POLITYKA BEZPIECZEŃSTWA

FUNDACJA KONGRES MORSKI W SZCZECINIE

1. CEL OPRACOWANIA DOKUMENTU

Celem opracowania niniejszego dokumentu jest wytyczenie zasad i wymagań w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez **FUNDACJĘ KONGRES MORSKI W SZCZECINIE** zwaną dalej również jako „Fundacja", biorąc pod uwagę, że w jednostce organizacyjnej nie został powołany Administrator bezpieczeństwa informacji. Ponadto, celem niniejszej Polityki Bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez Spółkę, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem. Wypracowane zasady i wymagania mają ukierunkować działania zmierzające do budowy systemu bezpieczeństwa, a potem jego utrzymywania podczas eksploatacji systemów informatycznych, na poziomie odpowiadającym potrzebom organizacji.

2. DEFINICJE

1) **administrator danych** – Fundacja Kongres Morski w Szczecinie
2) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne),

3) **informatyczne nośniki danych** – materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych osobowych w postaci cyfrowej lub analogowej,

4) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

5) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,

6) **przetwarzanie danych osobowych** – 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,

7) **rozliczalność danych** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

8) **rozporządzenie** – rozporządzenie 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. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285),

9) **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r., poz. 922),

10) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą (''anonimizacja''),

11) **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.

3. CEL POLITYKI BEZPIECZEŃSTWA

Celem Polityki bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez Fundację, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z

naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

4. ZAKRES STOSOWANIA POLITYKI BEZPIECZEŃSTWA

W ramach zabezpieczenia danych osobowych ochronie podlegają:

a) sprzęt komputerowy – serwer, komputery osobiste (w tym laptopy) i inne urządzenia zewnętrzne,
b) oprogramowanie,
c) dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych,
d) hasła użytkowników,
e) bazy danych i kopie zapasowe,
f) wydruki,
g) związana z przetwarzaniem danych dokumentacja papierowa.

Polityka bezpieczeństwa dotyczy przetwarzania wszystkich danych osobowych, przetwarzanych przez Fundację w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, a także w systemach informatycznych będących w dyspozycji Spółki i zawiera następujące informacje:

A. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),

B. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych,

C. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi,

D. sposób przepływu danych pomiędzy poszczególnymi systemami,

E. środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,

Polityka bezpieczeństwa ma zastosowanie wobec wszystkich komórek organizacyjnych Fundacji.

A. Obszar przetwarzania danych osobowych

Przetwarzanie danych osobowych przez Fundację odbywa się zarówno przy wykorzystaniu systemów informatycznych jak i poza nimi, tj. w wersji papierowej. Obszar przetwarzania danych osobowych przez Fundację został określony w załączniku nr 1 do Polityki bezpieczeństwa pt.: „Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe w Fundacji". Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych.

B. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych

Wykaz zbiorów danych osobowych przetwarzanych przez Fundację oraz programów zastosowanych do przetwarzania tych danych stanowi załącznik 2 do Polityki bezpieczeństwa pt.: „Wykaz zbiorów danych osobowych i systemów zastosowanych do ich przetwarzania".

C. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi

Pola informacyjne (rodzaje przetwarzanych danych osobowych) w odniesieniu do poszczególnych zbiorów danych zostały określone w dokumencie „Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania" stanowiącym załącznik nr 2 do Polityki bezpieczeństwa.

D. **Sposób przepływu danych pomiędzy poszczególnymi systemami**

Sposób przepływu danych pomiędzy różnymi systemami informatycznymi określa załącznik 2 do Polityki bezpieczeństwa pt.: „Wykaz zbiorów danych osobowych i systemów zastosowanych do ich przetwarzania".

E. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Do elementów zabezpieczenia danych osobowych przez Fundację zalicza się:

a) stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),
b) odpowiednie środki zabezpieczenia danych w systemach informatycznych (zabezpieczenia techniczne),
c) nadzór administratora danych nad wprowadzonymi zasadami i procedurami zabezpieczenia danych (zabezpieczenie organizacyjne),
d) bezpieczeństwo osobowe.

a) zabezpieczenia fizyczne obejmują:

- wydzielenie obszaru przetwarzania danych,
- dostęp do pomieszczeń, w których przetwarzane są dane osobowe objęty jest systemem kontroli dostępu,
- samodzielny dostęp do pomieszczeń jest możliwy wyłącznie dla osób upoważnionych, wstęp osób postronnych jest możliwy jedynie podczas obecności osób upoważnionych,
- przechowywanie akt w wersji papierowej w specjalnie do tego celu przeznaczonych pomieszczeniach, w zamykanych na klucz szafach,
- kopie zapasowe zbioru danych osobowych przechowywane są w sejfie w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,

b) zabezpieczenia techniczne obejmują:

