Polityka bezpieczeństwa danych osobowych

Cieszyński Ośrodek Kultury „Dom Narodowy"

Rynek 12

43-400 Cieszyn

Zatwierdzenie dokumentu: 11.05.2017 r.

sporządził:	Janusz Dębowski	ABI/DPO/IOD/Audytor Janusz Dębowski .....
zatwierdził:	Administrator Danych	DYREKTOR COK "DOM NARODOWY" ..... mgr Monika Sikora Monkiewicz

Spis treści

1. Informacje ogólne

1.1. Dokument spełnia wymogi ustawy z dnia 29.08.1997 o ochronie danych osobowych (Dz. U. 2016 poz. 922), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 nr 100 poz. 1024).

1.2. Zakres stosowania polityki.

Polityka Bezpieczeństwa Danych Osobowych opisuje podstawowe zasady przetwarzania oraz ochrony danych osobowych przed skutkami zagrożeń wewnętrznych oraz zewnętrznych, będących działaniem świadomym lub wynikiem błędu.

Niniejsza polityka wskazuje zasady przetwarzania danych osobowych, niezależnie od tego czy są one w formie dokumentacji papierowej czy elektronicznej, bez względu na rodzaj i format zapisu. Zasady opisane w niniejszym dokumencie obowiązują wszystkie osoby zaangażowane w przetwarzanie danych osobowych w firmie Cieszyński Ośrodek Kultury „Dom Narodowy".

1.3. Na dokumentację przetwarzanie danych osobowych składają się:

a) Polityka bezpieczeństwa danych osobowych,

b) Instrukcja zarządzania systemem informatycznym,

c) Instrukcja postępowania na wypadek naruszenia bezpieczeństwa danych osobowych.

Dokumentacja przetwarzania danych obowiązuje wszystkich pracowników oraz współpracowników firmy Cieszyński Ośrodek Kultury „Dom Narodowy", oraz obejmuje wszystkie obszary działania, gdzie występują dane osobowe.

1.4. Administratorem Danych Osobowych (ADO) jest Cieszyński Ośrodek Kultury „Dom Narodowy".

1.5. Administrator Danych może powołać Administratora Bezpieczeństwa Informacji (ABI), który będzie w jego imieniu sprawować nadzór nad bezpieczeństwem danych osobowych. Zakres kompetencji ABI opisany jest w ustawie o ochronie danych osobowych. W przypadku nie powołania ABI Administrator Danych pełni jego obowiązki.

1.6. Administrator Danych może powołać Administratora Systemu Informatycznego (ASI), który będzie sprawować nadzór nad bezpieczeństwem sieci oraz systemów informatycznych. Zakres kompetencji ASI opisany jest w zakresie indywidualnym ASI (powołaniu, ustanowieniu, etc.).W przypadku nie powołania ASI Administrator Danych pełni jego obowiązki.

Przetwarzanie danych osobowych w firmie Cieszyński Ośrodek Kultury „Dom Narodowy" jest dozwolone pod warunkiem przestrzegania wymogów ustawy o ochronie danych osobowych, niniejszej polityki oraz pozostałej dokumentacji przetwarzania danych osobowych.

2. Terminy i definicje

Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922);

Administrator Danych – Administrator Danych Osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych;

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

Dane wrażliwe – dane określone w artykule 27 ustawy, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, dane dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

Przetwarzanie danych – jakiekolwiek operacja wykonywana na danych osobowych, taka jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza ta, która wykonuje się w systemach informatycznych;

Zbiór danych osobowych – to każdy posiadający strukturę zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

Bezpieczeństwo danych osobowych – zachowanie poufności, dostępności oraz integralności danych osobowych.

