**POLITYKA BEZPIECZEŃSTWA I PRZETWARZANIA DANYCH OSOBOWYCH**

**Stowarzyszenia Compliance Polska**

1. Niniejsza Polityka Bezpieczeństwa iPrzetwarzania Danych Osobowych, zwana dalej Polityką, stanowi zbiór zasad   
   i regulacji ochrony danych osobowych w Stowarzyszeniu Compliance Polska z siedzibą w Warszawie, Al. Jerozolimskie 65/79 / 1724, 00-697 Warszawa, zwanym dalej Stowarzyszeniem. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).
2. Polityka zawiera opis zasad ochrony danych obowiązujących w Stowarzyszeniu.
3. Za wdrożenie, utrzymanie, nadzór i monitorowanie przestrzegania niniejszej Polityki jest odpowiedzialny Zarząd Stowarzyszenia, zaś za stosowanie niniejszej Polityki odpowiedzialni są:
   1. członkowie stowarzyszenia;
   2. współpracownicy świadczący usługi na podstawie umowy cywilno-prawnej;
   3. pracownicy,
   4. inne wyznaczone osoby.
4. Stowarzyszenie powinno zapewnić zgodność postępowania podmiotów przetwarzających dane osobowe z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Stowarzyszenie.
5. Użyte w niniejszej Polityce definicje oznaczają:
   1. Administrator Danych - Stowarzyszenie Compliance Polska z siedzibą przy Al. Jerozolimskich 65/79 / 1724, 00-697 Warszawa;
   2. Poufność danych - rozumie się przez to własność zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   3. Użytkownik - osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych.
   4. Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie.
   5. Uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

**§ 1   
Postanowienia ogólne**

1. Polityka dotyczy wszystkich danych osobowych przetwarzanych w Stowarzyszeniu, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych, na wniosek tych osób, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

**§ 2   
Dane osobowe przetwarzane przez Stowarzyszenie**

1. Administrator danych prowadzi rejestr czynności przetwarzania.
2. Rejestr jest narzędziem służącym do weryfikacji i rozliczania zgodności z ochroną danych.
3. Stowarzyszenie stale identyfikuje i weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze.
4. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.

**§ 3  
Zarządzanie bezpieczeństwem**

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w Stowarzyszeniu.
2. Wszystkie dane osobowe są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa na podstawie jednej z przewidzianych przepisami prawa podstaw dla przetwarzania danych.
3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   1. naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
   2. udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   3. niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   4. zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   5. przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
   6. spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
   7. naruszenie praw osób, których dane są przetwarzane.
4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik lub Podmiot przetwarzający zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do powiadomienia Administratora Danych o zdarzeniu niezwłocznie jednak nie później niż po upływie 3 godzin od powzięcia wiedzy o wystąpieniu zdarzenia.
5. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy zapewnienie, by:
   1. pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
   2. każdy z przetwarzających Dane osobowe był pisemnie upoważniony do ich przetwarzania,
   3. każda z tych osób zobowiązała się do zachowania danych osobowych przetwarzanych w Stowarzyszeniu w tajemnicy. Oświadczenie podlega włączeniu do akt pracownika lub dokumentów związanych z inną podstawą świadczenia usług.

**§ 4  
Powierzenie przetwarzania danych osobowych**

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi przepisami prawa.

**§ 5  
Realizacja praw jednostki**

1. Stowarzyszenie jest zobowiązane zapewnić gwarancje ochrony praw i wolności osób trzecich.
2. Stowarzyszenie dba o przejrzystość i sposób przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
3. Stowarzyszenie ułatwia osobom korzystanie z ich praw poprzez wszelkie działania prawem dozwolone.
4. Stowarzyszenie dokłada wszelkich starań w celu terminowej realizacji obowiązków względem tych osób.
5. Stowarzyszenie dokumentuje sposób realizacji obowiązków informacyjnych, zawiadomień i żądań osób.
6. Na żądanie osoby dotyczące dostępu do jej danych, Stowarzyszenie informuje osobę o przetwarzaniu jej danych oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących.
7. Stowarzyszenie niezwłocznie informuje osobę o rozpatrzeniu lub odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
8. Stowarzyszenie uzupełnia i aktualizuje dane, w tym na żądanie osoby. Stowarzyszenie ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych.
9. Na żądanie osoby, Stowarzyszenie usuwa dane, gdy:
   1. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
   2. dane były przetwarzane niezgodnie z prawem
   3. zgoda na ich przetwarzanie została cofnięta,
   4. brak jest podstawy prawnej przetwarzania,
   5. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   6. konieczność usunięcia wynika z realizacji obowiązku prawnego.

**§ 6  
Obowiązki informacyjne**

1. Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.
2. Stowarzyszenie informuje osobę o przetwarzaniu jej danych podczas pozyskiwania danych od tej osoby.
3. Stowarzyszenie informuje osoby o wszelkich operacjach przeprowadzanych na danych osobowych, w tym o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych,
4. Stowarzyszenie niezwłocznie zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

**§ 7  
Określenie środków niezbędnych dla zapewnienia prawidłowego przetwarzanych danych**

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności przetwarzanych danych.
2. Zastosowane środki ochrony, w tym techniczne i organizacyjne, powinny być adekwatne do stwierdzonego poziomu ryzyka, w tym:
   1. Wstęp do pomieszczeń, w których przetwarzane są dane osobowe, powinien być ograniczony jedynie do osób odpowiednio upoważnionych.
   2. Pomieszczenia powinny być zamykane na czas nieobecności Użytkowników, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
   3. Szafki, w których przechowywane są dokumenty zawierające dane osobowe powinny być zamykane.
   4. Usuwanie dokumentów zawierających dane osobowe powinno być przeprowadzane w niszczarce.
   5. Sieć powinna być odpowiednio zabezpieczona.
   6. Sprzęt komputerowy powinien być chroniony przed złośliwym oprogramowaniem.
   7. Urządzenia na których przechowywane są dane (komputer stacjonarny, urządzenia przenośne) powinny być zabezpieczone odpowiednimi hasłami.

**§ 8  
Postępowanie w przypadku naruszenia zasad ochrony danych osobowych**

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osoby fizycznej.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki - jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Administrator zawiadamia o incydencie także osobę, której dane dotyczą niezwłocznie.

**§ 9  
Postanowienia końcowe**

1. Przed dopuszczeniem do pracy/wykonania umowy przy przetwarzaniu danych osobowych, każdy pracownik/współpracownik zobowiązany jest do zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym z niniejszą Polityką.