POLITYKA OCHRONY DANYCH OSOBOWYCH

FUNDACJA EKOROZWOJU
EKOCENTRUM WROCŁAW
UL. ŚW. WINCENTEGO 25A,C, 50-252 WROCŁAW
KRS: 0000178876

1. Wstęp

1.1. INFORMACJE OGÓLNE

1. Regulamin niniejszy określa tryb i zasady ochrony danych osobowych przetwarzanych przez Fundację

2. Dokument Polityki Ochrony Danych Osobowych został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:
a) 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) , zwanym dalej „Rozporządzeniem"
b) Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (zwaną dalej Ustawą)

3. „Polityka bezpieczeństwa" obowiązuje wszystkie osoby pracujące przy przetwarzaniu danych osobowych w Fundacji Ekorozwoju, niezależnie podstawy zatrudnienia, a także podmioty którym powierzono przetwarzanie danych na podstawie odrębnych porozumień.
4. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia ochrony danych osobowych przetwarzanych przez Fundacja.
5. Fundacja prowadzi rejestr czynności przetwarzania danych osobowych, stanowiący załącznik 6 do niniejszego dokumentu

1.2. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Ilekroć w niniejszym dokumencie jest mowa o :
a) **Fundacji** – rozumie się przez to **Fundację Ekorozwoju**
b) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
c) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
d) **przetwarzaniu danych** rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
e) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
f) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
g) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
h) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
i) **administratorze danych osobowych** - w świetle art. 4 pkt 7) Rozporządzenia, rozumie się przez to Fundację, jako podmiot decydujący o celach i środkach przetwarzania danych osobowych;

j) **administratorze systemu informatycznego (ASI)** - rozumie się przez to osobę zatrudnioną przez Fundację, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
k) **użytkowniku systemu informatycznego** - rozumie się przez to upoważnionego przez Fundację, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;
l) **projekcie** - zestaw działań realizowanych przez Fundację zgodnie z jej celami statutowymi
m) **powierzeniu przetwarzania danych osobowych** - rozumie się przez to przekazanie odrębnemu od Fundacji organizacyjnie i funkcjonalnie podmiotowi danych osobowych przetwarzanych przez Fundację, na podstawie zawartej umowy o powierzeniu przetwarzania danych osobowych, dla przetwarzania przez ten podmiot przekazanych danych w celach i w sposób określony w umowie przez Fundację. Podmiot któremu powierzono przetwarzanie danych osobowych nie decyduje autonomicznie o celach i warunkach przetwarzania danych osobowych, będąc związanym w tym zakresie wytycznymi określonymi przez Fundację.
n) **serwerze** - rozumie się serwer plików, bezpiecznie przechowujący dane lub udostępniający je wybranym użytkownikom. Współpracuje z urządzeniami podłączonymi do internetu i pozwala na zdalny dostęp do plików;
o) **uczestniku projektu** - rozumie się osoby trzecie uczestniczące w Projektach i innych wydarzeniach organizowanych lub prowadzonych przez Fundację.
p) **współpracowniku Fundacji** – rozumie się przez to osoby wykonujące na rzecz Fundacji zlecone zadania na podstawie innej niż umowa o pracę, w szczególności w ramach umów cywilnoprawnych, w tym wykonywanych w ramach własnej działalności gospodarczej oraz wolontariatu.