Dokumentacja bezpieczeństwa danych osobowych – dokument Polityki bezpieczeństwa danych Osobowych, Instrukcja zarządzania systemem informatycznym, polityki bezpieczeństwa informacji, regulaminy, procedury, instrukcje, formularze przyjęte do stosowania w firmie Cieszyński Ośrodek Kultury „Dom Narodowy" wskazujące reguły i zasady postępowania przy przetwarzaniu danych osobowych;

Hasło – co najmniej 8-znakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Użytkownik – jest to osoba zatrudniona na podstawie umowy, która przetwarza dane osobowe znajdujące się w zbiorach danych za pomocą systemu informatycznego;

Identyfikator użytkownika – jest to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych;

Incydent bezpieczeństwa – zdarzenia, czynności, zaniechania, zjawiska, które wskazują na możliwe naruszenie zasad ochrony opisanych w dokumentacji bezpieczeństwa danych osobowych, błędów zabezpieczeń, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem danych osobowych;

Zabezpieczenia – środki służące utrzymaniu bezpieczeństwa informacji, łącznie z politykami, procedurami, regulaminami, instrukcjami, lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;

Nośnik danych – przedmiot, urządzenie elektroniczne lub jego część, na której można zapisywać i odtwarzać informacje, np. papier, klisza, taśma, twardy dysk, płyta CD-ROM, pendrive, laptop, smartfon, itp.

3. Organizacyjne i techniczne środki ochrony bezpieczeństwa danych osobowych

3.1. W celu zabezpieczenia przetwarzania danych osobowych stosowane są następujące zasady:

3.1.1. Przetwarzanie danych osobowych jest dopuszczalne gdy:

a) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;

d) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;

e) 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;

f) nie narusza to praw i wolności osób, których dane są przetwarzane

3.1.2. Zasady gromadzenia danych osobowych.

a) zbierane dane osobowe mogą być wykorzystywane tylko do jasno oznaczonych celów, w granicach obowiązującego prawa,

g) zakres zbieranych danych musi być adekwatny do celu, w jakim są przetwarzane. nie wolno gromadzić informacji nadmiarowych,

h) po ustaniu celu przetwarzania powinny być one usunięte lub przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą,

i) gromadzenie danych wrażliwych jest zabronione, chyba że zostanie spełniony jeden z warunków:

- osoba, której dane dotyczą wyrazi na to pisemną zgodę,
- pozwalają na to obowiązujące przepisy prawa lub jest to konieczne do dopełnienia obowiązku prawnego,

3.1.3. Zbiory danych osobowych przetwarzanych w firmie Cieszyński Ośrodek Kultury „Dom Narodowy" podlegają rejestracji, na zasadach określonych w ustawie. Decyzję o konieczności rejestracji podejmuje ADO. Wszyscy pracownicy mają obowiązek zgłosić do ADO konieczność przetwarzania danych w nowych zbiorach. Zgłoszenie musi mieć miejsce przed rozpoczęciem gromadzenia danych.

3.1.4. Każdej osobie, której dane będą gromadzone w zbiorach przysługuje prawo do kontrolowania treści ich danych osobowych oraz ich poprawiania, jeśli dane te są nieaktualne lub błędne.

3.1.5. Na ADO spoczywa obowiązek informowania osób, których dane są lub będą przez niego przetwarzane o:

a) adresie swojej siedziby i pełnej nazwie;

b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

c) prawie dostępu do treści swoich danych oraz ich poprawiania;

d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

3.1.6. Udostępnienie danych podmiotom zewnętrznym może odbywać się tylko i wyłącznie w granicach prawa, na wniosek pisemny – chyba, że przepisy stanowią inaczej. Wniosek musi określać kto będzie odbiorcą danych, podstawę udostępnienia, zakres jaki ma zostać udostępniony. Decyzję o udostępnieniu podejmuje ADO, który prowadzi rejestr udostępnień.

3.1.7. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi jedynie na podstawie umowy powierzenia. Podmiot, który podejmuje się przetwarzania danych zobowiązany jest do zastosowania zabezpieczeń określonych w ustawie. Wzór umowy wskazany jest w załączniku nr 7 do niniejszej polityki.

