POLITYKA PRYWATNOŚCI WE WROCŁAWSKIM STOWARZYSZENIU DOBRZE UBEZPIECZONYCH UL. ENERGETYCZNA 14/3A WROCŁAW

SPIS TREŚCI:

METRYKA DOKUMENTU

Tytuł dokumentu	Polityka prywatności
Dokument opublikował	
Dokument wytworzył	
Data publikacji	2021-06-09

REJESTR ZMIAN DOKUMENTU

Data	Akcja	Autor zmiany
202106	Utworzenie dokumentu	

§1. Wprowadzenie

Wrocławskie Stowarzyszenie Dobrze Ubezpieczonych, ul. Energetyczna 14/3A, Wrocław, zwane dalej WSDU, jako administrator danych osobowych, przykłada dużą wagę do ochrony danych osobowych oraz poszanowania prywatności osób, których dane są przetwarzane.

1. Charakter działania WSDU wymaga podejmowania działań ze szczególną starannością z uwzględnieniem indywidualnych interesów osób fizycznych, w szczególności członków stowarzyszenia, pracowników, klientów, kontrahentów WSDU.
2. Niniejsza Polityka Prywatności, zwana dalej „**Polityką**" opisuje sposób przetwarzania danych osobowych we WSDU zgodnie z przepisami prawa, w szczególności 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 (dalej „**RODO**") oraz innymi przepisami prawa polskiego europejskiego (dalej łącznie „**Przepisy ochrony danych**").
3. Niniejszy dokument stanowi wykonanie obowiązku, o którym mowa w art. 24 ust. 2 RODO.
4. Ewidencje określone niniejszym dokumentem mogą być prowadzone formie papierowej lub w sposób elektroniczny.
5. Jeżeli co innego nie wynika z Polityki lub przepisów prawa ustalenie treści załączników, o których mowa w Polityce, należy do Prezesa WSDU.
6. **Definicje**

1. **Administrator danych, ADO** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administrator danych jest odpowiedzialny za zgodne z prawem przetwarzanie danych osobowych.
2. **Administrator systemu informatycznego, ASI** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych.
3. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
4. **Osoba upoważniona** – osoba posiadająca upoważnienie wydane przez administratora danych (lub osobę uprawnioną przez niego) oraz dopuszczona do przetwarzania danych w zakresie określonym w upoważnieniu.
5. **Powierzenie przetwarzania danych osobowych** – zlecenie części lub całości procesu przetwarzania danych osobowych innemu podmiotowi, działającemu za zlecenie oraz w imieniu ADO, w drodze umowy.
6. **Procesor** - podmiot przetwarzający dane osobowe na zlecenie i w celu wyznaczonym przez Administratora danych osobowych, w oparciu o zapisy umowy powierzenia przetwarzania danych.
7. **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub

niezautomatyzowany, w tym m.in. 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.

8. **Właściciel procesu przetwarzania, WPP -** osoba odpowiedzialna za całokształt przetwarzania danych w ramach wydzielonego, zdefiniowanego obszaru, procesu lub czynności przetwarzania danych osobowych.
9. **Załącznik** - stanowiący integralną część Polityki dokument wydany na jej podstawie przez Administratora Danych Osobowych.

§2. Cel

Celem Polityki jest określenie i wdrożenie jednolitych zasad bezpieczeństwa przetwarzania i ochrony danych przetwarzanych przez WSDU, w szczególności:

1) ustanowienie organizacji bezpieczeństwa danych osobowych;
2) określenie sposobu prowadzenia dokumentacji przetwarzania danych osobowych;
3) określenie zakresu obowiązków i odpowiedzialności osób przetwarzających dane osobowe;
4) określenie zasadniczych wymagań w zakresie przetwarzania i ochrony danych osobowych.

