Polityka Ochrony Danych Osobowych

Administrator Danych:

Stowarzyszenie Świętokrzyskie

Wodne Ochotnicze Pogotowie Ratunkowe

ul. Zagórska 182 a

25-362 Kielce

§1

Postanowienia Ogólne

1. Polityka Ochrony Danych Osobowych jest dokumentem opracowanym i wdrożonym w Stowarzyszeniu Świętokrzyskie Wodne Ochotnicze Pogotowie Ratunkowe, (dalej: Stowarzyszenie) w celu zapewnienia przestrzegania zasad ochrony danych osób fizycznych, które są przez nie przetwarzane oraz opisu stosowanych środków technicznych i organizacyjnych, mających na celu zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną.

2. Stowarzyszenie Świętokrzyskie Wodne Ochotnicze Pogotowie Ratunkowe jest administratorem danych osób fizycznych, które są przetwarzane w ramach prowadzonej przez Stowarzyszenie działalności.

3. Mając na uwadze zgodne z prawem przetwarzanie danych osobowych członków Stowarzyszenia, byłych członków, współpracowników, pracowników, kontrahentów oraz innych osób fizycznych, Stowarzyszenie zwane dalej także Administratorem Danych, wprowadza do stosowania niniejszą Politykę Ochrony Danych Osobowych. Niniejsza Polityka stanowi politykę ochrony danych w rozumieniu art. 24 ust. 2 RODO.

4. Stowarzyszenie zapewnia, że:

a) nie prowadzi przetwarzania danych, które wiązałoby się z wysokim ryzykiem naruszenia praw lub wolności osoby fizycznej;

b) uwzględnia ochronę danych w fazie projektowania oraz stosuje domyślną politykę ochrony tam, gdzie ma to zastosowanie;

c) respektuje prawa osoby, której dane dotyczą, w szczególności prawa dostępu do danych, sprostowania danych, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu, zgodnie z aktualnie obowiązującymi przepisami prawa;

d) jeśli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to przed rozpoczęciem przetwarzania dokona oceny skutków dla planowanych operacji przetwarzania danych osobowych.

5. Administrator danych przeprowadził analizę i nie wyznaczył Inspektora Ochrony Danych. Analiza stanowi Załącznik nr 1 do niniejszej Polityki Ochrony Danych.

6. Pracownicy i współpracownicy Stowarzyszenia są zobowiązani do zapoznania się z obowiązującymi procedurami i instrukcjami, a także stosowania tych zasad.

§2

Definicje

1. Administrator Danych - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszym dokumencie rozumie się przez to Stowarzyszenie Świętokrzyskie Wodne Ochotnicze Pogotowie Ratunkowe.

2. 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.

3. Dane osobowe zwykłe - to dane osobowe, które określają podstawowe dane identyfikujące osobę fizyczną. Mogą być to takie dane, jak imię i nazwisko, data urodzenia, numer PESEL, adres zamieszkania, adres e-mail, numer telefonu.

4. Dane osobowe szczególnie chronione – to np. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, stan zdrowia i wszelkie informacje dotyczące zdrowia psychicznego lub fizycznego, kod genetyczny, dane genetyczne i biometryczne, nałogi lub życie seksualne.

5. Ustawa – oznacza ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych.

6. RODO - oznacza 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).

7. 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. Zbiór może być prowadzony w formie papierowej lub w systemie informatycznym.

8. Przetwarzanie danych – 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. Zasady określone w niniejszej polityce należy stosować przy każdej operacji na danych.

9. Powierzenie danych osobowych – przetwarzanie danych osobowych w imieniu administratora.

10. Udostępnienie danych - przekazanie danych osobowych innemu administratorowi danych na podstawie odpowiednich przepisów prawa.

11. Osoba upoważniona - osoba upoważniona przez Administratora Danych do przetwarzania danych w celu i zakresie określonym w upoważnieniu. Osobą upoważnioną może być osoba zatrudniona na podstawie umowy o pracę, umowy cywilnoprawnej, stażysta lub wolontariusz.

12. Państwo trzecie - państwo nienależące do Europejskiego Obszaru Gospodarczego.

13. System informatyczny – zespół powiązanych ze sobą środków technicznych (urządzenia komputerowe, drukujące, oprogramowanie), zabezpieczeń, sieć informatyczna i udostępniane przez nią zasoby.