1.3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Fundacji Ekorozwoju,

Siedziba Fundacji znajduje się przy ul. Św. Wincentego 25A,C we Wrocławiu. W budynku znajduje się stanowisko przy wejściu, umożliwiające kontrolę osób wchodzących do budynku. Na zewnątrz budynku znajduje się niewielkie podwórko odgrodzone płotem od ulicy. Dane osobowe w Fundacji przetwarzane są w samym budynku. Pomieszczenia, w których przetwarzane są dane osobowe, wyposażone są w drewniane szafy oraz szafki z szufladami do przechowywania dokumentacji, które są zamykane na klucz. Do poszczególnych pomieszczeń, w których są przetwarzane dane, mają dostęp jedynie pracownicy i współpracownicy Fundacji, których praca związana jest bezpośrednio z przetwarzaniem tych danych. Dostęp do danych w formie papierowej mają jedynie w dni robocze od godziny 08:00 do 17:00. Dostęp do kluczy do budynku posiadają wyłącznie pracownicy i współpracownicy Fundacji. Fundacja prowadzi listę osób posiadających klucze do budynku. Ponadto, pracownicy, współpracownicy i wolontariusze fundacji, w zakresie niezbędnym do wykonywania ich funkcji i zadań, upoważnieni są do przetwarzania danych na komputerach przenośnych, pod warunkiem ich należytego zabezpieczenia. Dane osobowe przetwarzane przez Fundację są przechowywane na serwerach zewnętrznych znajdujących się na terenie Unii Europejskiej, jednakże w pozostałym zakresie są przetwarzane w sposób opisany powyżej.

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych:
2. 1. W Fundacja przetwarza się następujące dane osobowe:
a) dane pracowników i współpracowników,

b) dane wolontariuszy,
c) dane uczestników projektów,
d) dane kandydatów do pracy,
e) dane osób otrzymujących Newslettery,
f) dane darczyńców,

2.2 Dane w powyższych zbiorach mają formę papierową i/lub elektroniczną, i są przetwarzane są w organizacji w formie papierowej i elektronicznej oraz są przetwarzane w zasobach systemu informatycznego w programach typu MS Excel, MS Word, MS Outlook, MS Access lub równoważnych, a także w ramach systemu informatycznego użytkownika Google.pl, w tym Google Drive, oraz przechowywane są na serwerze.

2.3 Dane osobowe pracowników oraz osób współpracujących z Fundacja przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:
a) imiona i nazwiska,
b) adres zamieszkania (kraj, miejscowość wraz z kodem pocztowym, ulica, numer domu, numer mieszkania),
c) serię i numer dowodu osobistego, numer ewidencyjny PESEL i/lub NIP,
d) data i miejsce urodzenia,
e) numer konta bankowego,
f) dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej),
g) wykształcenie i historia zatrudnienia.

2.4. Dane osobowe wolontariuszy przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:
a) imiona i nazwiska,
b) adres zamieszkania (kraj, miejscowość wraz z kodem pocztowym, ulica, numer domu, numer mieszkania),
c) dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej).
d) dane paszportowe, w przypadku cudzoziemców
e) inne niezbędne dane wynikające z wymogów donatora, zgodnie z wymaganiami realizowanych działań

2.5. Dane osobowe uczestników projektów przetwarzane są w formie papierowej oraz elektronicznej i mogą obejmować następujący zakres:
a) imiona i nazwiska,
b) dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej),
c) adres zamieszkania

2.6. Dane osobowe kandydatów do pracy przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:
a) imiona i nazwiska,
b) adres zamieszkania (miejscowość wraz z kodem pocztowym, ulica, numer domu, numer mieszkania),
d) data i miejsce urodzenia,
e) dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej),
f) wykształcenie i historia zatrudnienia.

2.7. Dane osób otrzymujących Newsletter przetwarzane są w formie papierowej oraz elektronicznej i mogą obejmować następujący zakres:
a) imiona i nazwiska,
b) adres poczty elektronicznej,

c) kod pocztowy

2.8. Dane osobowe darczyńców są w formie papierowej oraz elektronicznej i mogą obejmować następujący zakres:
a) imiona i nazwiska,
b) adres zamieszkania ,jeżeli darczyńca chce pozostawić takie informacje,
c) NIP jeżeli darowizna została dokonana w formie 1% podatku dochodowego,
d) numer konta bankowego, jeżeli darowizna została dokonana przelewem,
e) dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej), jeżeli darczyńca chce pozostawić takie informacje

2.9. Do zasobów systemu informatycznego służącego do przetwarzania danych osobowych zalicza się:
a) domeny internetowe zapewniające funkcjonalności w formie poczty e-mail, stron internetowych oraz usług umożliwiających korzystanie z dysków zewnętrznych,
b) program do obsługi rachunkowej i kadrowej, gdzie przetwarzane są dane pracowników i współpracowników fundacji, darczyńców i wolontariuszy
c) serwer, w którym przechowywane są zbiory danych osobowych określone w pkt: 2.3-2.8.
d) programy typu MS Excel, MS Word oraz MS Outlook, MS Access i programy równoważne, a także programy wchodzące w system informatyczny użytkownika Google.pl, w tym Google Drive w których przetwarzane są zbiory danych osobowych określone w pkt: 2.3-2.8.

