

POLITYKA OCHRONY DANYCH
W STOWARZYSZENIU RADOŚĆ W DĘBICY

opracowana zgodnie z 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).

Inspektor Ochrony Danych:

imię i nazwisko: Piotr Wysowski

Obowiązuje od: 07.09.2022

Zatwierdzono:

Spis treści

DEFINICJE	4
ZAKRES STOSOWANIA	7
OBYWIAZKI OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE	7
OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH	8
CHARAKTERYSTYKA ZBIORÓW DANYCH OSOBOWYCH	9
ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH	9
PLAN KONTROLI	10
SPOSÓB UDZIELANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH:	11
ZBIERANIE DANYCH OSOBOWYCH:	12
OBYWIAZEK INFORMACYJNY	12
INFORMOWANIE O PRZETWARZANYCH DANYCH OSOBOWYCH.	14
POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH.	14
UDOSTĘPNIENIE DANYCH OSOBOWYCH.	15
ODMOWA UDOSTĘPNIENIA DANYCH	15
PRZEKAZANIE DANYCH DO PAŃSTWA TRZECIEGO LUB ORGANIZACJI MIĘDZYNARODOWEJ.	15
WYKAZ ZAŁĄCZNIKÓW	17

§ 1

AKTY PRAWNE

1. 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; RODO) z dnia 27 kwietnia 2016 r. (Dz.Urz.U.E.L Nr 119).
2. Konstytucja RP z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 z późn. zm.).
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 z późn. zm.; UoODO).

§ 2

CEL

1. Celem niniejszego dokumentu jest wprowadzenie spójnych zasad ochrony i bezpieczeństwa danych osobowych, ustalanie zasad, procedur i obowiązków w oparciu i zgodnie z 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; RODO), Konstytucją RP, ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000)
2. Celem nadrzędnym Polityki Ochrony Danych jest pomoc w zapewnieniu podstawowych zasad:
 - 1) zgodności przetwarzania danych z prawem, rzetelności i przejrzystości,
 - 2) ograniczenia celu,
 - 3) minimalizacji danych,
 - 4) merytorycznej poprawności,
 - 5) ograniczenia przechowywania,
 - 6) poufności i integralności,
 - 7) rozliczalności,
 - 8) innych zidentyfikowanych aktywów informacyjnych.
3. Polityka Ochrony Danych określa zasady zarządzania bezpieczeństwem ochrony danych osobowych i obejmujące zasady zarządzania systemem chroniącym dane oraz sposoby reagowania na zagrożenia.
4. Zastosowanie niniejszej Polityki Ochrony Danych powinno zapewnić wprowadzenie zabezpieczeń adekwatnych i proporcjonalnych do wyników szacowania ryzyka występującego dla przetwarzanych i przechowywanych danych w jednostce oraz w systemach informatycznych jednostki.
5. Polityka Ochrony Danych jest dokumentem przeznaczonym do użytku wewnętrznego w jednostce, obowiązującym w stosunku do zasad i reguł z obszaru ochrony danych osobowych.
6. Polityka Ochrony Danych zawiera procedury odpowiedzialności pracowniczej w zakresie naruszenia bezpieczeństwa ochrony danych oraz określa zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych. Każdy z pracowników, a także osób

mających dostęp do danych na podstawie stosunku cywilno- prawnego powinien zapoznać się z zasadami niniejszej Polityki.

7. Polityka Ochrony Danych służy zapewnieniu odpowiedniej wiedzy oraz procedur dotyczących sieci informatycznej w zakresie pojawiających się nowych zagrożeń oraz metod jej ochrony.

§ 3

DEFINICJE

Administrator Danych Osobowych (ADO)– Stowarzyszenie Radość w Dębicy (zamiennie: „Stowarzyszenie”) decydujące o celach i środkach przetwarzania danych osobowych;

Inspektor Ochrony Danych (IOD) - oznacza osobę powołaną przez ADO w Stowarzyszeniu, wpisaną do prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych rejestru.

Polityka – Polityka ochrony danych w Stowarzyszeniu Radość w Dębicy.

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);

UODO - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych-(Dz.U. z 2018 r. poz. 1000)

Kodeks Dobrych Praktyk - jest dokumentem wewnętrznym, którego celem jest podnoszenie, doskonalenie i wprowadzanie standardów w obszarze ochrony danych w naszej jednostce, a także podniesienie świadomości pracowników jednostki w zakresie dobrych praktyk obszaru ochrony danych.

Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Szczególna kategoria danych osobowych - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne; dane dotyczące stanu zdrowia

Dane biometryczne — dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne (art. 4 pkt 14 RODO);

Dane dotyczące zdrowia — dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia (art. 4 pkt 15 RODO);

Zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Upoważnienie- dokumenty wydany przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, może również określać identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;

Osoba upoważniona do przetwarzania danych osobowych – osoba, która otrzymała odpowiednie imienne upoważnienie od ADO i złożyła oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych;

Zgoda osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Odbiorca danych - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

Organizacja międzynarodowa - oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;

Strona trzecia - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

Użytkownik/pracownik (w tym podmiotu trzeciego) - osoba przetwarzająca dane na podstawie upoważnienia ADO w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w jednostce lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;

Naruszenie bezpieczeństwa ochrony danych – wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, obniżenia wymaganego poziomu poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet jeżeli nie prowadzą do negatywnych skutków dla organizacji. Zdarzenia lub działania, które mogą prowadzić do naruszenia praw lub wolności osób fizycznych;

Naruszenie ochrony danych osobowych - oznacza 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;

Przetwarzanie – oznacza operację 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;

Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby

fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

System informatyczny (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Nośnik komputerowy (wymienny) - nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dyski flash, pendrive;

Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

Zabezpieczenie systemu informatycznego - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

Zakład Aktywności Zawodowej (ZAZ) - Zakład Aktywności Zawodowej Stowarzyszenia Radość w Dębicy

Zasada integralności i poufności - oznacza przetwarzanie 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;

Zasada merytorycznej poprawności - oznacza, że dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

Zasada minimalizacji danych - oznacza, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

Zasada ograniczenia celu - oznacza, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

Zasada ograniczenia przetwarzania - oznacza, że 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą;

Zasada rozliczalności – ADO jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie;

Zasada zgodności z prawem, rzetelności i przejrzystości – oznacza przetwarzanie danych wyłącznie w przypadku spełnienia jednego ze wskazanych w RODO warunków (art. 6 i 9) oraz przekazanie osobie, której dane są pozyskiwane informacji określonych w art. 13 i 14.

§ 4

ZAKRES STOSOWANIA

Politykę stosują osoby przetwarzające dane osobowe i inne dane chronione, niezależnie od formy zatrudnienia w Stowarzyszeniu Radość lub Zakładzie Aktywności Zawodowej. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, wolontariusze oraz osoby realizujące zadania na podstawie podpisanej ze Stowarzyszeniem lub ZAZ umowy cywilnoprawnej, a także pracownicy i współpracownicy podmiotów trzecich, z którymi została zawarta umowa, na mocy której ww. osoby mają dostęp do informacji chronionych, w tym do danych osobowych.

1. Polityka ma zastosowanie do wszystkich danych osobowych oraz innych informacji podlegających ochronie, przetwarzanych w pomieszczeniach Stowarzyszenia niezależnie od formy ich przetwarzania. Polityka odnosi się do danych osobowych:

- 1) przetwarzanych w zbiorach tradycyjnych, w szczególności kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
- 2) przetwarzanych w systemach informatycznych.

2. Dla skutecznej realizacji Polityki ADO zapewnia:

- 1) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
- 2) kontrolę, monitoring i nadzór nad przetwarzaniem danych osobowych,
- 3) monitorowanie zastosowanych środków ochrony,
- 4) możliwość realizacji wytycznych, jeśli zostaną wskazane przez UODO.
- 5) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku;
- 6) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- 7) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

§ 5

OBOWIĄZKI OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

1. Każda osoba przetwarzająca dane osobowe na potrzeby Stowarzyszenia oraz ZAZ jest zobowiązana zapoznać się z treścią przedmiotowej Polityki oraz bezwzględnie stosować się do jej zapisów. Osoby przetwarzające dane osobowe czynią to na podstawie wydanego przez ADO - upoważnienia (załącznik nr 2 do niniejszej Polityki).
2. Użytkownicy/ pracownicy są zobowiązani są do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:
 - a. pisemnego wnioskowania o zewidencjonowanie nowych zbiorów danych osobowych w rejestrze czynności przetwarzania prowadzonego przez Inspektora Ochrony Danych,