14. Użytkownik – osoba upoważniona przez Administratora Danych, przetwarzająca dane osobowe w systemie informatycznym na podstawie przydzielonych jej uprawnień.

15. IOD lub Inspektor – w niniejszej Polityce IOD lub Inspektor oznacza inspektora ochrony danych, o którym mowa w art. 37 RODO, jeżeli został powołany lub jeżeli istnieje prawny obowiązek jego powołania, lub inną osobę wyznaczoną przez Administratora do zapewnienia zgodności z ochroną danych w pozostałych przypadkach. W przypadku niepowołania IOD, obowiązki przypisane IOD w Polityce wykonuje Administrator.

16. Organ Nadzorczy – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie w celu monitorowania stosowania RODO, zgodnie z art. 51 RODO, w tym Prezes Urzędu Ochrony Danych Osobowych.

§3

Zadania i obowiązki Administratora Danych

1. Administrator Danych decyduje o celach i sposobach przetwarzania danych. Do jego obowiązków należy w szczególności:

a) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane dotyczą;

b) stosowanie środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;

c) nadzorowanie i kontrolowanie wdrożonych do stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii tych danych, w szczególności zabezpieczających dane przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, utratą, zmianą, uszkodzeniem lub zniszczeniem;

d) kontrola nad tym, kto i w jakim zakresie ma dostęp do danych,

e) respektowanie praw osób, których dane dotyczą, w szczególności prawa dostępu do treści danych oraz och poprawiania, a także prawa do przenoszenia danych, prawa do wstrzymania przetwarzania danych ze względu na szczególną sytuacją osoby - na podstawie obowiązujących przepisów prawa.

f) spełnienie obowiązku informacyjnego wobec osoby, której dane dotyczą, zgodnie z aktualnie obowiązującymi przepisami;

g) zapewnienia zapoznania pracowników i współpracowników, zgodnie z obowiązującymi przepisami prawa, z zasadami ochrony danych osobowych.

§4

Zadania i obowiązki osób upoważnionych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, które posiadają imienne upoważnienie nadane przez Administratora Danych. Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 2 do niniejszej Polityki.

2. Upoważnienie wydawane jest przez Administratora Danych w celu i zakresie wynikającym z zadań i obowiązków służbowych.

3. Upoważnienie wydawane jest przed rozpoczęciem o przetwarzania danych osobowych na czas trwania umowy o pracę lub innej umowy cywilnoprawnej, a także na czas wykonania określonego zadania, które związane jest z przetwarzaniem danych.

4. Osoba upoważniona do przetwarzania danych osobowych składa pisemne oświadczenia o zobowiązaniu do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Wzór oświadczenia osoby upoważnionej do przetwarzania danych osobowych stanowi Załącznik nr 3 do niniejszej Polityki.

5. Osoba upoważniona do przetwarzania danych jest zobowiązana do:

a) przetwarzania danych osobowych zgodnie z upoważnieniem wydanym przez Administratora Danych;

b) stosowania się do instrukcji i procedur zawartych w dokumentacji przetwarzania danych, wydanych przez Administratora Danych;

c) stosowania wprowadzonych środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione;

d) umożliwienia przeprowadzenia czynności w toku sprawdzenia planowanego lub doraźnego prowadzonego przez Administratora Danych lub na jego zlecenie;

e) sprawowania nadzoru nad obiegiem oraz przechowywaniem i zabezpieczeniem dokumentów zawierających dane osobowe, do których ma dostęp w chwili wykonywania czynności służbowych;

f) każdorazowego niezwłocznego informowania Administratora Danych w sytuacji naruszenia ochrony danych osobowych lub uzasadnionego podejrzenia takiego naruszenia.

§5

Zadania Inspektora Ochrony

Do zadań Inspektora Ochrony Danych, zgodnie z art. 39 ust. 1 Ogólnego rozporządzeniem o ochronie danych należy w szczególności:

a) informowanie kierownika jednostki organizacyjnej oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy aktualnie obowiązujących przepisów o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Ogólnego rozporządzeniem o ochronie danych, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

f) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Ogólnego rozporządzeniem o ochronie danych.

Administrator podjął decyzję o niewyznaczeniu Inspektora Ochrony Danych.

§6

Ogólne zasady przetwarzania danych osobowych

1. Stowarzyszenie przetwarza dane osobowe wyłącznie, gdy jest to dopuszczone aktualnie obowiązującymi przepisami prawa.

2. Dane osobowe mogą być przetwarzane wyłącznie w celu i zakresie, w jakim zostały zgromadzone, a także nie dłużej niż jest to niezbędne dla osiągnięcia tego celu.