- systemy informatyczne zastosowane do przetwarzania danych osobowych spełniają wymagania określone w Rozporządzeniu,
- w systemach informatycznych w Fundacji obowiązują zabezpieczenia na poziomie wysokim, zgodnie z załącznikiem do Rozporządzenia,
- zastosowano mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; uprawnienia są różne dla różnych grup użytkowników,
- zastosowano odpowiednie i regularnie aktualizowane narzędzia ochronne, w tym oprogramowanie antywirusowe, które jest regularnie aktualizowane,
- system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
- tworzone są regularnie kopie zapasowe zbiorów danych przetwarzanych w systemach informatycznych oraz kopie programów służących do przetwarzania danych osobowych,
- zastosowano zabezpieczenia systemu przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (listwy przeciwzakłóceniowe),

c) zabezpieczenia organizacyjne obejmują:

- osobą odpowiedzialną za bezpieczeństwo danych osobowych jest administrator danych oraz wyznaczona przez niego osoba, która opracowuje i aktualizuje Politykę bezpieczeństwa, załączniki do Polityki bezpieczeństwa oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- pracownicy Fundacji, którzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą, o zaobserwowanych nieprawidłowościach informują administratora danych lub wyznaczoną przez niego osobę;

- osoby upoważnione do przetwarzania danych osobowych mające dostęp do danych osobowych, które są w dyspozycji Fundacji, zobowiązane są do utrzymywania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu z określonego stanowiska, a także po ustaniu zatrudnienia; w tym celu osoby te podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia,
- przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które zostały upoważnione do przetwarzania danych osobowych zgodnie z art. 37 ustawy,
- osoby przetwarzające dane osobowe zostały upoważnione do przetwarzania danych osobowych poprzez wpisanie określonych kompetencji do zakresu obowiązków na danym stanowisku. Określone stanowiska wraz z przypisanym zakresem upoważnienia znajdują się w ewidencji osób upoważnionych do przetwarzania danych osobowych, stanowiącej załącznik 4 do Polityki bezpieczeństwa.

d) zabezpieczenie osobowe

- należy stosować klauzulę o zachowaniu poufności danych osobowych w umowach o pracę oraz w umowach ze zleceniobiorcami, z którymi związane jest przetwarzanie danych osobowych;
- wprowadza się obowiązek raportowania do administratora danych wszelkich naruszeń (incydentów), zauważonych podatności i innych słabych punktów oraz przypadków błędnego działania sprzętu i oprogramowania.

5. ROZPOWSZECHNIANIE I ZARZĄDZANIE DOKUMENTEM POLITYKI

1. Niniejszy dokument zawiera informacje o zabezpieczeniach, dlatego też został objęty ochroną na zasadzie tajemnicy przedsiębiorstwa w myśl art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.

U. z 2018 r., poz. 419). Wybrane jego elementy mogą zostać udostępnione innym podmiotom po zawarciu stosownej umowy o zachowaniu poufności.

2. Za zarządzanie dokumentem Polityki Bezpieczeństwa, w tym jego rozpowszechnianiem, aktualizacją, utrzymywaniem spójności z innymi dokumentami, jest odpowiedzialny administrator danych.
3. Z treścią niniejszego dokumentu powinni być zapoznani powinny zostać zapoznane wszystkie osoby upoważnione do przetwarzania danych osobowych, które z racji wykonywanych obowiązków i czynności mają dostęp do danych osobowych.
4. Integralną część niniejszej Polityki Bezpieczeństwa stanowią następujące załączniki:

a) Załącznik nr 1 – Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe;
b) Załącznik nr 2 – Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania;
c) Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych;
d) Załącznik nr 4 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 1 do Polityki Bezpieczeństwa:
FUNDACJA KONGRES MORSKI W SZCZECINIE

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe

Lp.	Lokalizacja – adres i numer budynku	Numer pomieszczenia/ przeznaczenie	Uwagi
1	SIEDZIBA FUNDACJI KONGRES MORSKI W SZCZECINIE, ALEJA WOJSKA POLSKIEGO 86, 70-482 SZCZECIN	POMIESZCZENIE BIUROWE 1B	POMIESZCZENIE ZAMYKANE NA KLUCZ

Załącznik nr 2 do Polityki Bezpieczeństwa:

Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania

Lp.	Nazwa zbioru danych osobowych	System zastosowany do przetwarzania /nazwa systemu informatycznego/	Zakres danych osobowych w zbiorze danych /kategorie danych/	Komunikacja z innymi systemami (T/N)	Przepływ danych
1	Zbiór danych uczestnikó w 10. Międzynarodowego Kongresu Morskiego	Rejestrator EVENEA	**1)** Imiona i nazwiska **2)** Numer telefonu **3)** Adres e-mail **4)** Nazwa firmy		Dane w postaci elektronicznej

Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych;

Załącznik nr 4 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 3 i 4 dostępny jest w biurze Fundacji Kongres Morski w Szczecinie – Al. Wojska Polskiego 86, 70-482 Szczecin