- b. bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
 - c. występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,
 - d. zapoznania się i przestrzegania Kodeksu Dobrych Praktyk – stanowiącym załącznik nr 1.
3. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z RODO, czy UoODO, stosuje się przepisy tych ustaw.
4. Użytkownicy/pracownicy przetwarzający dane osobowe obowiązani są dołożyć należytej staranności w celu ochrony interesów osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:
 - a. przetwarzane zgodnie z powszechnie obowiązującym prawem i regulacjami wewnętrznymi,
 - b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
 - c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
 - d. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
 - e. oraz by wypełniany był obowiązek informacyjny, w przypadkach wskazanych w przepisach prawa powszechnie obowiązującego.
5. Naruszenie postanowień niniejszej Polityki może skutkować zablokowaniem dostępu użytkownika/ pracownika do informacji chronionych i systemów.
6. Każde naruszenie bezpieczeństwa w zakresie ochrony danych powinno być niezwłocznie zgłaszane ADO i IOD, a w przypadku naruszeń bezpieczeństwa dotyczących systemów informatycznych ADO i dodatkowo Informatykowi obsługującego Stowarzyszenie.
7. W razie wykrycia naruszenia ochrony danych osobowych każdy użytkownik/ pracownik ma obowiązek postępować zgodnie ze wskazaniem zawartymi w Procedurze postępowania w przypadku wystąpienia incydentu w zakresie bezpieczeństwa informacji i naruszenia danych osobowych w Stowarzyszeniu.
8. Osoby odpowiedzialne za zarządzanie kadrami w Stowarzyszeniu informują niezwłocznie ADO i/lub IOD o każdej zmianie w zakresie czynności użytkowników/ pracowników, która wiąże się ze zmianą zakresu uprawnień do przetwarzania danych osobowych.
9. Cofnięcie upoważnień do przetwarzania informacji chronionych powinno nastąpić niezwłocznie po zakończeniu wykonywania obowiązków użytkownika/ pracownika.

§ 6

OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

1. W Stowarzyszeniu Radość w Dębicy dane osobowe przetwarzane są w ramach zbiorów danych osobowych, wskazanych w rejestrze czynności przetwarzania.
2. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach z zachowaniem dedykowanego do tej czynności sprzętu oraz wszelkich innych urządzeń.

3. Wynoszenie zbiorów danych osobowych poza obszar przetwarzania możliwy jest za wyłączną zgodą Administratora Danych Osobowych.

§ 7

CHARAKTERYSTYKA ZBIORÓW DANYCH OSOBOWYCH

1. Rejestr czynności przetwarzania stanowi odrębny element składowy Polityki ochrony danych zgodnie z art. 30 RODO.
2. Przetwarzanie danych osobowych, zgodnie z celem działalności, jest możliwe, jeżeli jest to niezbędne do wypełnienia usprawiedliwionych interesów ADO, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Przetwarzanie jest również dozwolone, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych lub jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. W szczególności można przetwarzać dane osobowe, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, a także gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
3. Osoby przetwarzające zgromadzone dane są zobowiązane w szczególności do:
 - 1) przetwarzania danych zgodnie z aktami prawa powszechnie obowiązującego lub aktami prawa wewnętrznego, w zakresie zgodnym z upoważnieniem podpisanym przez ADO;
 - 2) przechowywania danych osobowych we właściwych zbiorach danych, zgodnie z celem utworzenia zbiorów;
 - 3) modyfikowania i usuwania danych, zgodnie z wnioskiem złożonym przez osobę, której dane dotyczą oraz ograniczenia przetwarzania danych.

§ 8

ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH

1. Zarząd Stowarzyszenia Radość odpowiada za zakres i bezpieczeństwo przetwarzania danych osobowych w Stowarzyszeniu.
2. Administrator Danych Osobowych jest odpowiedzialny za przestrzeganie przepisów RODO, UoODO i musi być w stanie wykazać ich przestrzeganie (tzw. zasada rozliczalności RODO).
3. **Administrator Danych Osobowych zapewnia:**
 - 1) przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
 - 2) zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu”);
 - 3) adekwatność danych osobowych, tj.: dane osobowe powinny być stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

