundacji oraz miejsca przebywania pracowników upoważnionych do przetwarzania danych osobowych.

Załącznik nr.2.

Zasady retencji danych osobowych w Fundacji im. Lesława A. Pagi określają zasady postępowania dotyczące ustalania czasu przetwarzania danych osobowych zbieranych w Fundacji.

1. Procedura ma zapewnić realizację wymogów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; dalej „RODO") w odniesieniu do zasady ograniczonego przetwarzania danych osobowych, o której mowa w art. 5 ust. 1 lit. d RODO. Zgodnie z wymaganiami dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

1. Zastosowanie
Procedura retencji ma zastosowanie do wszystkich pracowników i współpracowników Fundacji, a także innych osób dopuszczonych do przetwarzania danych osobowych z organizacją.

2. Powiązania z innymi dokumentami.
Szczegółowe zasady dotyczące archiwizacji danych i ich utylizacji, w odniesieniu do rodzajów nośników, na których zostały one zapisane, określone są w dokumentach Polityka bezpieczeństwa ochrony danych w Fundacji.

3. Zasady postępowania przy ustalaniu czasu retencji danych osobowych

1.1 Zgodnie z wymaganiami RODO dla każdego rozpoznanego procesu przetwarzania danych osobowych (czynności przetwarzania) należy określać okres, przez który dane osobowe, przetwarzane

w ramach tego procesu, będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.

1.2 Kryteria ustalania okresu, o których mowa w ust. 1 mogą być określane w poniższy sposób:

a. do czasu zakończenia realizacji umowy i związanych z tym roszczeń;

b. do czasu wycofania zgody lub zgłoszenia sprzeciwu;

c. przez okres wymagany przez przepis prawa.

1.3 Dane osobowe przetwarzane przez Fundację przechowywane będą przez okres niezbędny do realizacji celu dla jakiego zostały zebrane oraz zgodnie z terminami archiwizacji określonymi przez ustawę.

1.4 Informacje dotyczące ustalonego czasu, przez który dane osobowe będą przechowywane, lub kryteria ustalania tego okresu należy zamieszczać w klauzulach informacyjnych podczas realizacji procesu zbierania danych osobowych, zarówno bezpośrednio od osoby, której dane dotyczą zgodnie z art. 13 RODO oraz w sytuacji zbierania danych z innych źródeł zgodnie z art. 14 RODO.

1.5 W przypadku zmiany celu przetwarzania danych lub zmiany kryterium ustalenia czasu retencji konieczna jest ocena celu, adekwatności i czasu przetwarzania danych w odniesieniu do nowego celu.

1.6 W przypadku zmiany celu przetwarzania w danym procesie merytoryczny pracownik Fundacji przekazuje na piśmie Inspektorowi Ochrony Danych fakt zmiany procesu przetwarzania danych wraz z informacjami o zakładanym czasie przetwarzania danych.

4. Zasady postępowania przy usuwaniu danych po ustalonym czasie retencji

1.1 Obowiązek usunięcia danych osobowych zależy od wystąpienia określonego zdarzenia (które powiązane jest z określonym celem przetwarzania danych):

a. od cofnięcia zgody przez osobę, której dane dotyczą – jeżeli podstawą prawną przetwarzania jest art. 6 ust. 1 lit. a) RODO – w przypadku przetwarzania danych w celach marketingowych na podstawie zgody;

b. od wyrażenia sprzeciwu przez osobę, której dane dotyczą – jeżeli podstawą prawną przetwarzania jest art. 6 ust. 1 lit. f) RODO – przetwarzanie danych jest niezbędne w celu realizacji uzasadnionego interesu administratora (w celu prowadzenia marketingu bezpośredniego);

c. od przedawnienia roszczeń – jeżeli dane były uprzednio przetwarzane w celu realizacji umowy;

d. od upływu terminów wynikających z przepisów prawa – w odniesieniu do danego procesu przetwarzania danych.

1.2 W sytuacji zakończenia ustalonego czasu retencji danych osobowych, w danym procesie MAI, w zależności od rodzaju nośnika, na którym dane są zapisane podejmuje działania zgodnie z przyjętymi w Urzędzie procedurami dotyczącymi usuwania danych z nośników elektronicznych lub brakowania dokumentacji papierowej.