3. Dane osobowe po wykorzystaniu są niezwłocznie usuwane lub przechowywane wyłącznie w postaci uniemożliwiającej identyfikację osób, których dotyczą, o ile przepisy odrębnych ustaw nie precyzują określonego czasu przechowywania danych.

4. Dane osobowe są przetwarzane przez Stowarzyszenie, gdy:

a) Administrator Danych uzyskał zgodę osoby, której dane dotyczą;

b) jest to niezbędne do wykonania umowy, której strona jest osobą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;

c) jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych osobowych;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

5. Administrator Danych może powierzać dane innym podmiotom państwa trzeciego poza obszarem Europejskiego Obszaru Gospodarczego zgodnie z przepisami ogólnego rozporządzenia o ochronie danych osobowych (RODO).

6. Administrator Danych przetwarza szczególne kategorie danych, tzw. dane wrażliwe, gdy jest to niezbędne do wypełnienia obowiązków statutowych i ustawowych ciążących na administratorze, wyłącznie w granicach określonych przepisami prawa.

Administrator przetwarza dane szczególnych kategorii tylko gdy:

a) wyraźna zgoda- osoba, wyraziła wyraźną zgodę na przetwarzanie tych danych

b) prawo pracy i ubezpieczenia społeczne- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, na podstawie przepisu prawa lub porozumienia zbiorowego

c) dane upublicznione- przetwarzanie dotyczy danych w sposób oczywisty upublicznionych przez osobę

d) roszczenia-przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń

e) przepis prawa. na podstawie prawa państwa członkowskiego lub UE

f) medycyna pracy i leczenie- gdy przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, diagnozy, leczenia etc.

g) w innych przypadkach wymienionych w art. 9 ust. 2 RODO, np. ochrona żywotnych interesów, działalność fundacji, stowarzyszeń i innych podmiotów niezarobkowych, zdrowie publiczne.

7. Przetwarzanie danych karnych jest dopuszczalne jedynie na podstawie konkretnego przepisu prawa lub zezwolenia lub innej decyzji uprawnionego organu oraz pod warunkiem istnienia jednej z podstaw prawnych przetwarzania, o której mowa w art. 6 RODO.

8. W ramach wykonywania działalności, Administrator przetwarza dane szczególnych kategorii, w tym w szczególności dane dotyczące zdrowia pracowników lub kandydatów do pracy. Jeżeli Administrator ustali, że zwykle w ramach swojej działalności przetwarza dane szczególnych kategorii lub dane karne w innych sytuacjach niż jako Pracodawca:

a) Administrator zweryfikuje, czy zachodzą przesłanki dopuszczalności przetwarzania takich danych, o których mowa powyżej.

b) W razie braku podstawy przetwarzania Administrator zaprzestaje przetwarzania pozbawionego podstawy i postanawia o usunięciu danych, ewentualnie uzupełnia brakującą podstawę prawną (np. uzyskuje stosowne zgody).

c) W celu uniknięcia niezgodnego z prawem przetwarzania danych szczególnych kategorii Administrator zwraca Personelowi szczególną uwagę na postanowienia Polityki dotyczące danych szczególnych kategorii, a jeżeli uzna to za potrzebne, określa dodatkowe instrukcje dla Personelu, a co najmniej na przykład Administrator wskazuje, że przy ocenie zasadności udzielenia urlopu w związku ze złym stanem zdrowia członka rodziny nie należy żądać informacji, kogo dotyka zły stan zdrowia ani przede wszystkim, na czym konkretnie polega, bez wyraźnej zgody osoby, na której stan zdrowia powołuje się członek Personelu. W razie mimowolnego uzyskania takich informacji, nie należy ich dalej przetwarzać. Nawet w przypadku, gdy dane szczególnych kategorii zostały podane przez osobę z własnej woli, Administrator prosi o wyrażenie przez nią wyraźnej zgody na przetwarzanie tych danych, jeżeli zamierza takie dane wykorzystać.