3. Opis struktury zbiorów danych przetwarzanych elektronicznie wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi:
3.1 Domeny internetowe poprzez zapewnienie poczty e-mail oraz usług dysków zewnętrznych w formie tzw. „chmury" pozwalają na przetwarzanie danych określonych w pkt: 2.3-2.8 w szczególności poprzez przesyłanie ich i wzajemne udostępnianie pomiędzy pracownikami i współpracownikami. Dostęp do tych funkcjonalności wymaga wskazania konta użytkownika i przypisanego do niego hasła, co wyklucza dostęp osób trzecich.

3.2 Programy rachunkowo-kadrowe, gdzie przetwarzane są w formie elektronicznej dane osobowe obejmujące pkt. 2.3-2.8, dostępny wyłącznie dla pracowników i współpracowników prowadzących bieżącą obsługę rachunkowo - kadrową.

3.3 Serwer, gdzie przechowywane są i archiwizowane dane osobowe określone w pkt: 2.3-2.8., do którego dostęp posiadają jedynie pracownicy oraz współpracownicy, z komputerów podłączonych do sieci informatycznej Fundacji.

3.4 Przenośne, prywatne komputery i inne urządzenia elektroniczne upoważnionych pracowników, współpracowników i wolontariuszy Fundacji, pod warunkiem ich odpowiedniego zabezpieczenia.

3.5 W programach MS Excel, Word, oraz Outlook przetwarzane są w formie elektronicznej dane osobowe określone w pkt: 2.3-2.8 przechowywane na serwerze oraz poszczególnych komputerach. Przetwarzanie polega na systematyzacji oraz wykorzystaniu już posiadanych danych osobowych.

4. Sposób przepływu danych pomiędzy systemami:
4.1 Fundacja nie posiada własnego systemu informatycznego służącego do przetwarzania danych osobowych. Dane osobowe przetwarzane są przy użyciu edytora tekstu (MS Word), arkusza kalkulacyjnego (MS Excel) lub programu pocztowego MS Outlook oraz programów równorzędnych (np. pakiet Open Office) lub programy wchodzące w system informatyczny użytkownika Google.pl, w tym Google Drive.

4.2. Wszystkie wyżej wymienione systemy informatyczne są systemami odrębnymi i nie współpracują ze sobą, choć możliwe jest przesyłanie pomiędzy nimi poszczególnych kategorii danych osobowych.

4.4 Podmioty, do których przekazywane są dane to:
a) Zakład Ubezpieczeń Społecznych,
b) Urzędy Skarbowe
c) Biuro Rachunkowe, które prowadzi sprawy rachunkowo - kadrowe Fundacji,
d) Podmioty finansujące, współfinansujące lub współorganizujące wraz z Fundacją Projekty, którym Fundacja zobowiązana jest udostępnić dane Pracowników, Współpracowników, Wolontariuszy lub Uczestników Projektów, w celu prowadzenia, rozliczenia i sprawozdania z przeprowadzonych działań,
e) Edukatorzy prowadzący zajęcia z uczestnikami projektów lub innymi osobami trzecimi.