1.3 Administrator lub Inspektor ochrony danych monitoruje realizację wymogów dotyczących usuwania lub anonimizacji danych osobowych.

1.5 Administrator lub Inspektor ochrony danych po zakończeniu ustalonego czasu retencji danych dla danego procesu przetwarzania danych usuwa wpis dotyczący tego procesu w rejestrze czynności przetwarzania danych.

5. Kategorie zbieranych danych osobowych oraz ich retencja

Przetwarzane są lub mogą być następujące dane osobowe:

1.1 Dane osobowe Uczestników programów, osób zgłaszających się w procesie rekrutacji do programów Fundacji, zewnętrznych współpracowników Fundacji, Partnerów i Sponsorów, grantodawców, Patronów medialnych. Dane te przetwarzamy w celu realizacji celów statutowych Fundacji. Dane przechowywane są przez okres nie krótszy niż 10 lat z wyatkiem jasnego wycofania zgodny na przechowywanie danych.

1.2 Rejestry korespondencji - Dane nadawców i odbiorców korespondencji przetwarzane są w celu zapewnienia właściwego obiegu i nadzoru nad korespondencją – realizując prawnie uzasadniony interes Fundacji. Dane przechowywane są przez okres nie krótszy niż 5 lat.

1.3 Dane pracowników

Podanie danych jest obowiązkiem ustawowym wynikającym z przepisów m.in. ustawy z dnia 26 czerwca 1974 r. Kodeks pracy. Dane przechowywane są przez okres przewidziany w powyższych przepisach prawa, który wynosi nie mniej niż 50 lat dla akt osobowych. Pozostałe dokumenty pracownicze przechowywane są przez okres określony w wymogach JRWA (3 lata dla danych związanych z dochodzeniem roszczeń ze stosunku pracy od dnia, w którym roszczenie stało się wymagalne; 10 lat dla danych dotyczących roszczeń stwierdzonych prawomocnym orzeczeniem organu powołanego do rozstrzygania sporów, również roszczeń stwierdzonych ugodą zawartą w trybie określonym w kodeksie przed takim organem, od dnie uprawomocnienia się orzeczenia lub zawarcia ugody; 10 lat dla danych związanych z przechowywaniem protokołów ustalenia okoliczności i przyczyn wypadku przy pracy wraz z pozostałą dokumentacją powypadkową).

1.4 Dane kandydatów do pracy. Dane osobowe kandydatów do pracy przetwarzane są w oparciu o ich zgodę oraz wypełnienie obowiązku prawnego ciężącego na Administratorze w związku z przeprowadzaną rekrutacją. Podanie danych jest dobrowolne ale niezbędne do uczestnictwa w rekrutacji. Dane przechowywane są przez trzy miesiące od zakończenia naboru lub do momentu wycofania zgody przez osobę.

1.5 Dane stażystów, praktykantów, wolontariuszy - Dane te przetwarzane są w celu realizacji stażu, praktyki, wolontariatu w oparciu o przepisy ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy, ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie oraz zapisy umowy. Dane przechowywane są przez okres nie krótszy niż 10 lat.

6. Szczególny okres przetwarzania danych osobowych

Zgodnie z zasadą minimalizacji danych i ograniczenia przechowywania zakazane jest przechowywanie danych ponad okres, w jakim jest to niezbędne do celu i jakim zostały zebrane.

Na podstawie art. 5 ust. 2 RODO Administrator jest odpowiedzialny za przestrzeganie przepisów o ochronie danych osobowych oraz musi być w stanie wykazać „rozliczalność” z realizacji wymagań stosowanych w rozporządzeniu RODO.