9. Administrator identyfikuje sytuacje, w których może dojść do przypadkowego przetwarzania danych szczególnych kategorii lub danych karnych i podejmuje działania zapobiegające niezgodnemu z prawem przetwarzaniu. W szczególności Administrator odbiera pisemne oświadczenia i zobowiązania Personelu odpowiedzialnego za odbieranie korespondencji przychodzącej co do (i) zachowania w poufności i nieprzekazywania informacji o korespondencji zawierającej Dane Szczególnych Kategorii i Danych Karnych nikomu oprócz jej adresata, (ii) o środkach zabezpieczających, jakie należy podjąć dla ochrony takiej korespondencji, (iii) o odpowiedzialności

dyscyplinarnej i karnej za nieautoryzowane rozpowszechnianie lub wykorzystanie danych szczególnych kategorii lub danych karnych.

10. W przypadku, gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

11. Administrator Danych stosuje ogólne zasady przetwarzania danych osobowych, tj.:

a) zasadę zgodności z prawem, rzetelności i przejrzystości - dane mogą być przetwarzane, jeśli Administrator Danych będzie dysponował przynajmniej jedną z przesłanek przetwarzania wskazanych w obowiązujących przepisach prawa;

b) zasadę celowości - dane przetwarza tylko dla zgodnych z prawem celów i nie poddaje dalszemu przetwarzaniu niezgodnemu z tymi celami;

c) zasadę ograniczonego celu- przetwarzane dane niezbędne ze względu na cel zbierania danych, nie zbiera danych na tzw. zapas.

d) zasadę prawidłowości - zapewnia się, aby dane były zgodne z prawdą, kompletne i aktualne;

e) zasada ograniczenia przechowywania- dane nie są przetwarzane dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania lub uregulowane obowiązującymi przepisami;

f) zasada minimalizacji- dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

g) zasadę integralności i poufności - dane przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych, w tych ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Administrator jest odpowiedzialny za przetwarzanie danych zgodnie w/w zasadami i jest w stanie wykazać ich przestrzeganie (zasada rozliczalności).

§7

Obszar przetwarzania danych osobowych i jego ochrona

1. Obszarem przetwarzania u Administratora Danych obejmuje się wszystkie pomieszczenia, w których wykonuje się jakiekolwiek operacje na danych osobowych, w szczególności wprowadza się, modyfikuje, archiwizuje, usuwa dane, a także wszystkie miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe.

2. W celu ochrony obszaru przetwarzania przed dostępem osób nieupoważnionych Administrator Danych stosuje kontrolę politykę kluczy zabezpieczając w ten sposób budynki lub pomieszczenia, w których przetwarza się dane osobowe.

3. Dostęp do pomieszczenia, w którym dane osobowe są przetwarzane mogą mieć wyłącznie osoby upoważnione. Obecność innych osób może mieć miejsce wyłącznie pod nadzorem osoby upoważnionej.

5. W przypadku, gdy nie jest możliwe nadzorowanie pracy osób nieupoważnionych w obszarze przetwarzania Administrator Danych zapewnia zabezpieczenie danych osobowych, znajdujących się w danym pomieszczeniu, w taki sposób, aby nie było możliwe zabranie, zniszczenie lub jakikolwiek dostęp do tych danych.

§8

Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych.

1. W Stowarzyszeniu został ustalony sposób postępowania w przypadku stwierdzenia lub uzasadnionego podejrzenia naruszenia bezpieczeństwa danych osobowych, bez względu na formę przetwarzania danych. Wdrożono Procedurę naruszeń, która stanowi Załącznik nr 4 do niniejszej Polityki. Administrator Danych prowadzi rejestr naruszeń.

2. 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.

3. Do sytuacji naruszenia dochodzi w szczególności, gdy następuje:

a) wykorzystanie danych osobowych w celach niezgodnych z tym, dla którego zostały zgromadzone;

b) udostępnienie lub umożliwienie dostępu do danych osobowych osobom lub podmiotom do tego nieupoważnionym;

c) nieautoryzowany dostęp do danych, modyfikacje lub zniszczenie danych

d) pozyskiwanie danych z nielegalnych źródeł.

4. Wszystkie osoby upoważnione do przetwarzania danych osobowych są zobowiązane poinformować Administratora Danych o ewentualnych naruszeniach bezpieczeństwa ochrony danych osobowych lub uzasadnionych podejrzeniach wystąpienia takiego naruszenia.

5. Jeśli naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych Administrator Danych niezwłocznie, ale nie później, niż w ciągu 72h od chwili stwierdzenia naruszenia informuje o tym organ nadzorczy ochrony danych, a także osobę, której dane dotyczą, by umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych.