§3. Zakres stosowania

1. Politykę stosuje się w odniesieniu do wszelkich danych i informacji, dotyczących zidentyfikowanych, bądź możliwych do zidentyfikowania osób fizycznych.
2. Politykę stosuje się w odniesieniu do wszelkich danych osobowych przetwarzanych w związku z prowadzeniem działań własnych i ustawowych oraz powierzonych WSDU, niezależnie od tego, czy są one przetwarzane w zbiorach danych.
3. Politykę stosuje się do danych, niezależnie od formy ich przetwarzania, o ile tylko stanowią one dane osobowe.
4. Politykę stosuje się niezależnie od miejsca przetwarzania danych oraz wykorzystywanych w tym celu narzędzi. Postanowienia Polityki dotyczą przetwarzania danych poza siedzibą Administratora danych oraz przy wykorzystaniu narzędzi niestanowiących własności WSDU, w tym narzędzi stanowiących własność podmiotów upoważnionych do przetwarzania lub działających na rzecz WSDU.
5. Zobowiązanie dotyczące konieczności stosowania Polityki dotyczy wszelkich podmiotów przetwarzających dane z upoważnienia Administratora danych, w tym w szczególności pracowników, zleceniobiorców, współpracowników oraz partnerów współpracujących z Administratorem danych.
6. Do stosowania Polityki zobowiązane są podmioty przetwarzające dane w oparciu o zawartą umowę powierzenia przetwarzania danych, przy założeniu, że stosowanie postanowień Polityki zostanie potwierdzone w umowie.

§4. Odpowiedzialność

1. **Administrator danych** jest odpowiedzialny za:

a) przetwarzanie danych zgodnie z obowiązującymi przepisami prawa, nie naruszając praw i wolności osób, których dane dotyczą,

b) określenie i wdrożenie odpowiednich środków technicznych i organizacyjnych zabezpieczających przetwarzanie i gwarantujących zgodność z prawem, przy uwzględnieniu charakteru, zakresu, kontekstu i celu przetwarzania danych jak również ryzyka naruszenia praw i wolności osób, których dane dotyczą,

2. **Podmiot przetwarzający** oraz każda **osoba działająca z upoważnienia Administratora danych** jest odpowiedzialna za:

a) przetwarzanie danych wyłącznie na udokumentowane polecenie Administratora danych, zgodnie ze wskazanym przez niego zakresie oraz przy wykorzystaniu zaakceptowanych narzędzi i środków,

b) przetwarzanie danych osobowych zgodnie z zasadami zawartymi w Polityce.

3. W celu zapewnienia nadzoru nad sprawnością systemu informatycznego WSDU jako ADO, może część lub całość czynności powierzyć Administratorowi Systemu Informatycznego. W przypadku niewyznaczenia ASI, odpowiedzialność za wykonywanie czynności związanych z bezpieczeństwem systemu informatycznego ciąży na ADO.

4. **Administrator Systemu Informatycznego** jest odpowiedzialny za:

a) opracowanie procedur dla działań systemowych związanych ze środkami przetwarzania lub przesyłania informacji takich, jak procedury uruchamiania i zatrzymania urządzeń, przygotowania kopii zapasowych, konserwacji sprzętu, obsługi nośników, zarządzania pomieszczeniami komputerowymi;

b) rejestrację użytkowników w systemie informatycznym oraz nadawanie, modyfikacja i odbieranie wymaganych uprawnień na podstawie potwierdzonych wniosków przełożonych;

c) nadzór nad czynnościami związanymi z funkcjonowaniem oraz zabezpieczeniem urządzeń oraz oprogramowania systemów informatycznych WSDU.

d) podejmowanie działań w przypadku naruszeń bezpieczeństwa systemu informatycznego w tym przywrócenie stanu prawidłowego, zidentyfikowanie przyczyn naruszenia i osób odpowiedzialnych oraz przedstawienie wniosków;

e) nadzór nad świadczeniem usług wsparcia systemów informatycznych przez podmioty zewnętrzne.