4.5 Przelewy bankowe i międzybankowe są realizowane za pośrednictwem internetu.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych

5.1. Środki organizacyjne:

5.1.1 Do zastosowanych przez Administratora Danych i osoby przez niego upoważnione w Fundacji. środków organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy:

a) opracowanie i wdrożenie „Polityki ochrony danych osobowych”
b) opracowanie i wdrożenie „Instrukcji Zarządzania Systemem Informatycznym służącej do przetwarzania danych osobowych w Fundacji,
c) nadanie przez Administratora członkom organów organizacji, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom organizacji upoważnień do przetwarzania danych osobowych,
d) nadawanie przez Administratora pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w związku z realizacją projektów/zadań, w których Fundacja będzie partnerem [niezależnie od tego, czy lider projektu/zadania (realizator) udzieli takiego upoważnienia, czy też nie],
e) nadawanie przez Administratora pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w pozostałych przypadkach przetwarzania danych osobowych występujących w organizacji,
f) wyznaczenie Administratora Systemu Informatycznego (ASI) ,
g) Zobowiązanie pracowników i współpracowników do zachowania poufności w zakresie przetwarzania danych, a także zapoznanie ich z Polityką Ochrony Danych Osobowych i Instrukcją Obsługi Systemu Informatycznego
h) sprawowanie przez Administratora oraz ASI kontroli i nadzoru nad procesem wprowadzania danych osobowych do zbioru oraz ich udostępniania.

5.1.2. Osobami upoważnionymi do przetwarzania danych osobowych w Fundacji są:
a) Administrator Danych, w osobie przedstawicieli organów Fundacji,
b) Administrator Systemów Informatycznych,
c) Pracownicy i współpracownicy Fundacji,
d) osoby prowadzące obsługę księgowo-kadrową Fundacji,

5.1.3 Katalog osób upoważnionych do przetwarzania danych osobowych w organizacji nie ma charakteru zamkniętego i może zostać poszerzony o nowe stanowiska w razie wystąpienia uzasadnionej konieczności.

5.1.4 Dla potrzeb ochrony danych osobowych przetwarzanych w organizacji w formie papierowej stosuje się zabezpieczenia polegające na przechowywaniu:
a) dokumentacji bieżącej w szafach w obszarze przetwarzania danych osobowych,
b) dokumentacji archiwalnej i dokumentacji pracowniczej w szafach w obszarze przetwarzania danych osobowych

5.2. Środki techniczne:

5.2.1 Dostęp do danych osobowych przetwarzanych w systemach informatycznych chroniony jest poprzez:

a) zastosowanie loginów i haseł uniemożliwiających nieuprawnione korzystanie osobom nieupoważnionym,
b) ustawienie monitorów komputerów w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
c) Lista loginów i haseł jest wyłącznie w Posiadaniu ASI, który podejmuje odpowiednie środki w celu zapewnienia jej poufności
d) w razie wystąpienia konieczności uzyskania dostępu do któregoś z komputerów w czasie nieobecności pracownika użytkującego komputer, Administrator może zwrócić się do ASI w celu uzyskania hasła do danego komputera po to aby umożliwić wykonanie niezbędnych czynności innemu pracownikowi. Po powrocie pracownika użytkującego dany komputer zmianie ulega hasło dostępu.

5.2.3 W Fundacji dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (MS Word), arkuszach kalkulacyjnych (MS Excel), programie Outlook lub programach równorzędnych (np. pakiet Open Office) i innych programach do tworzenia baz danych oraz w systemach informatycznych do ochrony systemu informatycznego stosuje się systemy antywirusowe oraz firewall. Wszystkie dane przetworzone za pomocą tych programów przechowywane są na serwerze lub dyskach twardych komputerów fundacji.

5.2.4. Elektroniczne przetwarzanie danych osobowych odbywa się na komputerach stacjonarnych i laptopach. Dla zminimalizowania ryzyka dostania się ich zawartości w niepowołane komputery zabezpieczone są hasłami, a kadra Fundacji została zapoznana z „Polityką Ochrony Danych Osobowych" i przeszkolona w zakresie ochrony danych osobowych

6. Pozostałe informacje

6.1. W Fundacja nie przetwarza się poza uzasadnionymi przepisami prawa przypadkami przetwarzania danych o stanie zdrowia ani danych wrażliwych (sensytywnych), do których należy przetwarzanie danych o stanie zdrowia:

a) pracowników Fundacji – przetwarzanie danych wynika z odrębnych przepisów prawa i dotyczy obowiązku przeprowadzenia badań lekarskich wstępnych (przed zawarciem umowy o pracę) oraz badań lekarskich okresowych (wykonywanych w trakcie trwania zatrudnienia) i badań lekarskich pochorobowych (wykonywanych w trakcie trwania zatrudnienia, przed powrotem do pracy po nieobecności spowodowanej długotrwałym zwolnieniem lekarskim),
b) pracowników i współpracowników Fundacji – przetwarzanie danych o stanie zdrowia w tym przypadku wynika z konieczności udokumentowania faktu bycia osobą niepełnosprawną poprzez przedstawienie orzeczenia o stopniu niepełnosprawności.

