POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W STOWARZYSZENIU „MUDITA" Z SIEDZIBĄ W KRAKOWIE

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Dokument określa zasady bezpieczeństwa przetwarzania danych osobowych, jakie powinny być przestrzegane i stosowane w Stowarzyszeniu „MUDITA" z siedzibą w Krakowie (dalej: Stowarzyszenie) przez pracowników, współpracowników oraz wolontariuszy, którzy biorą udział w przetwarzaniu danych osobowych, powierzaniu przetwarzania danych osobowych bądź w administrowaniu danymi osobowymi. Stosowanie zasad określonych w niniejszym dokumencie ma na celu uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe.
2. Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:
    a. rozporządzeniu 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;
    b. ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych oraz aktach wykonawczych do niniejszej ustawy.

§ 2

Ilekroć w Polityce jest mowa o:

1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, jak również sieciowe nośniki informacji (m. in. „chmury"), z których korzysta Stowarzyszenie, m. in. Google Workspace,
4) kartotece - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,
5) Administratorze Danych - rozumie się przez to Stowarzyszenie „MUDITA" z siedzibą w Krakowie,
6) Zarządzie - rozumie się przez to Zarząd Stowarzyszenia, działającego w imieniu Administratora Danych.
7) użytkowniku – rozumie się przez to osobę wyznaczoną przez Zarząd lub osobę przez niego upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadającą ustalony identyfikator i hasło; przez użytkowników rozumie się pracowników, współpracowników oraz wolontariuszy Stowarzyszenia,
8) pomieszczeniach - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

§ 3

1. Ochrona danych osobowych w Stowarzyszeniu jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, używane aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia gwarantują:
    a) poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
    b) integralność danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    c) rozliczalność - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
    d) integralność systemu - rozumie się przez to nienaruszalność systemu, niemożność jakiejkolwiek manipulacji,

e) uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 4

1. Realizację zamierzeń określonych w § 3 ust. 2 powinny zagwarantować następujące założenia:
   a) wdrożenie procedur określających postępowanie osób działających w Stowarzyszeniu przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych,
   b) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
   c) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych w postaci fizycznej lub w systemie informatycznym – stosownie do indywidualnego zakresu upoważnienia,
   d) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie,
   e) śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   a) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
   b) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmian zawartości danych, utratę całości lub części danych),
   c) naruszenie lub próby naruszenia integralności systemu,
   d) zmianę lub utratę danych zapisanych na kopiach zapasowych,
   e) naruszenie lub próby naruszenia poufności danych lub ich części,
   f) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   g) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   h) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach.
2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II
Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych

§ 6

Każdy nowo zaangażowany użytkownik - przed dopuszczeniem do dostępu do danych osobowych – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków realizowanych przez Stowarzyszenie.

§ 7

1. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu należy:
   a) zwracać szczególną uwagę przy wchodzeniu i wychodzeniu z obiektów użytkowanych przez Stowarzyszenie na podejrzane osoby lub samochody parkujące w pobliżu,
   b) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
   c) przestrzegać procedur i zasad bezpieczeństwa podczas przetwarzania danych w postaci elektronicznej w systemie informatycznym, w szczególności nie pozostawiać urządzeń, na których przetwarzane są dane, włączonych i bez nadzoru (tzw. polityka czystego biurka),
   d) przestrzegać zasad i procedur ochrony danych osobowych, w czasie czynności podejmowanych na rzecz Stowarzyszenia.

2. Użytkownicy zobowiązani są, w przypadku dokonania identyfikacji ewentualnych występujących zagrożeń, przedkładać Zarządowi propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.

§ 8

1. Kartoteki przechowywane są w przeznaczonych do tego miejscach, do których dostęp mają wyłącznie użytkownicy.
2. Użytkownicy, o których mowa w ust. 1, odpowiedzialni są za rzetelne prowadzenie kartotek, ich kompletność oraz ochronę.
3. Rejestr atrybutów użytkowników pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych prowadzi Zarząd.