3.1.8. Umowy powierzenia danych osobowych ewidencjonowane. Wzór ewidencji wskazany znajduje się w załączniku nr 8 do niniejszej polityki.

3.1.9. Naruszenie przepisów i zasad ochrony danych osobowych stanowi pogwałcenie obowiązków pracowniczych, które może być sankcjonowane zgodnie z przepisami prawa.

3.2. W celu zabezpieczenia przetwarzania danych osobowych stosowane są następujące zabezpieczenia organizacyjne:

3.2.1. Nośniki tradycyjne i elektroniczne zawierające dane osobowe muszą być zabezpieczone podczas użytkowania, transportu oraz przechowywania przed dostępem osób nieuprawnionych i kradzieżą.

3.2.2. Do przetwarzania danych osobowych dostęp mogą mieć jedynie osoby, które zostały do tego pisemnie upoważnione przez Administratora Danych Osobowych oraz zapoznane z wymogami ochrony danych osobowych. Przetwarzanie może odbywać się jedynie w zakresie wskazanym w upoważnieniu. Wzór upoważnienia został określony w załączniku nr 5 do niniejszej polityki. ADO prowadzi ewidencję osób upoważnionych wg. wzoru określonego w załączniku nr 6 do niniejszej polityki.

3.2.3. Osoby zatrudnione w firmie Cieszyński Ośrodek Kultury „Dom Narodowy" podpisują stosowne oświadczenia o zachowaniu poufności (zał. 5) oraz są informowani o monitorowaniu systemu informatycznego oraz nadzorowaniu przez pracodawcę korespondencji służbowej, przesyłanej drogą elektroniczną (zał. 9).

3.2.4. Stanowiska pracy, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych osobowych (np. interesanci albo inni pracownicy) - muszą być zaprojektowane w sposób, uniemożliwiający takim osobom wgląd do tych danych (polityka czystego biurka). Osoby nieupoważnione nie mogą pozostawać w obszarze przetwarzania danych bez nadzoru.

3.2.5. Przetwarzanie danych osobowych może być realizowane jedynie w obszarze zdefiniowanym w załączniku nr 1 do niniejszej polityki, określającym obszary przetwarzania danych osobowych.

3.2.6. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek poinformować ADO o wszelkich podejrzeniach wystąpienia incydentu bezpieczeństwa dotyczącego danych osobowych, zgodnie z „Instrukcją postępowania na wypadek incydentu bezpieczeństwa danych osobowych".

3.2.7. Upoważnieni, którzy przetwarzają dane w systemach informatycznych (użytkownicy), mają obowiązek znać i przestrzegać „Instrukcję zarządzania systemem informatycznym".

3.3. W celu ochrony danych stosowane są następujące zabezpieczenia fizyczne:

3.3.1. Budynek zabezpieczony jest zamykanymi drzwiami i oknami,

3.3.2. Pomieszczenia, w których są przechowywane dane osobowe są wyposażone w czujki systemu alarmowego,

3.3.3. Wejście do pomieszczeń biurowych w godzinach pracy jest dozorowane,

3.3.4. Wejście do siedziby firmy jest monitorowane za pomocą kamery przemysłowej – kamery zamontowane wewnątrz budynku.

3.4. W celu ochrony danych stosowane są następujące zabezpieczenia zbiorów przetwarzanych cyfrowo.

3.4.1. Stanowiska komputerowe w pomieszczeniach, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych osobowych (np. interesanci albo inni pracownicy) - muszą być umieszczone w sposób, uniemożliwiający takim osobom wgląd do tych danych (polityka czystego ekranu). Stacje robocze, zwłaszcza te, które gromadzą dane osobowe muszą być ustawione w sposób uniemożliwiający wyniesienie ich przez osobę nieupoważnioną.