5. **Właściciele procesów przetwarzania** są odpowiedzialni za: nadzór nad stosowaniem zasad przetwarzania danych w podległych im procesach przetwarzania danych osobowych, a w razie zaistnienia zmian dokonywanie aktualizacji mających wpływ na bezpieczeństwo przetwarzania danych osobowych.

§5. Zasady podstawowe przetwarzania danych

1. Przetwarzanie danych osobowych przez WSDU jest dopuszczalne wyłącznie zgodnie z przepisami obowiązującego prawa.

2. W przypadku, gdy do przetwarzania danych konieczne jest uprzednie uzyskanie zgody osoby, której dane dotyczą, zgoda taka winna być:

a) dobrowolna – pozyskana w okolicznościach umożliwiających swobodne wyrażenie woli osoby ją składającej,

b) świadoma – osoba składająca oświadczenie powinna zostać poinformowana komu i w jakim celu przekazywane są dane oraz w jaki sposób będą one przetwarzane,

c) konkretna – treść zgody powinna wskazywać jednoznacznie, na co godzi się osoba ją składająca,

d) wyraźna – zgoda musi polegać na aktywnym działaniu osoby, która jej udziela,

e) uprzednia – pozyskana przed wprowadzeniem danych do systemu WSDU.

3. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty,

b) zbierane dla konkretnych, wyraźnych i prawnie uzasadnionych celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

d) prawidłowe i w razie potrzeby uaktualniane,

e) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

4. WSDU podejmuje działania w celu zapewnienia prawidłowości przetwarzanych danych, a w razie konieczności ich uaktualnienia, usunięcia lub sprostowania w sytuacji ich nieprawidłowości w stosunku do celów przetwarzania.

5. W celu zapewnienia realizacji zasady ograniczonego przetwarzania, dane osobowe przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą przechowywane są przez okres nie dłuższy niż jest to niezbędne do realizacji celów przetwarzania, chyba że przetwarzanie odbywa się w celach archiwalnych, badań naukowych, historycznych lub dla celów statystycznych i zachowane są środki techniczne i organizacyjne zapewniające poszanowanie zasady minimalizacji danych.

6. Dane osobowe przetwarzane są w sposób zapewniający odpowiednie bezpieczeństwo, w szczególności poprzez zabezpieczenie przed przetwarzaniem niezgodnym z prawem, przypadkową utratą, zniszczeniem lub uszkodzeniem, które rozumie się jako zapewnienie atrybutów integralności i poufności danych.

7. Bezpieczeństwo przetwarzania danych osobowych osiąga się w szczególności poprzez zastosowanie zasad:

a. poufności – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;

b. integralności – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

c. dostępności – zapewnienie, że informacja jest osiągalna i możliwa do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;

d. rozliczalności – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

e. autentyczności – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);

f. niezaprzeczalności – brak możliwości wyparcia się swojego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;

g. niezawodności – zapewnieniu spójności oraz zamierzonych zachowań i skutków.

8. WSDU wdraża odpowiednie środki w celu umożliwienia realizacji praw oraz ułatwienia komunikacji z osobami których dane dotyczy.

§6. Zasady dopuszczania osób do przetwarzania danych osobowych

1. Dostęp do danych osobowych mogą posiadać wyłącznie osoby upoważnione do przetwarzania danych osobowych, po zaznajomieniu z zasadami ochrony i bezpieczeństwa przetwarzania danych osobowych oraz wynikającymi z tego obowiązkami.
2. Upoważnienia do przetwarzania danych osobowych nadaje Prezes WSDU.
3. Za przygotowanie upoważnienia do przetwarzania danych w WSDU jest odpowiedzialna wyznaczona przez ADO osoba.
4. Zaznajomienie osoby z zasadami przetwarzania danych osobowych co potwierdzane jest poprzez złożenie podpisu na „**Oświadczeniu o zachowaniu poufności**” oraz „**Upoważnieniu do przetwarzania danych osobowych**”