Załącznik nr. 3

Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych

1. Nadanie upoważnienia.
    a. W przypadku zatrudnienia nowego pracownika, który w ramach swoich obowiązków służbowych będzie przetwarzał dane osobowe, istnieje konieczność nadania mu stosownego upoważnienia do przetwarzania danych osobowych.

b. Administrator danych przed nadaniem pracownikowi upoważnienia, organizuje dla niego szkolenie.

c. Szkolenie jest przeprowadzone przez inspektora ochrony danych. Podczas szkolenia informuje się pracownika o podstawowych aspektach prawnych związanych z ochroną danych osobowych (najważniejsze definicje, odpowiedzialność prawna, obowiązek właściwego zabezpieczenia danych przetwarzanych w formie papierowej oraz w systemach informatycznych).

d. Szkolenie przeprowadzane jest w dowolnej formie (szkolenie stacjonarne, szkolenie e-learningowe, szkolenie poprzez rozesłanie materiałów drogą elektroniczną wraz z testem do rozwiązania itp.).

e. Osobie, która ukończyła szkolenie nadawane jest upoważnienie do przetwarzania danych osobowych w zgodzie z art. 29 Ogólnego rozporządzenia o ochronie danych*.

f. Upoważnienie nadawane jest przez osoby upoważnione do działania w imieniu Fundacji tj. Zarządu Fundacji i Rady Fundacji.

g. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

2. Zmiana zakresu upoważnienia

a. Zakres nadanego pracownikowi upoważnienia może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań zgodnie z poleceniami przełożonego w zakresie obowiązków oraz w świetle aktualnej umowy o pracę lub umowy cywilno- prawnej a także w zgodzie z uprawnieniami do systemów informatycznych.

b. Zmiana zakresu wydanego upoważnienia jest odnotowywana w prowadzonej ewidencji upoważnień (w odniesieniu do procesów przetwarzania danych).

3. Utrata prawa do przetwarzania danych osobowych (odwołanie upoważniania)

a. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:

a.i. zmiany stanowiska pracy na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,

a.ii. umyślnego naruszenia zasad ochrony danych osobowych określonych w przepisach prawa w tym w szczególności w Ogólnym rozporządzeniu o ochronie danych* jak również w przypadku naruszenia zasad określonych w wewnętrznych przepisach administratora

a.iii. rozwiązania stosunku pracy,

a.iv. rozwiązania umowy cywilnoprawnej.

a.v. Utrata prawa do przetwarzania danych osobowych a w konsekwencji odwołanie upoważnienia następuje poprzez jego wycofanie w ewidencji upoważnień.

Załącznik nr. 4

Ewidencja osób upoważnionych do przetwarzania danych osobowych – uaktualniono: **01.03.2021**

Imię i nazwisko	**Stanowisko**	**Zakres dopuszczenia do przetwarzania**	**Data wydania upoważnienia**	**Identyfikator dla systemu informatycznego**
Ewa Paga	CEO	Administrator-	01.01.2019	poufny

		pełny		
Marta Płowiec	COO	Administrator-pełny	01.01.2019	poufny
Tomasz Kaczmarczyk	Office Manager	IOD-pełny	01.01.2019	poufny
Aleksandra Rak	PM	pełny	01.04.2020	poufny
Paulina Paga	PM	pełny	01.12.2019	poufny
Angelika Cieśla	PM	pełny	01.12.2020	poufny
Katarzyna Strzelecka	PM	W zakresie obowiązków	01.02.2021	poufny
Artur Wywigacz	konsultant	W zakresie obowiązków	01.03.2020	poufny

Załącznik nr. 5

Procedura postępowania z incydentami ochrony danych osobowych w Fundacji im. Lesława A. Pagi.