6. Sytuacjami ryzyka naruszenia praw lub wolności osób fizycznych są w szczególności takie możliwe negatywne konsekwencje, jak:

a) powstanie uszczerbku fizycznego osoby, której dane dotyczą;

b) szkody majątkowe lub niemajątkowe osoby fizycznej;

c) utrata kontroli nad własnymi danymi;

d) ograniczenie praw osoby fizycznej;

e) kradzież lub fałszowanie tożsamości;

f) naruszenie dobrego imienia, naruszenie poufności danych objętych tajemnicą zawodową;

g) inne szkody gospodarcze lub społeczne.

7. Naruszenia nie zgłasza się organowi nadzorczemu, ani osobie, której dane dotyczą, jeśli Administrator Danych będzie w stanie wykazać, że jest mało prawdopodobne, by doszło do naruszenia praw lub wolności osób fizycznych.

8. W przypadku naruszenia ochrony danych Administrator Danych, niezależnie od tego, czy nastąpiło naruszenia praw lub wolności osób fizycznych, przeprowadza sprawdzenie w celu określenia, dlaczego doszło do naruszenia i jakie środki zapobiegawcze wprowadzić.

§9

Obowiązek informacyjny

1. Każdej osobowe przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych u Administratora Danych.

2. Administrator Danych informuje osoby, której dane dotyczą, o swoich danych, adresie siedziby, celu zbierania danych, obowiązku lub dobrowolności ich podania, a także przekazuje inne informacje, które mogą być wymagane aktualnie obowiązującymi przepisami prawa.

3. Obowiązek informacyjny w przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą wykonywane jest przed rozpoczęciem ich zbierania danych. Osobę, której dane dotyczą informuje się o:

a) dokładnej nazwie i adresie swojej siedziby;

b) celu zbierania danych:

c) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej;

d) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.

e) innych informacjach, wynikających z aktualnych przepisów prawa:

- w jakim celu przetwarza dane na podstawie interesu prawnego administratora danych;

- czy ma zamiar przekazania danych do państwa trzeciego;

- podaje okres przez który dane będą przetwarzane, a gdy nie jest to możliwe to podaje kryteria ustalenia tego okresu;

- informacje o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych (jeśli przetwarzanie odbywa się na podstawie umowy lub zgody);

- jeśli przetwarzanie odbywa się na podstawie zgody osoby to informuje ją o prawie do cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

- o prawie wniesienia skargi do organu nadzorczego;

- o profilowaniu i jego konsekwencjach, jeśli jest to zasadne;

4. Powyższych informacji nie udziela się, jeśli osoba dysponuje już tymi informacjami, a Administrator Danych będzie w stanie to wykazać.

5. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych - poinformować ją dodatkowo o:

a) źródle danych

b) kategoriach danych osobowych.

6. Administrator Danych ma również na uwadze, że każda osoba, której dane dotyczą, może wystąpić z wnioskiem o otrzymanie informacji o jej danych, które są przetwarzane w zbiorze u Administratora Danych, zgodnie z obowiązującymi przepisami. Odpowiedź na zapytanie osoby, której dane dotyczą, jest udzielana na piśmie w terminie nieprzekraczającym miesiąca od daty wpłynięcia wniosku.

7. Wyłączenie obowiązku udzielenia odpowiedzi następuje wyłącznie w przypadkach, określonych aktualnie obowiązującymi przepisami prawa.

§10

Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych odbywa się wyłącznie na podstawie umowy zawartej na piśmie pomiędzy Administratorem Danych, a podmiotem trzecim, któremu dane się powierza w celu i zakresie wykonania konkretnej czynności w imieniu Administratora Danych.

2.Stowarzyszenie powierza przetwarzane dane osobowe osób fizycznych, w szczególności w celu:

a) korzystania z usług z zakresu BHP,

b) korzystania z usług dostawcy hostingu,

c) korzystania z usług biura kadrowo-księgowego.

3. Umowa powierzenia określa w szczególności cel i zakres powierzenia przetwarzania danych osobowych. Wzór umowy powierzenia stanowi Załącznik nr 5 do niniejszej Polityki

4. Administrator Danych powierza dane osobowe wyłącznie tym podmiotom, które gwarantują zastosowanie środków organizacyjnych i technicznych, zabezpieczających dane przed dostępem osób nieupoważnionych na zasadach określonych w przepisach prawa. Administrator stosuje zasady powierzenia przetwarzania oraz listę wymogów, jakie Podmiot Przetwarzający musi spełnić, które zostały opisane w dokumencie stanowiącym Załącznik nr 6 do niniejszej Polityki – „Lista kontrolna Oceny Podmiotu Przetwarzającego".