   Załącznik nr 1 Upoważnieniu do przetwarzania danych osobowych – członkowie stowarzyszenia

   Załącznik nr 2 Upoważnieniu do przetwarzania danych osobowych – umowy o pracę, umowy cywilnoprawne

   Załącznik nr 3 Cofnięciu upoważnienia do przetwarzania danych osobowych

   Załącznik nr 4 Oświadczeniu o zachowaniu poufności
5. Dokumenty, o których mowa w punkcie poprzednim zostają dołączone, przez osobę zajmującą się sprawami pracowniczymi, odpowiednio do akt osobowych pracownika, przez wskazaną przez ADO osobę do dokumentacji zleceniobiorcy, współpracownika, kontrahenta.
6. Osoby dopuszczone do przetwarzania danych osobowych upoważnione są do przetwarzania danych wyłącznie na okres i w zakresie niezbędnym do wykonywania powierzonych im obowiązków.
7. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania poufności tych danych oraz sposobów ich zabezpieczenia, również po zakończeniu współpracy z ADO, niezależnie od formy tej współpracy.
8. Ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie z **Załącznikiem nr 10**.
9. Osobom upoważnionym, którym jest to niezbędne, ASI tworzy konto użytkownika w systemie informatycznym WSDU.
10. ASI nadaje, modyfikuje oraz odbiera uprawnienia użytkowników na podstawie:
    a) wiadomości mail – od Prezesa WSDU lub wskazanej osoby;
    b) pisma – od przełożonego;

c) w uzasadnionych przypadkach telefonicznie, co wymaga późniejszego pisemnego potwierdzenia przez przełożonego.

§7. Zasady określania środków bezpieczeństwa

1. W celu zachowania bezpieczeństwa i zapobieganiu przetwarzaniu niezgodnemu z prawem Administrator danych szacuje ryzyka właściwe dla przetwarzania oraz wdraża odpowiednie środki mitygujące te ryzyka.
2. Oceniając ryzyko w zakresie bezpieczeństwa danych Administrator danych bierze pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.
3. Środki powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ich ochronie.

§8. Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Administrator danych ma obowiązek dołożyć wszelkich starań w celu wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów Przepisów ochrony danych, w szczególności poprzez wdrożenie zasad uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych.
2. W celu wdrożenia zasad Administrator danych realizuje:
    a) ocenę ryzyka - dla każdej inicjatywy realizowanej w organizacji Administratora,
    b) oceny skutków dla ochrony danych - w przypadku, gdy przetwarzanie danych osobowych, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych oraz gdy taki obowiązek wynika z przepisów prawa,
    c) konsultacje z organem nadzorczym - w przypadkach określonych w art. 36 RODO lub przewidzianych w innych przepisach.
3. Podstawowymi działaniami Administratora danych dążącymi do realizacji opisanych zasad jest minimalizacja zakresu przetwarzania danych oraz stosowanie technicznych środków zabezpieczeń, takich jak szyfrowanie, pseudonimizacja lub anonimizacja.
4. Za realizację powyższych zasad odpowiedzialni są właściciele poszczególnych procesów przetwarzania (WPP).

§9. Podejście oparte na ryzyku

1. WPP zobowiązany jest do wykonania szacowania ryzyka w odniesieniu do charakteru, zakresu, kontekstu i celów przetwarzania danych.
2. WPP zobowiązany jest wykonać szacowanie ryzyka:
    a) dla każdej nowej czynności przetwarzania danych („**inicjatywy**”);

b) w sytuacji zmiany charakteru, zakresu, kontekstu i celów istniejących czynności lub w przypadku zmiany przepisów mających znaczenie dla tego procesu;

c) regularnie nie rzadziej niż raz na 12 miesięcy.