1. Prawidłowe stosowanie procedury postępowania z naruszeniem ochrony danych osobowych wymaga znajomości obowiązującej Polityki Ochrony Danych Osobowych Fundacji, a w szczególności zawartych w niej wyrażeń takich jak np. Administrator Danych Osobowych oraz zrozumienia zasad przetwarzania danych osobowych.
2. Procedura postępowania z naruszeniem ochrony danych osobowych zawiera szczegółowe rozwiązania względem Rozdziału XV Polityki Ochrony Danych Osobowych „Naruszenia Bezpieczeństwa Danych Osobowych", stosownie do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych, dalej RODO).
3. Naruszeniem ochrony danych osobowych jest każde zdarzenie, zależne jak i niezależne od woli ludzkiej, powodujące zagrożenie bezpieczeństwa danych osobowych, w szczególności :
   - prowadzące do utraty integralności danych (np. pozostawianie dokumentów zawierających dane w miejscach powszechnie dostępnych)
   - zagrażające poufności danych (np. przesyłanie danych drogą elektroniczną bez zabezpieczenia dostępu do plików)
   - zagrażające rozliczalności danych (np. korzystanie przez kilka osób z jednego hasła dostępu)
   - zagrażające dostępności do danych (np. zgubienie nośnika pendrive, na którym znajdowały się dane osobowe, a użytkownik nośnika nie sporządził kopii zapasowej).
   2. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:
   - stwierdzono naruszenie obowiązujących przepisów wewnętrznych,
   - stwierdzono naruszenie obowiązujących przepisów prawa,
   - stwierdzono naruszenie zabezpieczeń fizycznych lub informatycznych,
   - stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
   - inne okoliczności wskazujące, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych przez jednostkę.
4. Administrator może uzyskać informacje o naruszeniu ochrony danych osobowych z różnych źródeł, w szczególności poprzez poinformowanie o tym przez osobę zatrudnioną przy przetwarzaniu danych oraz uzyskanie informacji od podmiotu przetwarzającego dane, który na mocy art. 33 ust. 2 RODO, ma obowiązek bez zbędnej zwłoki zgłosić naruszenie administratorowi.

5. Zgłoszenie podmiotu przetwarzającego odbywa się na zasadach określonych w odrębnych umowach powierzenia przetwarzania danych.
6. O każdym przypadku podejrzenia naruszenia ochrony danych osobowych należy powiadomić przełożonego oraz inspektora ochrony danych.
    a. Forma powiadomienia:
    1) Pracownik lub jego przełożony przesyła wiadomośc e-mail ze szczegółowymi informacjami dotyczącymi wydarzenia do Zarządu Fundacji lub Rady Fundacji.
    2) Powiadomienia należy dokonać niezwłocznie, jednak nie później niż w ciągu 24 godzin od stwierdzenia podejrzenia naruszenia ochrony danych osobowych.
    4. W przypadku wątpliwości pracownik powinien skonsultować się z inspektorem ochrony danych np. w kwestii poprawnego wypełnienia formularza.
    5. Każdy pracownik, który stwierdzi podejrzenie naruszenia ochrony danych jest zobowiązany w miarę możliwości podjąć czynności niezbędne do powstrzymania skutków naruszenia.
7. Ocena, czy podejrzenie naruszenia stanowi naruszenie ochrony danych osobowych.
    a. Po uzyskaniu informacji o podejrzeniu naruszenia ochrony danych, należy ocenić, czy naruszenie to stanowi naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO, a więc czy jest to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
    b. Jeżeli zgłoszone podejrzenie naruszenia nie stanowi naruszenia ochrony danych osobowych w rozumieniu w art. 4 pkt 12 RODO, wówczas na administratorze nie ciąży obowiązek zgłoszenia tego faktu organowi nadzorczemu, o czym inspektor ochrony danych niezwłocznie zawiadamia administratora.
    c. W przypadku stwierdzenia innego rodzaju naruszeń przepisów o ochronie danych (np. naruszenia zasad, obowiązków informacyjnych itp.) administrator nie ma obowiązku zawiadamiania o tym organu nadzorczego. Inspektor ochrony danych udziela odpowiednich zaleceń w zakresie obowiązków spoczywających na administratorze danych osobowych na mocy obowiązujących przepisów.
8. Ocena, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą i udokumentowanie naruszenia.
    a. W przypadku stwierdzenia, że nastąpiło naruszenie ochrony danych (incydent bezpieczeństwa pociągający za sobą skutek w postaci zniszczenia, utraty, nieuprawnionego zmodyfikowania, ujawnienia lub dostępu do danych), należy – zgodnie z art. 33 ust. 1 RODO – dokonać oceny prawdopodobieństwa, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.
    b. W przypadku, gdy:
        b.i. naruszenie nie powoduje ryzyka naruszenia praw lub wolności osób fizycznych lub jest ono mało prawdopodobne – inspektor ochrony danych dokonuje wpisu do rejestru incydentów, o czym niezwłocznie informuje administratora;
        b.ii. naruszenie ochrony danych będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych – inspektor ochrony danych dokonuje wpisu do rejestru incydentów oraz rekomenduje administratorowi zgłoszenie naruszenia Prezesowi Urzędu Ochrony Danych Osobowych w trybie i na zasadach określonych w art. 33 RODO;
        b.iii. naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw i wolności osób fizycznych – inspektor ochrony danych dokonuje wpisu do rejestru incydentów oraz rekomenduje administratorowi zgłoszenie naruszenia Prezesowi Urzędu Ochrony Danych Osobowych w trybie i na zasadach określonych w art. 33 RODO, a