5. Administrator Danych sprawuje kontrolę nad tym w jakim zakresie i w jakim celu powierza dane osobowe. Prowadzi w tym celu ewidencję podmiotów, którym dane zostały powierzone do przetwarzania. Ewidencja podmiotów stanowi Załącznik nr 7 do niniejszej Polityki.

§11

Udostępnianie danych osobowych

1. Administrator Danych udostępnia dane osobowe przetwarzane w zbiorach danych wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na podstawie aktualnych przepisów prawa.

2. Dane osobowe mogą być udostępniane na podstawie:

a) wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa, w szczególności sąd, prokuratura, policja.

b) wniosku innej osoby lub podmiotu, na zasadach określonych w przepisach prawa.

3. Wszystkie osoby upoważnione, które otrzymają wniosek o udostępnienie danych, zobowiązane są do przekazywania go bezpośrednio do Administratora Danych, który podejmuje decyzję o udostępnieniu lub odmowie udostępnienia.

§12

Prawa jednostki

1. Przejrzystość oraz tryb korzystania z praw:

a) **Czytelność.** Administrator dokłada starań, aby przekazywane informacje oraz sposób (styl) komunikacji z osobami, których dane dotyczą były czytelne i zrozumiałe dla odbiorców.

b) **Ułatwianie.** Administrator ułatwia osobom, których dane dotyczą, wykonywanie przysługujących im praw związanych z przetwarzaniem ich danych poprzez działania takie jak np. zamieszczanie na stronie internetowej Administratora odpowiednich informacji lub odwołań (linków) do informacji o sposobie korzystania z przysługujących im praw, w tym o wymaganiach dotyczących identyfikacji, sposobach kontaktu.

c) **Terminowość.** Prawa jednostki wykonywane są przez Administratora w terminie jednego miesiąca. Wykonanie żądań wymagających większego wysiłku organizacyjnego może zostać przedłużone o dwa miesiące, za powiadomieniem osoby.
d) **Weryfikacja tożsamości.** Administrator weryfikuje tożsamość osób, chcących zrealizować swoje prawa związane z przetwarzaniem danych za pomocą dokumentów tożsamości lub innych dowodów wykazujących tożsamość osoby, takich jak uwierzytelniony email, uwierzytelniony adres pocztowy, hasło, dostęp do uwierzytelnionego numeru telefonu. Administrator nie polega wyłącznie na uwierzytelnieniu ustnym (podanie informacji – wiedzy o osobie).
e) **Prawa innych.** Realizując Prawa Jednostki, Administrator chroni prawa i wolności osób innych niż osoba, której dane dotyczą w ten sposób, że w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób, na przykład może skutkować nieuprawnionym ujawnieniem tajemnicy lekarskiej lub tajemnicy dokumentacji medycznej, Administrator może zwrócić się do wnioskodawcy w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową wykonania żądania.
f) **Ustawy szczególne.** Administrator nie ma prawa odmówić wykonania Prawa Jednostki, chyba że konkretny przepis wydany w granicach upoważnienia wynikającego z RODO wprost wyłącza dane uprawnienie osoby. W szczególności nie można odmówić pacjentowi wydania pierwszej – bezpłatnej kopii danych z powołaniem na ustawę o prawach pacjenta i Rzeczniku Praw Pacjenta
g) **Dokumentowanie.** Administrator dokumentuje obsługę Praw Jednostki postępując zgodnie z Załącznikiem nr 8 do niniejszej Polityki – Procedura Obsługi Praw Jednostki

§13

Rejestr czynności przetwarzania

1. Administrator Danych prowadzi rejestr czynności przetwarzania.
2. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych, czyli zasady rozliczalności.
3. Rejestr czynności prowadzony jest w formie elektronicznej.
4. Administrator udostępnia Rejestr na żądanie Organu Nadzorczego. Organ Nadzorczy w przypadku prowadzenia Kontroli Zewnętrznej w siedzibie Administratora ma prawo dostępu do sprzętu, gdzie prowadzony jest Rejestr, przeglądania Rejestru oraz sporządzania kopii czy wydruków obrazów z ekranu komputerowego.