3. Realizacja inicjatywy wymaga uzyskania pozytywnej oceny szacowania ryzyka.

4. Szacowanie ryzyka powinno uwzględniać czynniki takie jak:

a) prawdopodobieństwo wystąpienia określonego zdarzenia będącego naruszeniem;

b) powagę tego zdarzenia (wymiernej wielkości szkody oraz zakresu występowania szkód) jakie zdarzenie to może spowodować;

c) wpływu zdarzenia na atrybuty w zakresie dostępności, integralności oraz poufności;

d) wystąpienie okoliczności wymagających od Administratora danych wyznaczenia IOD;

e) dostępne środki minimalizujące przetwarzanie danych w zakresie ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

5. Administrator danych zobowiązuje się do stosowania następujących zasad dla opisanego procesu szacowania ryzyka:

a) szacowanie odbywa się w oparciu o obiektywną i rzeczową analizę przy wykorzystaniu metodyki zaakceptowanej przez Administratora danych;

b) szacowanie ryzyka jest procesem ciągłym, dla którego wdrożone środki ochrony i zabezpieczenia techniczne i organizacyjne podlegają cyklicznemu monitorowaniu i doskonaleniu.

6. Administrator danych wykonuje ocenę skutków dla ochrony danych w następujących sytuacjach:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych wskazanych w art. 9 ust. 1 RODO;

c) przetwarzania na dużą skalę danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa;

d) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie;

e) jeżeli w wyniku szacowania ryzyka stwierdzone zostanie, że dany rodzaj przetwarzania z dużym prawdopodobieństwem powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

7. Ocena skutków dla ochrony danych obejmuje w najmniejszym zakresie następujące elementy:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania;

b) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;

d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych.

§10. Konsultacje z organem nadzorczym

1. W przypadku, gdy ocena ryzyka wykaże, że przetwarzanie danych może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw i wolności podmiotów danych i brak jest możliwości zastosowania działań mających na celu zminimalizowanie tego ryzyka, Administrator danych zobowiązany jest do dokonania konsultacji z organem nadzorczym danej czynności przetwarzania.
2. Przekazując dokumentację dotyczącą ocenianej czynności Administrator danych przedstawia organowi dane w zakresie obejmującym minimum:
    a) zidentyfikowane obowiązki Administratora danych i podmiotów przetwarzających biorących udział w konsultowanej czynności;
    b) wykorzystane środki techniczne i organizacyjne dążące do ochrony praw i wolności osób fizycznych;
    c) dane kontaktowe osoby odpowiedzialnej w WSDU za przetwarzanie danych osobowych;
    d) ocenę skutków dla ochrony danych;
    e) inne informacje, których zażąda organ nadzorczy w toku prac konsultacyjnych.
3. Osobą odpowiedzialną za przeprowadzenie konsultacji osoba wskazana przez Administratora danych.
4. Osoba wskazana przez Administratora danych prowadzi rejestr inicjatyw, które podlegały konsultacjom.

§11. Prawa osób, których dane dotyczą

1. ADO zobowiązany jest do ułatwienia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15-22 RODO.
2. ADO realizuje prawa podmiotu danych bez zbędnej zwłoki, a w każdym razie w terminie nie przekraczającym miesiąca liczonym od daty otrzymania żądania.
3. W przypadku braku możliwości realizacji żądania w terminie wskazanym w ust. 2 ADO ma prawo do przedłużenia terminu realizacji o kolejne dwa miesiące, przy jednoczesnej konieczności poinformowania podmiotu danych o takim przedłużeniu terminu wraz ze wskazaniem przyczyny. ADO przekazuje informację w formie pisemnej lub elektronicznej, nie później niż przed upływem miesiąca od daty otrzymania żądania.
4. ADO realizuje prawa podmiotu wyłącznie po zidentyfikowaniu osoby żądającej oraz potwierdzeniu przysługiwania jej praw.
5. Działania wynikające z realizacji art. 15-22 RODO są wolne od opłat, chyba że:
    a) żądanie ma charakter nieuzasadniony i został on potwierdzony przez ADO;
    b) żądanie ma charakter nadmierny, w szczególności ze względu na swój ustawiczny charakter i został on potwierdzony przez ADO.

