

Polityka bezpieczeństwa w Fundacji Dom Muzyka Seniora w Kątach

§1.

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Fundacji Dom Muzyka Seniora w Kątach ul. Brzozowa 24, 05-532 Baniocha.

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

Jednostka – Fundacja Dom Muzyka Seniora w Kątach ul. Brzozowa 24, 05-532 Baniocha.

- 1.** dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, 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;
- 2.** 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;
- 3.** Administrator - Fundacja Domu Muzyka Seniora w Kątach
- 4.** system informatyczny – system przetwarzania danych w Fundacji Dom Muzyka Seniora w Kątach wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,

5. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

§3.

- 1) Utrzymanie bezpieczeństwa przetwarzanych przez Jednostkę informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
- 2) Dane osobowe muszą być:
- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
 - zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
 - adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
 - 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;
 - 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;
 - przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

§4.

1. W systemie informacyjnym Jednostki przetwarzane są informacje służące do wykonywania

zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.

2. Politykę Bezpieczeństwa stosuje się do:

- 1) danych osobowych mieszkańców i ich opiekunów przetwarzanych w systemie informatycznym,
- 2) danych partnerów biznesowych,
- 3) wszystkich informacji dotyczących danych pracowników Jednostki, w tym danych osobowych personelu i treści zawieranych umów o pracę,
- 4) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
- 5) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
- 6) rejestru osób dopuszczonych do przetwarzania danych osobowych,
- 7) innych dokumentów zawierających dane osobowe.

3) Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Jednostki w szczególności do:

- 1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
- 2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
- 3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
- 4) Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, zleceniobiorcy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§5.

1. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

2. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, mogą być udostępnione jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
3. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§6.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

§7.

Za bezpieczeństwo danych osobowych Jednostki, odpowiadają:

- 1) Administrator Fundacja Dom Muzyka Seniora

§8.

Administrator zobowiązany jest do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
2. określenie pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
3. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
4. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,

5. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
6. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
7. określanie, które osoby i na jakich prawach mają dostęp do danych informacji,

§9.

1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§10.

Rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1) Zabezpieczenia fizyczne:

1. pomieszczenia zamykane na klucz,
2. szafy pancerne z zamkami,

2) Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:

3. przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
4. przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.

1) Zabezpieczenia organizacyjne:

5. osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Ochrony Danych Osobowych

§11.

Ustala się następującą Organizację pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:

- 1) w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
- 2) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
- 3) w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
- 4) po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

§12.

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

- 7) stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
- 8) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§13.

Każdy pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym, lub przetwarzanych w inny sposób, zobowiązany jest do niezwłocznego poinformowania o tym administratora tego systemu informatycznego.

§14.

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na

określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§15

1. Gdy Administrator stwierdzi lub uzyska informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:
 - 1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
 - 2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
 - 3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.
 - 4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.
 - 5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
 - 6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę

nieupoważnioną, tą samą drogą.

2. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych.
3. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
4. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
5. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
6. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne.

FUNDACJA
"DOM MUZYKA SENIORA"
Prezes Zarządu

Fundacja Dom Muzyka Seniora
Agnieszka Dublaszewska
Wiceprezes Zarządu

DOM MUZYKA SENIORA
Anna Skotlicka
p.o. DYREKTORA