§ 14

Odpowiedzialność osób przetwarzających dane osobowe

1. Wszyscy pracownicy i współpracownicy Stowarzyszenia są zobowiązani do przestrzegania zasad, instrukcji i procedur wprowadzonej dokumentacji przetwarzania danych osobowych.

2. Nieprzestrzeganie zasad ochrony danych osobowych może skutkować odpowiedzialnością każdej osoby, która dopuściła się naruszenia, na zasadach określonych w przepisach, a w szczególności, gdy:

a) przetwarza w zbiorze danych dane osobowe do których przetwarzania nie jest została upoważniona, których przetwarzanie jest zabronione lub niezgodne z celem zebrania danych;

b) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;

c) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw.

§ 15

Analiza ryzyka

1. W celu określenia odpowiednich środków bezpieczeństwa danych, Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii, a następnie przypisuje poszczególne poziomy zabezpieczeń w Rejestrze. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.
2. W związku z obowiązkiem przeprowadzenia analiz ryzyka przetwarzania danych Administrator zapewnia sobie odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
3. W ramach analizy ryzyka Administrator kategoryzuje aktywa, dane oraz czynności przetwarzania pod kątem ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. Metodyka analizy ryzyka stanowi Załącznik nr 9 Polityki.

§ 16
Współadministrowanie

1. Współadministrowanie zachodzi w sytuacji, gdy co najmniej dwóch Administratorów wspólnie ustala cele i sposoby przetwarzania. Administratorzy powinni mieć zbliżoną siłą przetargową oraz możliwości ustalania celów i sposobów przetwarzania danych.
2. Administrator weryfikuje przypadki, w których dochodzi do współadministrowania danymi. W przypadku współadministrowania danymi Administrator wraz z pozostałymi współadministratorami zawierają stosowną umowę o współadministrowanie oraz opracowują treść niezbędnych informacji dla osób – wzór klauzuli o współadministrowaniu zawarta jest w załączniku nr 10 do niniejszej Polityki. Umowa o współadministrowanie powinna być zawarta w formie dokumentowej i określać podział obowiązków w zakresie (i) odpowiedzialności za

poinformowanie o zbieraniu Danych (ii) obsługi Praw Jednostki, (iii) poziomu bezpieczeństwa. Ad Wzór Umowy o Współadministrowanie stanowi Załącznik nr 10 do niniejszej Polityki.

§17
Szkolenia

1. Administrator przeprowadza lub umożliwia przeprowadzanie szkoleń z zakresu przetwarzania danych w świetle RODO w celu budowania świadomości z zakresu ochrony danych wśród Personelu.

§18

Przegląd ochrony danych

1. Zaleca się, aby Administrator przeprowadzał co najmniej raz w roku przegląd w zakresie ochrony danych, należycie go dokumentując w postaci raportu lub w innej formie przyjętej u Administratora.

§19

Monitoring Organu Nadzorczego

1. Administrator prowadzi bieżący monitoring aktywności Organów Nadzorczych i Europejskiej Rady Ochrony Danych w zakresie wytycznych, orzecznictwa, kontroli i innych informacji dotyczących aktualnych wymagań prawych. Monitoring wymagań prawnych obejmuje w szczególności: (i) opublikowane oraz wchodzące w życie akty prawa powszechnie obowiązującego (ii) wytyczne oraz zalecenia Organów Nadzorczych (iii) wiążące wytyczne innych organów (np. Komisja Europejska, Europejska Rada Ochrony danych); (iv) kodeksy branżowe (v) wytyczne do certyfikacji (vi) udokumentowane dobre praktyki stosowania prawa (vii) istotne orzecznictwo sądów i trybunałów.

Lista załączników:

Załącznik nr 1- Analiza konieczności wyznaczenia IOD,
Załącznik nr 2- Upoważnienie do przetwarzania danych osobowych,
Załącznik nr 3- Oświadczenie o zachowaniu tajemnicy służbowej,
Załącznik nr 4- Procedura naruszeń,
Załącznik nr 5- Wzór umowy powierzenia,
Załącznik nr 6- Lista kontrola dla podmiotu przetwarzającego,

Załącznik nr 7- Ewidencja podmiotów przetwarzających,
Załącznik nr 8- Procedura obsługi praw jednostki,
Załącznik nr 9- Metodyka analizy ryzyka.
Załącznik nr 10-Umowa o współadministrowaniu.

……..……

podpis Administratora Danych