także zawiadomienie osób, których dane dotyczą w trybie i na zasadach określonych w art. 34 RODO.

c. Wszelkich rekomendacji, o których mowa w pkt 2.2, inspektor ochrony danych dokonuje niezwłocznie, jednak nie później niż w terminie 36 godzin od uzyskania informacji o podejrzeniu naruszenia ochrony danych.

d. Zawiadomienia osób, o którym mowa w pkt 2.2.3 dokonuje inspektor ochrony danych na polecenia administratora.

e. Wpis do rejestru incydentów, zgodnie z art. 33 ust. 5 RODO zawiera m.in. okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

9. Zgłoszenie naruszenia ochrony danych organowi nadzorczemu.

a. Zgodnie z art. 33 ust. 3 RODO, administrator zgłasza zaistniałe naruszenie organowi nadzorczemu bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

b. Dopuszczalne jest późniejsze zawiadomienie, po upływie 72-godzinnego terminu, zwłaszcza w przypadku, gdy naruszenie ma poważny charakter i administrator koncentruje się w pierwszej kolejności na ograniczeniu skutków naruszenia, a następnie stara się spełnić pozostałe obowiązki, jednak wówczas należy wyjaśnić przyczyny opóźnienia.

c. W przypadku, gdy zgłoszenie wszystkich wymaganych informacji nie jest możliwe z zachowaniem terminu wskazanego w pkt 3.1, administrator dokonuje zgłoszenia częściowego, tj. przekazuje informacje, które są znane administratorowi w chwili dokonania zgłoszenia przed upływem 72 godzin, a następnie sukcesywnego uzupełniania zgłoszenia, zgodnie z art. 33 ust. 4 RODO.

Załącznik 6.
Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE

do przetwarzania danych osobowych

.....,

miejscowość, data

Na podstawie:

3. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
4. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

5. **Upoważniam**

6. **Pana/Panią ……**
7. **Dział: .....**
8. do przetwarzania danych osobowych w formie elektronicznej lub papierowej, w ramach pełnionych obowiązków służbowych, wynikających z:
    9. *umowy o pracę / umowy cywilnoprawnej (np. umowy zlecenia, o dzieło) / umowy praktyki / stażu**
    oraz obowiązków zleconych jednorazowo lub na stałe przez przełożonego.
10. Upoważnienie do przetwarzania danych osobowych w systemach informatycznych jest określane poprzez indywidualnie przyznawane prawa dostępu do każdego systemu.
11. Dla potrzeb wykonywanej pracy, w tym czynności zlecanych przez przełożonego, upoważniam Panią/Pana do tworzenia rejestrów w plikach programów biurowych (np. MS Word, MS Excel, MS Access) oraz podręcznych archiwach papierowych, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych, wdrożonych w Fundacji im. Lesława A. Pagi.

.....

podpis przedstawiciela Zarządu

Odebrałem w dniu: .....
.....
podpis osoby upoważnionej

Załącznik nr. 7

Procedura realizacji praw osób, których dotyczy przetwarzanie danych osobowych

Skąd mamy Państwa dane?

Państwa dane pozyskaliśmy:

1. bezpośrednio od Państwa,
2. z bazy mailingowej, do której się Państwo dopisaliście poprzez nasza stronę internetową;
3. od partnera / podmiotu trzeciego współpracującego z Fundacją, który udostępnił Państwa dane osobowe na podstawie Państwa zgody,
4. ze źródeł publicznie dostępnych, np. z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej czy innych podobnych źródeł.