Obowiązki informacyjne

6. Działając jako ADO, WSDU zobowiązana jest do spełnienia obowiązku informacyjnego w stosunku do osób, których dane osobowe są gromadzone, chyba że przepis prawa zwalnia ze spełnienia tego obowiązku.
7. Osoba, której dane są gromadzone powinna uzyskać informację o:
   a) adresie siedzibie i pełnej nazwie Administratora danych wraz z danymi kontaktowymi;
   b) gdy ma to zastosowanie – danych kontaktowych Inspektora Ochrony Danych;
   c) celach przetwarzania danych osobowych wraz z podstawą prawną przetwarzania;
   d) gdy ma to zastosowanie – informacje na temat przetwarzania w oparciu o prawnie uzasadniony interes realizowany przez Administratora danych lub stronę trzecią;
   e) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją (lub przewiduje się przekazanie danych);
   f) gdy ma to zastosowanie – o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
   g) okresach, przez które dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tych okresów;
   h) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   i) gdy ma to zastosowanie - przetwarzaniu w oparciu o zgodę i związanym z tym prawie do cofnięcia zgody w dowolnym momencie;
   j) prawie do wniesienia skargi do organu nadzorczego;
   k) czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
   l) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
   m) w przypadku pozyskania danych nie bezpośrednio od osoby, której dane dotyczą, dodatkowo o źródle pochodzenia danych.
8. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych są odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO.
9. Za stosowanie właściwych klauzuli informacyjnych, przy zbieraniu danych osobowych odpowiadają osoby zaangażowane w proces zbierania danych osobowych.
10. Osoby, projektujące procesy związane, choćby pośrednio, z przetwarzaniem danych, zobowiązane są do przekazania informacji, o których mowa w ust.7 przed pozyskaniem danych, a w przypadku pozyskania danych nie bezpośrednio od osoby, której dane dotyczą:
    a) w rozsądnym terminie po uzyskaniu danych, najpóźniej w ciągu miesiąca,
    b) najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą,
    c) jeśli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

Załącznik nr 5 - wzór klauzuli informacyjnej dla osoby fizycznej – art. 13 RODO

Załącznik nr 6 - wzór klauzuli informacyjnej dla osoby fizycznej pozyskanych od innego podmiotu– art. 14 RODO

Załącznik nr 7 - wzór klauzuli informacyjnej dla osoby fizycznej –członka WSDU

Załącznik nr 8 - wzór klauzuli informacyjnej dla osoby fizycznej działającej w imieniu innego niż osoba fizyczna podmiotu– art. 13 RODO

Prawo dostępu do danych oraz ich poprawiania

11. Osobie, której dane osobowe są przetwarzane przez WSDU. należy zapewnić możliwość dostępu do dotyczących jej danych osobowych, w tym uzyskania ich kopii, w celu ich weryfikacji i poprawiania, a także do wszelkich informacji dotyczących przetwarzania jej danych osobowych, o których mowa w ust. 7.

Prawo wycofania zgody

12. W przypadku, gdy przetwarzanie danych osoby wynika z udzielonej wcześniej przez nią zgody, osobie, której dane dotyczą przysługuje prawo wycofania takiej zgody w każdym czasie. Wycofanie zgody pozostaje bez wpływu na zgodność z prawem działań podejmowanych przez ADO przed jej wycofaniem.

Prawo sprzeciwu

13. Osobie, której dane dotyczą przysługuje prawo sprzeciwu w związku z jej szczególną sytuacją, w przypadku, gdy przetwarzanie danych osoby:
    a) odbywa się w realizacji uzasadnionych celów ADO lub odbiorców danych lub
    b) jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

    W przypadku zgłoszenia sprzeciwu, zabronione jest dalsze przetwarzanie danych osobowych, chyba że istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

14. Osobie, której dane dotyczą przysługuje prawo sprzeciwu wobec przetwarzania danych w celach marketingowych. W przypadku zgłoszenia sprzeciwu, zabronione jest dalsze przetwarzanie danych w tych celach.