- 4) prawidłowość danych osobowych i w razie potrzeby ich uaktualnianie; podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
 - 5) przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
 - 6) przetwarzanie 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 („integralność i poufność”).
4. Administrator Danych Osobowych zapewnia i stosuje odpowiednie środki informatyczne, techniczne i organizacyjne.
 5. ADO zapewniając ochronę przetwarzanych danych osobowych odpowiednią do wyników analizy ryzyka, a w szczególności
 - 1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych;
 - 2) podejmuje decyzje o technicznych i organizacyjnych zabezpieczeniach oraz wdraża zasady i procedury postępowania mające na celu zapewnienie adekwatnego poziomu bezpieczeństwa przetwarzanych danych;
 - 3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków;
 - 4) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych;
 - 5) zapewnia środki techniczne oraz organizacyjne w celu zapewnienia działań wymaganych przez przepisy prawa dotyczące ochrony danych osobowych;
 - 6) zapewnia realizację praw osób, których dane osobowe są przetwarzane (m.in. prawo wglądu, poprawiania danych i wniesienia sprzeciwu wobec przetwarzanych danych);
 - 7) Występuje w postępowaniach przed organami publicznymi oraz w kontaktach z podmiotami trzecimi w sprawach związanych z pozyskiwaniem, przetwarzaniem, ochroną i powierzeniem danych osobowych;
 - 8) analizuje dokumentację i sprawozdania przedstawione przez Inspektora Ochrony Danych, weryfikuje ocenę ryzyka i ocenę skutków związane z przetwarzaniem danych osobowych, a także decyduje o formach przeciwdziałania ewentualnym zagrożeniom;
 - 9) zapewnia bezpieczne usunięcie danych osobowych w przypadku uzasadnionego żądania niezwłocznego usunięcia danych osobowych, bez zbędnej zwłoki.

§ 9

PLAN KONTROLI.

IOD wprowadza i realizuje wewnętrzny plan kontroli, który w szczególności powinien obejmować weryfikację:

1. zabezpieczeń: organizacyjnych i technicznych zbiorów danych osobowych,
2. zawierać plan kontroli stanu wiedzy pracowników

3. plan szkoleń przypominających
4. weryfikację zgodność dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa powszechnie obowiązującego i stosowanymi w jednostce zabezpieczeniami organizacyjno- technicznymi.

§ 11

SPOSÓB UDZIELANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH:

1. Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby upoważnione przez Administratora Danych Osobowych.
- 2. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:**
 - 1) przed rozpoczęciem przetwarzania musi zapoznać się z wewnętrzną dokumentacją z zakresu ochrony danych osobowych oraz przepisami powszechnie obowiązującymi
 - 2) należy złożyć oświadczenie o zapoznaniu się z dokumentacją ochrony danych osobowych
 - 3) dane osobowe można przetwarzać wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych, w zawartym upoważnieniu i tylko w celu wykonywania obowiązków służbowych,
 - 4) zobowiązana jest do przestrzegania tajemnicy danych osobowych, która obowiązuje przez cały okres zatrudnienia lub trwania stosunku cywilnoprawnego, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji, przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres realizacji umowy, a także po zakończeniu jej realizacji,
 - 5) stosowanie określonych przez ADO procedur oraz wytycznych mających na celu przetwarzanie danych zgodnie z obowiązującym prawem,
 - 6) zabezpieczenie danych osobowych przed udostępnieniem osobom nieupoważnionym,
 - 7) za realizację procedury nadawania uprawnień odpowiedzialny jest IOD lub wyznaczona do tego osoba, którym należy zgłaszać zapotrzebowanie na udzielenie upoważnienia, zmianę jego zakresu lub konieczność cofnięcia upoważnienia.
3. Zakres dostępu do danych gromadzonych w systemie przypisany jest do niepowtarzalnych identyfikatorów użytkownika, niezbędnych do pracy w systemach oraz aplikacjach, do których użytkownik/pracownik otrzymał stosowne uprawnienia na podstawie podpisanego upoważnienia do przetwarzania danych,
4. W dokumentach/aktach osobowych użytkownika/pracownika przechowuje się egzemplarz oryginalny upoważnienia do przetwarzania danych osobowych podpisany własnoręcznie przez użytkownika/pracownika, co jednocześnie jest potwierdzeniem, że użytkownik/pracownik przyjął treść upoważnienia do wiadomości.
5. Rozwiązanie stosunku pracy, stosunku cywilnoprawnego lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych. Zakończenie współpracy z podmiotem trzecim powoduje wygaśnięcie upoważnienia do przetwarzania danych udzielonych pracownikom i współpracownikom tego podmiotu,
6. Upoważnienia do przetwarzania danych osobowych udzielane są również wolontariuszom, praktykantom oraz stażystom. Zakończenie stażu, praktyki, wolontariatu powoduje wygaśnięcie upoważnienia.