Kto jest administratorem Państwa danych?

Fundacja im. Lesława A. Pagi z siedzibą w Warszawie (02-202) przy ul. Drawskiej 7, wpisaną do Krajowego Rejestru Sądowego w Sądzie Rejonowym dla m. st. Warszawy XII Wydział Gospodarczy, pod nr KRS 0000324112, NIP 701-017-05-17tel 786 175604, e-mail: sekretariat@paga.org.pl.

Jakie dane przetwarzamy?

Fundacja przetwarza następujące kategorie danych:

1. dane kontaktowe;
2. dane wymagane do identyfikacji na potrzeby zawarcia umowy, wykonania usługi i wystawienia faktury;
3. dane identyfikacyjne niezbędne do informowania o działalności statutowej Fundacji;
4. dana osobowe niezbędne do poinformowania o uczestnikach naszych projektów, prowadzących zajęcia w naszych projektach i informowania o naszej działalności;

Do czego będziemy używać Państwa danych osobowych?

Państwa dane osobowe będziemy przetwarzać w jednym lub więcej spośród następujących celów:

1. w celu realizacji działań statutowych Fundacji;
2. w celu zawarcia i wykonania umowy, którą zawarli Państwo z Fundacją,
3. w celu wykonania umowy zawartej z Fundacją na Państwa rzecz jako osoby trzeciej (art. 393 Kodeksu cywilnego), gdy stroną umowy jest inny podmiot,
4. w celu wypełnienia obowiązku prawnego ciążącego na Fundacji, np. wystawienia faktury lub rachunku,
5. w celach marketingowo-informacyjnych o naszych wydarzeniach i projektach edukacyjnych;,

Czy mają Państwo obowiązek podać dane osobowe?

W zakresie, w jakim przetwarzanie Państwa danych następuje w celu wykonania umowy z Fundacją, podanie przez Państwa danych jest warunkiem zawarcia tej umowy. Podanie danych ma charakter dobrowolny, lecz jest niezbędne do zawarcia i wykonania umowy. W przypadku niepodania danych osobowych umowa nie będzie zawarta. Podanie danych niezbędnych do wystawienia faktury jest obowiązkiem ustawowym i wynika z Ustawy o podatku od towarów i usług. W pozostałym zakresie podanie danych osobowych jest dobrowolne, nie jest wymogiem ustawowym lub umownym oraz nie stanowi warunku zawarcia umowy.

Jak cofnąć zgodę?

Można wyrazić zarówno wszystkie zgody lub niektóre z nich, jak i nie wyrazić

żadnej.

W każdej chwili mogą Państwo cofnąć każdą zgodę udzieloną Fundacji w związku z przetwarzaniem danych osobowych bez ponoszenia negatywnych konsekwencji. Wystarczy wysłać e-mail, zadzwonić lub przesłać wiadomość pocztą tradycyjną na wskazane powyżej dane kontaktowe. Wolę cofnięcia zgody można wyrazić w dowolny sposób, jedynym warunkiem jest, aby dotarła ona do naszej wiadomości. Cofnięcie zgody nie wpływa na zgodność z prawem przetwarzania Państwa danych przed jego dokonaniem, tzn. do momentu cofnięcia zgody przetwarzanie Państwa danych przez Fundację jest legalne.

Jak skontaktować się z naszym inspektorem ochrony danych osobowych? Można to zrobić telefonicznie pod numerem telefonu: 786 175604 lub e-mailowo pod adresem sekretariat@paga.org.pl

Na jakiej podstawie będziemy przetwarzać Państwa dane osobowe? Podstawą przetwarzania danych osobowych jest, w zależności od wykonywanych czynności:

1. zawarcie i wykonanie umowy z Fundacją,
2. wypełnienie obowiązku prawnego ciążącego na Fundacji (np. wystawienie faktury),
3. prawnie uzasadniony interes Fundacji informowanie o swoich projektach i wydarzeniach Fundacji lub wykonanie umowy zawartej z Fundacją na Państwa rzecz jako osoby trzeciej, gdy stroną umowy jest inny podmiot),
4. wyrażona przez Państwa zgoda.