6.2. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych przetwarzanych przez organizację, a zwłaszcza prawo do:

a) uzyskania wyczerpującej informacji, czy taki zbiór istnieje oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy;
b) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
c) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania w powszechnie zrozumiałej formie treści tych danych;
d) uzyskania informacji o źródle danych, z którego pochodzą dane jej dotyczące, chyba że Administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej;
e) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
f) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Rozporządzenia albo są już zbędne do realizacji celu, dla którego zostały zebrane.
g) żądania realizacji praw określonych w art. 17 Rozporządzenia, poprzez usunięcie danych w przypadku gdy:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwowym
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

6.3 Administrator może odmówić usunięcia danych, w przypadku gdy są one niezbędne do ustalenia, obrony lub dochodzenia roszczeń. W takich przypadkach dane są archiwizowane i przetwarzane wyłącznie na te potrzeby.
6.4. Dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. ADMINISTRATOR DANYCH

1. Administratorem Danych jest Fundacja Ekorozwoju ul. Św. Wincentego 25a,c, 50-252 Wrocław KRS: 0000178876

2. Do uprawnień i obowiązków Administratora należą m. in.:

a) stały nadzór nad treścią Polityki Ochrony Danych Osobowych i Instrukcji zarządzania systemem informatycznym,
b) aktualizacja i modyfikacja dokumentów obejmujących dane osobowe,
c) czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania,
d) prowadzenie jawnego rejestru zbiorów danych osobowych,
e) udział w kontrolach prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych,
f) udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,
g) nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych osobowych w trybie określonym w Rozdziale 3 niniejszego dokumentu,
h) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
i) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych, nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,

2.2. INSPEKTOR OCHRONY DANYCH

1. Inspektor Ochrony Danych może zostać wyznaczony przez Administratora Danych (wzór: Załącznik nr 1). Wykonuje on wtedy kompetencje Administratora Danych, chyba że przepisy prawa wymagają udziału Administratora.

2. Do uprawnień i obowiązków Inspektora Ochrony Danych, jeżeli zostanie wyznaczony, należą m. in.:
a) stały nadzór nad treścią Polityki Ochrony Danych Osobowych i Instrukcji zarządzania systemem informatycznym,
b) aktualizacja i modyfikacja ww. dokumentów,
c) czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania,
d) prowadzenie jawnego rejestru zbiorów danych osobowych,
e) udział w kontrolach prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych,
f) udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,
g) nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych osobowych w trybie określonym w Rozdziale 3 niniejszego dokumentu,
h) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
i) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,
j) nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,
k) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.
3. W przypadku wyznaczenia Inspektora Ochrony Danych, Administrator zapewnia, aby dane kontaktowe Inspektora były każdorazowo ujawniane w formularzach zgód, formularzach informacyjnych, a także informacjach przesyłanych do osób których dane są przetwarzane.

2.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Administrator Systemów Informatycznych wskazany jest przez Administratora Danych (wzór: załącznik nr 3 do Polityki Ochrony Danych Osobowych).

2. Do uprawnień i obowiązków Administratora Systemów Informatycznych należą w szczególności:
a) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
b) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
c) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
d) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.

2.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Ochrony Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu podstawy umownej wykonywanych obowiązków.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Użytkowników systemu informatycznego tworzy oraz usuwa Administrator Systemu Informatycznego, na polecenie Administratora Danych.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych,
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
    a. zawieszenia w pełnieniu obowiązków pracowniczych,
    b. poważnego naruszenia obowiązków pracowniczych, w szczególności w zakresie ochrony danych osobowych
    c. w przypadku współpracowników, naruszenia zawartej umowy lub ustania jej obowiązywania lub zawieszenia jej wykonywania.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku zobowiązaniowego stanowiącego podstawę świadczenia pracy lub innych usług.