3.4.2. Na wszystkich komputerach, gdzie przetwarzane są dane osobowe stosowana jest ochrona antywirusowa. Program antywirusowy zabezpieczony jest przed nieautoryzowanymi zmianami.

3.4.3. Do autoryzacji w systemach operacyjnych oraz systemach przetwarzających dane osobowe stosowane są mechanizmy autoryzacji użytkownika, wymagające podania identyfikatora użytkownika oraz hasła.

3.4.4. Użytkownicy pracują na kontach pozbawionych praw administracyjnych.

3.4.5. Kluczowe elementy infrastruktury informatycznej, biorącej udział w przetwarzaniu danych osobowych, wyposażone są w zasilanie awaryjne umożliwiające bezpieczne zakończenie operacji na danych i zamknięcie systemu – zgodnie z instrukcją zarządzania systemem informatycznym.

3.4.6. Wszystkie sieciowe urządzenia aktywne mają zablokowaną możliwość zmiany konfiguracji bez autoryzacji. W miejscu styku sieci komputerowej z siecią publiczną zastosowane są odpowiednie mechanizmy logiczne/fizyczne, zapewniające separację zasobów informacyjnych, uniemożliwiające dostęp osób niepowołanych z zewnątrz, a także pozwalające na kontrolę przepływających danych.

3.4.7. Kopie zapasowe danych są tworzone z częstotliwością odpowiednią do potrzeb firmy Cieszyński Ośrodek Kultury „Dom Narodowy". Nośniki zawierające kopie zapasowe przechowywane są w miejscu innym niż główna baza zawierająca dane osobowe.

3.4.8. Nośniki danych używane w procesie przetwarzania danych, które przestają pełnić swoja funkcję zostają fizycznie zniszczone, bądź poddane procesowi „czyszczenia" w sposób uniemożliwiający ich ponowne odczytanie.

3.4.9. Dane osobowe, które znajdują się na nośnikach elektronicznych, wynoszonych po za obszar przetwarzania, muszą zostać zabezpieczone mechanizmami kryptograficznymi.

3.4.10. Do systemu przetwarzającego dane osobowe dopuszczony może być użytkownik, który posiada ważne upoważnienie ADO do przetwarzania danych osobowych. Nadawanie uprawnień do systemów odbywa się w sposób określony w Instrukcji Zarządzania Systemem Informatycznym. Każdy użytkownik korzysta z systemów komputerowych w zakresie określonym uprawnieniami nadanymi przez ADO, adekwatnymi do pełnionych obowiązków.

4. Załączniki do Polityki Bezpieczeństwa Danych Osobowych

Załączniki stanowią integralną część dokumentu Polityki Bezpieczeństwa Danych Osobowych, jednak dokonywane w nich zmiany nie wymagają aktualizacji polityki bezpieczeństwa. Aktualna wersja oraz data wydania załącznika jest wymaganym elementem identyfikacji załącznika.

Załączniki nr 3 oraz nr 4 mogą się odnosić do dokumentacji technicznych oprogramowania przetwarzającego dane osobowe i mogą występować w formie elektronicznej lub tradycyjnej.

Dokumentacja niniejszej polityki zawiera:

a) Załącznik nr 1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są danych osobowe.

b) Załącznik nr 2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

c) Załącznik nr 3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

d) Załącznik nr 4. Sposób przepływu danych pomiędzy poszczególnymi systemami.

e) Załącznik nr 5. Wzorcowe upoważnienie do przetwarzania danych osobowych.

f) Załącznik nr 6. Wzorcowa ewidencja osób upoważnionych do przetwarzania danych osobowych.

g) Załącznik nr 7. Wzór umowy powierzenia przetwarzania danych osobowych.

h) Załącznik nr 8. Wzorcowa ewidencja udostępnień oraz powierzeń danych osobowych.

i) Załącznik nr 9. Wzorcowa informacja dla pracownika w zakresie monitoringu.