§ 12

ZBIERANIE DANYCH OSOBOWYCH:

- 1) Dane osobowe przetwarzane w Stowarzyszeniu oraz ZAZ mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą lub z innych źródeł. W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy upewnić się, że istnieje podstawa prawna przetwarzania danych.
- 2) Przetwarzanie i przechowywanie danych osobowych powinno odbywać się w postaci umożliwiającej identyfikację osób, których dotyczą.
- 3) Przetwarzanie i przechowywanie danych osobowych powinno odbywać się nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.
- 4) Dane osobowe, które są zbierane powinny być merytorycznie poprawne.
- 5) Zakres danych osobowych, które są zbierane, powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.
- 6) Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy odpowiedni przepis prawa wymaga ich archiwizacji przez określony czas.
- 7) Przetwarzanie danych osobowych kandydata do pracy jest możliwe podczas procesu rekrutacji wyłącznie po uzyskaniu jego pisemnego oświadczenia zawierającego zgodę na przetwarzanie jego danych osobowych w celu przeprowadzenia procesu rekrutacyjnego lub przyszłych procesów rekrutacyjnych. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu procesu rekrutacji dokumenty zawierające dane osobowe kandydatów do pracy są archiwizowane zgodnie z zapisami tych przepisów.
- 8) Zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 13

OBOWIĄZEK INFORMACYJNY

Administrator Danych Osobowych zobowiązany jest na etapie gromadzenia danych (niezależnie od tego, czy zbiera je bezpośrednio od osób, których one dotyczą, czy też pozyskania ich od podmiotu trzeciego) powiadomić osoby, których dane gromadzi o przysługujących im prawach oraz przekazać informacje o zasadach i celu przetwarzania danych osobowych (wypełnienie „obowiązków informacyjnych” wskazanych w art. 12, 13, 14, 22 i 25 RODO),

Zgodnie z art. 13 ust. 1 i 2 RODO, 14 do niezbędnych elementów informacyjnych zaliczyć należy podanie:

- 1) nazwy i adresu Administratora Danych Osobowych oraz adresu poczty elektronicznej i numeru telefonu oraz gdy ma to zastosowanie, tożsamości i danych kontaktowych przedstawiciela Administratora,
- 2) danych kontaktowych Inspektora Ochrony Danych,
- 3) celu przetwarzania danych osobowych oraz podstawy prawnej przetwarzania,
- 4) informacji o odbiorcach danych osobowych lub o kategoriach odbiorców,
- 5) informacji o zamiarze transferu danych osobowych do państwa trzeciego, ze szczególnym uwzględnieniem: przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, stwierdzenia lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub - w przypadku przekazania, o którym mowa w art. 46, art.

47 lub art. 49 ust. 1 akapit drugi RODO - wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,

- 6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
- 7) informacji o prawie do żądania od Administratora Ochrony Danych 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;
- 8) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
- 9) informacji o prawie wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych
- 10) informacji 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;
- 11) **W przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO, informacja powinna być poszerzona o:**
 - a) kategorie odnośnych danych osobowych;
 - b) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.
 - c) Informacje, o której mowa w pkt b każdorazowo należy przekazać indywidualnie osobie, której dane dotyczą przed podjęciem działań z jej danymi, a także dokumentować (najlepiej na piśmie podpisanym przez osobę, której dane dotyczą), że obowiązek informacyjny został wypełniony. Jeśli zamiast formy papierowej do gromadzenia danych wykorzystuje się system informatyczny to musi on zapewniać zapisanie w trwałej i wiarygodnej formie, że osoba podająca swoje dane za jego pomocą uzyskała informacje w zakresie określonym w przepisach prawa powszechnie obowiązującego.
 - d) Klauzula powinna być zrozumiała dla osób, których dane mają być gromadzone i przetwarzane.
 - e) Poświadczenie wykonania obowiązku informacyjnego może polegać na wypełnieniu odpowiednich formularzy (w tym w formie elektronicznej). Istotne jest, aby pola potwierdzające wyrażenie zgody na zbieranie i przetwarzanie danych w formularzu nie były domyślnie zaznaczane.
- 12) Treść klauzuli należy skonsultować każdorazowo z Inspektorem Ochrony Danych w celu potwierdzenia zgodności z obowiązującymi przepisami prawa powszechnie obowiązującego.
- 13) Informowanie powinno się dokonać bez prośby zainteresowanego. Powinno być ono wykonane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy uwzględnić także to, że informowana osoba musi mieć możliwość wniesienia sprzeciwu wobec przetwarzania jej danych i należy stworzyć jej warunki do wyrażenia tego sprzeciwu.
- 14) Wykonanie obowiązku informacyjnego jest zadaniem osoby przyjmującej dane osobowe, która po otrzymaniu potwierdzenia jego wykonania (w przypadku, gdy realizowany jest on w formie papierowej) przekazuje dowód wykonania obowiązku informacyjnego do Inspektora Ochrony Danych.