Kiedy i komu możemy przekazać dane, a komu na pewno ich nie przekażemy? Państwa dane możemy ujawnić odbiorcom, w postaci firm z nami współpracujących i wykonujących zadania na nasze zlecenie i naszą rzecz. W takim przypadku zawarta jest z tymi podmiotami umowa zapewniająca bezpieczeństwo Państwa danych. Z uwagi na to, iż podmioty te często się zmieniają, nie jesteśmy w stanie przedstawić ich kompletnej listy, jeśli chcą Państwo wiedzieć z kim współpracujemy aktualnie, zawsze można o to zapytać. Nie będziemy natomiast przekazywać Państwa danych osobowych do państwa trzeciego (poza Europejski Obszar Gospodarczy).

Co mogą Państwo robić z przekazanymi nam danymi osobowymi? Mają Państwo prawo do żądania od Fundacji dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także możemy je na Państwa żądanie przenieść do innego administratora danych. Odnośnie do przetwarzania Państwa danych w celu marketingu własnych produktów lub usług Fundacji mogą Państwo wnieść sprzeciw.

Do kiedy będziemy przechowywać Państwa dane?

Państwa dane osobowe będą przechowywane tak długo, jak jest to niezbędne do wykonania umowy łączącej Państwa z Fundacją lub umowy zawartej przez inny podmiot na Państwa rzecz, a po tym czasie przez okres czasu odpowiadający okresowi przedawnienia roszczeń, jakie może podnosić Fundacja i jakie mogą być podnoszone wobec Fundacji.

Jeśli Państwa dane osobowe będą przetwarzane w celu wypełnienia obowiązku prawnego ciążącego na administratorze, dane osobowe będą przechowywane przez czas niezbędny do wypełnienia tego obowiązku.

Dane przetwarzane na podstawie zgody będziemy przetwarzać do czasu wycofania przez Państwa tej zgody.

Jeśli Państwa dane osobowe będą przetwarzane na podstawie prawnie uzasadnionego interesu administratora, gdy podstawą tego przetwarzania jest wykonanie umowy zawartej z Fundacją na Państwa rzecz, dane będą przetwarzane do czasu wypełnienia prawnie uzasadnionego interesu stanowiącego podstawę tego przetwarzania.

Jeśli Państwa dane osobowe będą przetwarzane na podstawie prawnie uzasadnionego interesu administratora, gdy podstawą tego przetwarzania jest marketing bezpośredni swoich produktów i usług, Państwa dane osobowe będą przetwarzane do czasu wniesienia przez Państwa sprzeciwu.

Gdzie mogą Państwo wnieść skargę na przetwarzanie danych osobowych przez Fundację?

Obecnie takie skargi kierować można do Generalnego Inspektora Ochrony Danych Osobowych. Chcielibyśmy jednak zaznaczyć, że wkrótce właściwym organem nadzorczym w tej kwestii może być Prezes Urzędu Ochrony Danych Osobowych.

Jak nie będziemy przetwarzać danych osobowych?

Państwa dane osobowe nie podlegają zautomatyzowanemu przetwarzaniu (np. profilowaniu), które wywołuje wobec Państwa skutki prawne lub w podobny sposób istotnie na Państwa wpływa, niemniej jednak korzystamy z plików cookies oraz innych systemów rejestrujących ruch na naszych stronach internetowych (profilowanie w celach marketingowych).

Załącznik nr. 8

Ogólny opis organizacyjnych środków bezpieczeństwa:

1. Fundacja prowadzi politykę bezpieczeństwa związaną z posiadanymi danymi osobowymi zgodną z RODO.
2. Administratorem ogólnych zasad bezpieczeństwa jest Członek Zarządu ds. Operacyjnych działający w ścisłym porozumieniu z Inspektorem Danych Osobowych (IOD).
3. Fundacja zabezpiecza dane posiadanych przez siebie osób za pomocą systemu informatycznego dostępnego dla organizacji pozarządowej.
4. Dostęp do systemu informatycznego przysługuje tylko pracownikom i współpracownikom Fundacji posiadającym aktualną umowę o pracy/umowę zlecenie/ umowę o współpracy zgodną z obecnymi przepisami prawa pracy i prawa cywilnego.
5. Administrator w porozumieniu z IOD prowadzi bieżącą politykę nadzoru dostępu do poufnych informacji, jakimi są dane osobowe.
6. Posiadane dane osobowe są zabezpieczone hasło zgodnie z ogólnie przyjętymi normami bezpieczeństwa.
7. Posiadane dane osobowe mają charakter elektroniczny i papierowy.
8. Dane papierowe są przechowywane w archiwum siedziby Fundacji przy. Ul. Drawskiej 7, 02-202 Warszawa oraz w biurze Rachunkowym, które posiada odpowiednie uprawnienia do przechowywania danych wrażliwych i z którym Fundacja ma podpisaną umowę o powierzeniu danych osobowych na zasadach zgodnych z RODO, biuro z siedzibą ul. Gersona 9, 03-307 Warszawa.
9. Pomieszczenia, w których przetwarzane są dane wyposażone są w system alarmowy przeciwwłamaniowy.
10. Dane elektroniczne są przechowywane na podwójnie chronionym dysku wirtualnym Fundacji, do którego dostęp jest ograniczony.
11. Dane w postaci elektronicznej są zahasłowane, a hasła zmieniane co 3 do 6 miesięcy.
12. Osoby posiadające dostęp do danych elektronicznych posiadają odpowiednie zabezpieczenia antywłamaniowe na urządzenia elektroniczne.
13. W przypadku zgłoszenia nieprawidłowości w dostępie do danych osobowych Administrator i IOD niezwłocznie podejmują środki zabezpieczające polegające na utworzeniu kopii zapasowej bazy danych oraz ponownego zabezpieczenia hasłowanego posiadanej bazy danych osobowych.
14. Każda osoba posiadająca dostęp do danych osobowych podpisuje odpowiednie oświadczenie o zachowaniu poufności danych, do których ma dostęp.
15. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
16. Nadzór nad posiadaną bazą danych posiada również osoba zatrudniania w związku z wykonywaniem usług informatycznych na rzecz Fundacji.

17. Wszystkie nieprawidłowości w dostępie i obsłudze systemu przechowywania danych osobowych są niezwłocznie zgłaszane do Administratora i/lub IOD.

Załącznik 9.

Wzory wyznaczenia oraz odwołania Inspektora Ochrony Danych

Zawiadomienie o odwołaniu dotychczasowego inspektora ochrony danych i wyznaczeniu nowego (przetwarzanie danych w związku z zapobieganiem i zwalczaniem przestępczości)

Część A: Oznaczenie administratora danych			
Pełna nazwa administratora	Kliknij tutaj, aby wprowadzić tekst.		
REGON (jeśli został nadany) (opcjonalnie)	Kliknij tutaj, aby wprowadzić tekst.		
Adres:			
Państwo	Kliknij tutaj, aby wprowadzić tekst.	Miejscowość	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Ulica	Kliknij tutaj, aby wprowadzić tekst.
Powiat	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer / Numer lokalu: Podaj numer
Osoba/osoby uprawnione do reprezentowania administratora			
1.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst.	Stanowisko: Kliknij tutaj, aby wprowadzić tekst.	
2.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	
3.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	
4.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	
5.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	Stanowisko: Kliknij tutaj, aby wprowadzić tekst. (opcjonalnie)	

Część B: Dane dotychczasowego inspektora ochrony danych	
Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.

Część C: Dane kontaktowe inspektora ochrony danych			
Imię	Kliknij tutaj, aby wprowadzić tekst.	Nazwisko	Kliknij tutaj, aby wprowadzić tekst.
Telefon	Kliknij tutaj, aby wprowadzić tekst.	Adres e-mail	Kliknij tutaj, aby wprowadzić tekst.
Powyżej musi zostać podany telefon lub adres e-mail (oba pola nie mogą pozostać puste – zgodnie z brzmieniem art. 10 ust. 1 ustawy o ochronie danych osobowych)			