ROZDZIAŁ III
Przetwarzanie danych osobowych

§ 9

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego oraz karotek odbywa się wyłącznie na obszarze albo na wskazanych urządzeniach wyznaczonych bądź wskazanych przez Administratora Danych.
2. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Danych.
3. Przetwarzanie danych osobowych w postaci fizycznej (dokumentacja zawierająca dane osobowe użytkowników oraz osób trzecich) odbywa się wyłącznie w pomieszczeniach wskazanych przez Zarząd.
4. Przetwarzanie danych osobowych w postaci elektronicznej (dane przetwarzane w systemie informatycznym) odbywa się wyłącznie w miejscach i w sposób wskazany przez Zarząd. Dostęp do systemu, jak również dostęp do poszczególnych plików oraz ich kategorii jest ograniczony wyłącznie do osób wskazanych przez Zarząd.

§ 10

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić, aby:

a) drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby,
b) wydawanie kluczy do pomieszczeń podlegało rejestracji, z jednoczesnym poświadczeniem przez osobę odbierającą, faktu otrzymania kluczy do pomieszczenia,
c) przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych.

§ 11

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy oraz Zarząd.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności co najmniej jednego użytkownika lub za zgodą Administratora Danych.

Rozdział IV
Kontrola przestrzegania zasad zabezpieczenia ochrony danych osobowych

§ 12

1. Zarząd sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych.
2. Zarząd może upoważnić wybraną przez siebie osobę trzecią do wykonywania określonych zadań, o których mowa w ust. 1.
3. Zarząd lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
4. Przedmiotem kontroli, o których mowa w ust. 3 powinno być w szczególności:
   a) funkcjonowanie zabezpieczeń systemowych,
   b) prawidłowo funkcjonowania mechanizmów kontroli dostępu do zbioru danych,
   c) funkcjonowanie zastosowanych zabezpieczeń fizycznych,
   d) zasady przechowywania kartotek,
   e) zasady i sposoby likwidacji (zniszczenia) oraz archiwizowania zbiorów archiwalnych.,

f) zasady dotyczące przyznawania i cofania dostępu do systemów informatycznych poszczególnym użytkownikom.

Rozdział V
Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 13

1. Przed przystąpieniem do wykonywania czynności użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz sprawdzić, czy na użytkowanych przez niego urządzeniach nie doszło do nieautoryzowanych aktywności, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Zarządu lub upoważnioną przez niego osobę.
3. Postanowienia ust. 2 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych, jak i w kartotekach.

§ 14

1. Do czasu ustalenia planu dalszych działań z Zarządem, zgłaszający:
   a) powstrzymuje się od rozpoczęcia lub kontynuowania czynności na rzecz Stowarzyszenia, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
   b) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
   c) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 15

1. Zarząd lub upoważniona przez niego osoba sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:
   a) dacie i godzinie powiadomienia,
   b) sytuacji, jaka zaistniała,
   c) podjętych działaniach i ich uzasadnieniu.

2. Kopia raportu przekazywana jest bezzwłocznie Zarządowi, w przypadku, gdy raport sporządzony został przez osobę upoważnioną przez Zarząd.

§ 16

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować czynności na rzecz Stowarzyszenia dopiero po otrzymaniu pozwolenia od Zarządu lub osoby przez niego upoważnionej.

§ 17

1. W przypadku zaginięcia komputera lub nośników pamięci, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem (zarówno własnym, jak i stanowiącym własność Administratora Danych) niezwłocznie powiadamia Zarząd lub upoważnioną przez niego osobę, a w przypadku kradzieży występuje o powiadomienie jednostki policji bądź prokuratury.
2. W sytuacji, o której mowa w ust. 1, Zarząd lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt.

ROZDZIAŁ VI
Postanowienia końcowe

§ 18

Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

§ 19

1. Zarząd jest obowiązany zapoznać z treścią Polityki każdego Użytkownika.
2. Użytkownik zobowiązany jest złożyć oświadczenie o tym, że został zaznajomiony z obowiązującą Polityką bezpieczeństwa.
3. Oświadczenia przechowywane są w aktach personalnych użytkownika.

§ 20

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO, ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktach wykonawczych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.