6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy lub innej umowy którą były związane. W tym celu Administrator wprowadzi odpowiednie zapisy w umowach.

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Rozporządzenie przewiduje możliwość powierzenia przetwarzania danych osobowych przez Administratora Danych zewnętrznym podmiotom. W Fundacji odbywa się to na drodze umowy powierzenia, precyzujące zakres przekazanych danych, czynności wykonywane z tymi danymi, okres ich przetwarzania, cel ich przetwarzania, która zawiera również co najmniej następujące postanowienia, co do podmiotu przetwarzającego:

a) przetwarza on dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) podejmuje wszelkie środki w celu zabezpieczenia przetwarzanych danych zarówno w zakresie środków ochrony informatycznej jak i fizycznej,

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, przy zachowaniu wymogów Rozporządzenia

e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków podczas kontroli i zobowiązań nałożonych przez organy nadzorcze lub innych administratorów danych;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

5. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Wprowadzenie odpowiednich ze względu na charakter pracy Administratora Danych ogólnych zasad bezpieczeństwa przetwarzania danych - zgodnie z wymaganiami przepisów prawnych z zakresu ochrony danych osobowych – pozwala na prawidłowe przetwarzanie danych.

2. Postanowienia dotyczące ogólnych zasad bezpieczeństwa:

a) Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik lub współpracownik mający dostęp do danych.
b) Pracownicy i współpracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności wynikające z ich obowiązków na rzecz Fundacji
c) przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
d) w miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie 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.
e) Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści.
f) Niedopuszczalne, z zastrzeżeniem lit. g), 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.
g) Osoby upoważnione do przetwarzania danych w Fundacji uprawnione są do przetwarzania danych w ramach wykonywanej w Fundacji funkcji także na swoich prywatnych urządzeniach wynoszonych poza teren Fundacji, pod warunkiem ich prawidłowego zabezpieczenia oraz przetwarzania danych wyłącznie w ramach i na potrzeby wyznaczonych w ramach Fundacji zadań.
h) Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
i) Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy i współpracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

1. W przypadku stwierdzenia :

a) naruszenia zabezpieczeń systemu informatycznego,
b) naruszenia technicznego stanu urządzeń,
c) naruszenia zawartości zbioru danych osobowych,
d) ujawnienia metody pracy lub sposobu działania programu,
e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

<u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie Administratora oraz Inspektora Ochrony Danych o ile taki został wyznaczony.</u>

2. W razie niemożliwości zawiadomienia powyższych podmiotów należy powiadomić bezpośredniego przełożonego.

3. W przypadku stwierdzenia naruszenia, niezależnie od zgłoszeń o których mowa w ust. 1 i 2., należy:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
b) udokumentować wstępnie zaistniałe naruszenie;
c) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby przez niego upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator, Inspektor Ochrony Danych, lub osoba przez nich upoważniona

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji oraz dla praw i wolności osób których dane dotyczą
b) może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
c) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych Prezesa Urzędu Ochrony Danych Osobowych;
d) nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji;
e) informuje o naruszeniu osoby których danych ono dotyczy, jeżeli naruszenie będzie miało wpływ lub narazi prawa podmiotowe tej osoby, w szczególności jej dobra osobiste lub inne prawnie chronione interesy.

5. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, zasięga się niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. Inspektor Ochrony Danych, a jeżeli nie został wyznaczony, to Administrator dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;
b) określenie czasu i miejsca: naruszenia/ujawnienia i powiadomienia o tym fakcie;
c) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;
d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
e) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;
f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Raport, o którym mowa w pkt. 6, Inspektor Ochrony Danych niezwłocznie przekazuje Administratorowi Danych.

8. Zaistniałe naruszenie/ujawnienie ochrony danych osobowych może stać się przedmiotem szczegółowej analizy prowadzonej przez Administratora lub Inspektora Danych Osobowych.