Prawo do przeniesienia danych

15. WSDU jako ADO, zobowiązany jest do przekazania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe, które ta osoba dostarczyła.

16. Uprawnienie podmiotu danych realizowane jest w następujących przypadkach:
    a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy;
    b) przetwarzanie odbywa się w sposób zautomatyzowany.

17. Zakres danych podlegający przeniesieniu ustalany jest każdorazowo przez wskazaną przez Prezesa WDSU osobę analizującą zasadność realizacji wskazanego uprawnienia podmiotu danych.

18. Za powszechnie używany format elektroniczny uznaje się format .xls (MS Excel) oraz .csv (strukturyzowany plik tekstowy).

Prawo do usunięcia danych

19. WSDU jako ADO zobowiązany jest do niezwłocznego usunięcia danych podmiotu w przypadku zaistnienia jednej z następujących sytuacji:
    a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
    c) osoba, której dane dotyczą, wnosi sprzeciw w związku z jej szczególną sytuacją lub sprzeciw na przetwarzanie danych w celach marketingowych;
    d) dane były przetwarzane niezgodnie z prawem;
    e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega Administrator.

Prawo do ograniczenia przetwarzania danych

20. WSDU jako ADO zobowiązany jest do ograniczenia przetwarzania danych dotyczących osoby, wyłącznie do ich przechowywania, jeżeli:
    a) osoba kwestionuje prawidłowość danych;
    b) przetwarzanie jest niezgodne z prawem, lecz osoba, której dane dotyczą sprzeciwia się ich usunięciu;
    c) dane osobowe nie są już niezbędne dla realizacji celu przetwarzania, ale są one potrzebne osobie, której dane dotyczą,
    d) osoba, której dane dotyczą zgłosiła sprzeciw wobec przetwarzania danych ze względu na swoją szczególną sytuację.

§12. Sposób postępowania w przypadku naruszenia ochrony danych osobowych

1. Naruszeniem ochrony danych jest:
    a) jakiekolwiek naruszenie poufności, integralności, dostępności, autentyczności danych osobowych zawartych w dokumentach tradycyjnych lub elektronicznych,
    b) jakiekolwiek naruszenie niezawodności systemu informatycznego wykorzystywanego do przetwarzania danych osobowych, spowodowane awarią sprzętu lub oprogramowania, bądź działaniami dokonanymi przez osoby upoważnione lub nieupoważnione, mające wpływ na przetwarzane w tym systemie dane osobowe.
2. Naruszeniem ochrony danych jest w szczególności:
    a) naruszenie integralności terytorialnej obszaru przetwarzania danych: włamanie, wtargnięcie napastników;
    b) kradzież bądź zagubienie stacji roboczej lub nośnika z danymi osobowymi;
    c) włamanie do systemu informatycznego służącego do przetwarzania danych osobowych;
    d) przekazanie osobie nieuprawnionej, informacji o systemie informatycznym takich jak: hasła, sposób zabezpieczenia;
    e) posłużenie się cudzym hasłem dostępu przy przetwarzaniu danych osobowych;
    f) uzyskanie dostępu do obszaru przetwarzania lub bezpośrednio do danych osobowych przez osobę nieupoważnioną.

3. W przypadku wykrycia naruszenia bezpieczeństwa danych osobowych osoba upoważniona zobowiązana jest do przekazania informacji o zaistniałym zdarzeniu ABI oraz swojego przełożonego.
4. ADO zgłasza zaistniałe naruszenia ochrony danych właściwemu organowi nadzorczemu oraz informuje osoby, których dane dotyczą zgodnie z właściwymi przepisami RODO. ADO prowadzi rejestr zaistniałych naruszeń ochrony danych osobowych.
5. Szczegóły postępowania w sytuacji naruszenia ochrony danych oraz sposób ich dokumentowania określa Instrukcja Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych.