§ 13

INFORMOWANIE O PRZETWARZANYCH DANYCH OSOBOWYCH.

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych przez Stowarzyszenie Radość w Dębicy, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.
2. Na wniosek osoby, której dane dotyczą, Administrator Danych Osobowych jest zobowiązany do udzielania informacji. Informacja powinna być udzielona formie pisemnej oraz powszechnie zrozumiałej.
3. W razie wniesienia żądania oraz wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych osobowych, bez zbędnej zwłoki, powinien dokonać uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.
4. Osoba, której dane dotyczą, ma prawo wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach przetwarzania niezbędnego do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnego dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

§ 14

POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH.

1. Administrator Danych Osobowych:
 - 1) przekazuje dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego, w szczególności do: Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Państwowej Inspekcji Pracy, sądów powszechnych, Policji i Prokuratury, komorników.
 - 2) powierza przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej na piśmie, która określa zasady przetwarzania i zabezpieczenia danych osobowych.
2. Umowa powierzenia danych osobowych do przetwarzania musi być zawarta w formie pisemnej w dwóch jednobrzmiących egzemplarzach dla obu stron.
3. W przypadku zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem trzecim, ADO jednocześnie zobowiązuje ten podmiot w formie pisemnej do zachowania poufności powierzanych do przetwarzania danych osobowych oraz sposobów ich zabezpieczeń. Zobowiązanie powinno pozostać w mocy również po zakończeniu przetwarzania.
4. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.
5. Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednio ryzyka dla danych objętych ochroną, a w szczególności powinien stosować techniczne i organizacyjne środki bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

§ 15

UDOSTĘPNIENIE DANYCH OSOBOWYCH.

1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
 - 1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
 - 2) na podstawie umowy z innym podmiotem, w ramach, której istnieje konieczność udostępnienia danych;
 - 3) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o realizację praw powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi **załącznik nr 4** do Polityki.
4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na piśmie wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
6. Wniosek o udostępnienie przekazywany jest do właściciela zasobów danych osobowych, który podejmuje decyzję o udostępnieniu, i informuje o tym IOD.
7. Użytkownik/pracownik zasobów danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

§ 16

ODMOWA UDOSTĘPNIENIA DANYCH

Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałyby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy, a także gdy brak jest podstawy prawnej do udostępnienia danych.

§ 17

PRZEKAZANIE DANYCH DO PAŃSTWA TRZECIEGO LUB ORGANIZACJI MIĘDZYNARODOWEJ.

- 1) Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to 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.

- 2) W razie braku decyzji, o której mowa w pkt 1 Administrator Danych Osobowych lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowane prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.
- 3) W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w pkt 1 oraz braku odpowiednich zabezpieczeń, o których mowa w pkt 2, w tym wiążących reguł, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:
 - a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,
 - b) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przed umownych podejmowanych na żądanie osoby, której dane dotyczą,
 - c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną,
 - d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
 - e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,
 - f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody lub przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.
5. Szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej określone zostały określone w RODO. O wyrażenie zgody na przekazanie danych występuje właściciel zbioru, wskazując cel i zakres przekazywanych danych. Zgodę na ich przekazanie do państwa trzeciego lub organizacji międzynarodowej może wydać ADO po zasięgnięciu opinii Inspektora Ochrony Danych. ADO zobowiązany jest bezwzględnie przestrzegać postanowień RODO przy przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.

Niniejsza Polityka Ochrony Danych w Stowarzyszeniu Radość w Dębicy wchodzi w życie z dniem **07.09.2022 r.** i obowiązuje na wszystkich stanowiskach oraz we wszystkich obszarach, gdzie dochodzi do przetwarzania informacji podlegających ochronie.

Właścicielem niniejszego dokumentu jest ADO, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację niniejszego dokumentu.