9. Analiza, o której mowa w pkt. 8, powinna zawierać:
a) wszechstronną ocenę zaistniałego naruszenia/ujawnienia ochrony danych osobowych;
b) wskazanie odpowiedzialnych;
c) wnioski co do ewentualnych przedsięwzięć: proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom/ujawnieniom w przyszłości.

10. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 33 ust. 1 Rozporządzenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

11. Zgłoszenie, o którym mowa w ust. 10, musi co najmniej:
a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Fundacja Ekorozwoju sprawuje Administrator , Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
2. Czynności kontrolne przeprowadzane są raz do roku.
3. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności.
4. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji.
Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w niniejszym Rozdziale stanowi Załącznik nr 9 do niniejszej Polityki.

8. WYKAZ POZOSTAŁYCH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. Zastosowane środki techniczne i organizacyjne przedstawiono w załączniku nr 9 do Polityki Ochrony Danych Osobowych. Zastosowane je w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Środek ochrony technicznej i fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Prowadzona jest kontrola osób wchodzących i opuszczających obszar przetwarzania danych osobowych	**TAK**	
2. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są fizycznymi zabezpieczeniami w postaci zamków zamykanych na klucz**.**	**TAK**	
3. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych **niemetalowych szafach.**	**TAK**	
4. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**	**TAK**	
5. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**	**TAK**	
6. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny.**	**TAK**	
7. Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	**TAK**	
8. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	**TAK**	
9. Wyznaczono Inspektora Ochrony Danych	**NIE**	
10. Opracowano i wdrożono Politykę Ochrony Danych Osobowych	**TAK**	
11. Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	**TAK**	
12. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	**TAK**	
13. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	**TAK**	
14. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	**TAK**	
15. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	**TAK**	

ZAŁĄCZNIKI

Załącznik nr 1 – Ustanowienie Inspektora Ochrony Danych
Załącznik nr 2 – Upoważnienie Inspektora Ochrony Danych do nadawania upoważnień
Załącznik nr 3 – Ustanowienie Administratora Systemów Informatycznych
Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę
Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy innej niż umowa o pracę
Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności
Załącznik nr 6 – Rejestr Czynności przetwarzania danych
Załącznik nr 7 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych
Załącznik nr 9 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Dokument sporządzono: Data: …/…/…… (dd/mm/rrrr) Miejsce: ……	**Pełen podpis Administratora Danych:**	**Pieczęć**

Niniejszym, zgodnie z art. 37 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) i dyspozycją Rozdziału 2 Polityki Ochrony Danych Osobowych oraz reprezentując Administratora Danych – Fundację Ekorozwoju,

wyznaczam

Panią/Pana …….. na stanowisko **Inspektora Ochrony Danych Osobowych** w Fundacji Ekorozwoju.

Zakres obowiązków oraz warunki pełnienia funkcji Inspektora Ochrony Danych Osobowych określone są 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) roku oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną w Fundacji Ekorozwoju.

DATA I PODPIS OSOBY WYZNACZONEJ
NA STANOWISKO IODO

DATA I PODPIS OSOBY REPREZENTUJĄCEJ
ADMINISTRATORA DANYCH

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Ochrony Danych Osobowych oraz reprezentując Administratora Danych – Fundacja Ekorozwoju

upoważniam

Panią/Pana …….. **Inspektora Ochrony Danych Osobowych** w Fundacja Ekorozwoju do nadawania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO IODO

DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Ochrony Danych Osobowych oraz reprezentując Administratora Danych – Fundacja Ekorozwoju

wyznaczam

Panią/Pana …….. na stanowisko **Administratora Systemów Informatycznych (ASI)** w Fundacja Ekorozwoju

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są 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) oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną w Fundacji.

DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO ASI

DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, działając w imieniu Fundacji Ekorozwoju (dalej Fundacja), **upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona zobowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.
Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami 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) , zwanym dalej „Rozporządzeniem", ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych i obowiązującymi w Fundacja wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.
Upoważnienie jest ważne do odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Fundacji (w szczególności z Polityką Ochrony Danych Osobowych oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.
Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, działając w imieniu Fundacji Ekorozwoju (dalej Fundacja), **upoważniam:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami 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) , zwanym dalej „Rozporządzeniem", ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych i obowiązującymi w Fundacja wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz odpowiedzialności cywilnej.