§13. Zasady powierzenia przetwarzania danych osobowych

1. WSDU przewiduje możliwość powierzania przetwarzania danych osobowych innym podmiotom („**Procesorom**"). Powierzenie przetwarzania danych innym podmiotom może być wykonane wyłącznie na podstawie stosownej umowy powierzenia przetwarzania danych osobowych, określającej co najmniej:
    a) charakter i cel powierzenia przetwarzania,
    b) zakres danych wraz ze wskazaniem kategorii osób oraz czynności podlegających powierzeniu,
    c) sposób przetwarzania danych przez Procesora,
    d) czas trwania,
    e) zobowiązanie Procesora do zachowania adekwatnego poziomu bezpieczeństwa przetwarzania danych osobowych,
    f) obowiązki oraz prawa WSDU, w szczególności uprawnienie WSDU do przeprowadzenia kontroli przetwarzania danych przez Procesora oraz inne obowiązki i prawa ADO o których mowa w art. 28 ust. 3 RODO.
2. Umowa winna być sporządzona na piśmie. Postanowienia dotyczące powierzenia przetwarzania danych osobowych mogą być zawarte w ogólnej umowie zawieranej z wykonawcą w formie klauzuli lub w formie odrębnej umowy powierzenia przetwarzania danych.
3. WPP zobowiązana jest do uzyskania Prezesa WSDU przed zawarciem umowy powierzenia przetwarzania danych osobowych na powierzenie przetwarzania danych.

Załącznik nr 9 – wzór umowy powierzenia przetwarzania danych

Załącznik nr 11 wzór Rejestr umów powierzenia danych

§14. Zasady udostępnienia danych osobowych

1. WSDU przewiduje możliwość udostępnienia danych innym podmiotom.
2. Udostępnienie danych osobowych może odbyć się wyłącznie na podstawie przepisów prawa, lub gdy osoba, której dane są przetwarzane wyrazi na to swoją zgodę. Zgoda na udostępnienie danych powinna zostać utrwalona.

§15. Przegląd Polityki

1. Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi oraz zmianami faktycznymi.

2. Niezależnie od zmian prawnych i faktycznych ADO lub podmiot wskazany przez ADO jest odpowiedzialny za przegląd Polityki wraz z załącznikami stanowiącymi jej integralną część nie rzadziej niż raz na 12 miesięcy.
3. Zmiany oraz przeglądy dokumentacji muszą być odnotowywane w metryce dokumentu.

§16. Wejście w życie

1. Polityka Prywatności wchodzi w życie z dniem 9 czerwca 2021r.

2. Integralną częścią Polityki są:

Załącznik nr 1 wzór Upoważnieniu do przetwarzania danych osobowych – członkowie stowarzyszenia

Załącznik nr wzór 2 Upoważnieniu do przetwarzania danych osobowych – umowy o pracę, umowy cywilnoprawne,

Załącznik nr 3 wzór Cofnięciu upoważnienia do przetwarzania danych osobowych.

Załącznik nr 4 wzór Oświadczeniu o zachowaniu poufności

Załącznik nr 5 wzór klauzuli informacyjnej dla osoby fizycznej – art. 13 RODO

Załącznik nr 6 wzór klauzuli informacyjnej dla osoby fizycznej – art. 14 RODO

Załącznik nr 7 wzór klauzuli informacyjnej dla osoby fizycznej –członka WSDU

Załącznik nr 8 wzór klauzuli informacyjnej dla osoby fizycznej działającej w imieniu innego niż osoba fizyczna podmiotu– art. 13 RODO

Załącznik nr 9– wzór umowy powierzenia przetwarzania danych

Załącznik nr 10 wzór ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 11 wzór Rejestr umów powierzenia danych