Upoważnienie jest ważne do odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnione

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Fundacji (w szczególności z Polityką Ochrony Danych Osobowych oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych.

……..

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:

1 x oryginał dokumentacja kadrowa

1 x oryginał osoba upoważniona

……………………., dnia ……………..

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y . . . . zamieszkała/y w . . . . zatrudniona/y na stanowisku . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z …………………………….. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

…………………………………………………..
Podpis

Załącznik nr 6 – Rejestr Czynności Przetwarzania Danych

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Zakres przetwarzanych danych	Kategorie odbiorców
1.	Dane pracowników i współpracowników	Serwer , MS Word, MS Excel, MS Outlook, Konta bankowe, Program księgowo-Kadrowy, domeny zapewniające funkcjonalności chmury, e-mail I www	- księgowy - kadrowy - administracyjny	imiona i nazwiska, adres zamieszkania, seria i numer dowodu osobistego,numer ewidencyjny PESEL i/lub NIP, data i miejsce urodzenia,) numer konta bankowego, dane kontaktowe , wykształcenie i historia zatrudnienia.	ZUS, Urząd Skarbowy oraz Księgowość
2.	Kandydaci do pracy	Serwer, MS Word, MS Excel, MS Outlook,	- kadrowy	imiona i nazwiska, adres zamieszkania, data i miejsce urodzenia, dane kontaktowe) wykształcenie i historia zatrudnienia	Brak
3.	Wolontariusze	Serwer , MS Word, MS Excel, MS Outlook, , Program księgowo-kadrowy, domeny zapewniające funkcjonalności chmury, e-mail I www	- księgowy, - administracyjny	imiona i nazwiska, adres zamieszkania, dane kontaktowe	ZUS oraz Księgowość, podmioty finansujące, współfinansujące lub współorganizujące Projekty Fundacji, Edukatorzy
4.	Uczestnicy Projektów	Serwer , MS Word, MS Excel, MS Outlook, Konta bankowe, Program księgowo-Kadrowy, domeny zapewniające funkcjonalności chmury, e-mail I www	- administracyjny - organizacja i realizacja projektów	imiona i nazwiska, dane kontaktowe, adres zamieszkania	podmioty finansujące, współfinansujące lub współorganizujące Projekty Fundacji, Edukatorzy
5.	Otrzymujący Newsletter	Serwer , MS Word, MS Excel, MS Outlook, domeny zapewniające funkcjonalności chmury, e-mail I www	Informowanie o bieżących aktualnościach w Fundacji	imiona i nazwiska, adres poczty elektronicznej,	Brak
6.	Darczyńcy	Serwer , MS Word, MS Excel, MS Outlook, Konta bankowe, Program księgowo-Kadrowy, domeny zapewniające funkcjonalności chmury, e-mail I www	- księgowy	imiona i nazwiska, adres zamieszkania ,jeżeli darczyńca chce pozostawić takie informacje, NIP jeżeli darowizna została dokonana w formie 1% podatku dochodowego,numer konta bankowego, jeżeli darowizna została dokonana przelewem, dane kontaktowe, jeżeli darczyńca chce pozostawić takie informacje	Brak

Załącznik nr 7 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				

Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

	Adres / lokalizacja	Uwagi
Podmioty, którym Administrator Danych powierzył przetwarzanie danych osobowych		

.....
miejscowość, data

PROTOKÓŁ
Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*
w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej:.....
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli: .....
3. Data wykonania czynności kontrolnych:.....
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: .....
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:.....
.....
6. Ustalenia dokonane w trakcie czynności kontrolnych:.....
.....
.....
.....
.....
7. Wnioski i zalecenia pokontrolne:
.....
.....
.....
.....
.....
.....

(data i podpis osoby wykonującej czynności kontrolne) (data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:
1 x Kierownik kontrolowanej jednostki organizacyjnej
1 x Inspektor Ochrony Danych Osobowych

_____
* niepotrzebne skreślić