Załącznik Nr 1
do Zarządzenia Nr 12/05/2014
Dyrektora
Filharmonii Dolnośląskiej w Jeleniej Górze
z dnia 29 maja 2014r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
W
FILHARMONII DOLNOŚLĄSKIEJ W JELENIEJ GÓRZE

Jelenia Góra, maj 2014r.

Spis treści

Lp.	Wyszczególnienie	Nr strony
I.	Cel	3
II.	Podstawa prawna	3
III.	Terminologia	3
IV.	Odpowiedzialność	4
V.	Zagrożenia	5
VI.	Procedury	6
VII.	Obszar przetwarzania danych osobowych	8
VIII.	Wykaz zbiorów danych osobowych	8
IX.	Opis struktury zbiorów danych osobowych	8
X.	Sposób przepływu danych pomiędzy poszczególnymi systemami	8
XI.	System zabezpieczenia danych osobowych	9
XII.	Przeglądy i aktualizacje polityki	9
	Załącznik nr 1 – wykaz budynków i pomieszczeń	11
	Załącznik nr 2 – wzór wykazu zbiorów danych osobowych	12
	Załącznik nr 3 – wzór opisu struktury zbiorów	13

I. Cel

1. Polityka Bezpieczeństwa to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych w Filharmonii Dolnośląskiej w Jeleniej Górze. Polityka Bezpieczeństwa określa w szczególności sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną.
2. Polityka Bezpieczeństwa ma zastosowanie do zbioru danych osobowych niezależnie od formy ich przetwarzania:
a) tradycyjnie – w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
b) w systemach informatycznych – także w przypadku przetwarzania danych poza zbiorem danych osobowych.
3. Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:
1) poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
2) integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3) rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
4. Niniejsza Polityka nie ma zastosowania w ochronie informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

II. Podstawa prawna

Polityka Bezpieczeństwa została opracowana na podstawie ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. Nr 100, poz. 1024).

III. Terminologia

1.Użyte w Polityce Bezpieczeństwa określenia oznaczają:
1) Polityka – Polityka Bezpieczeństwa w Filharmonii Dolnośląskiej w Jeleniej Górze (PB),
2) Filharmonia Dolnośląska w Jeleniej Górze – Filharmonia,
3) Administrator Danych (AD) – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem Danych w Filharmonii jest Dyrektor,

4) Administrator Bezpieczeństwa Informacji (ABI) – pracownik Filharmonii wyznaczony przez Administratora Danych do nadzorowania przestrzegania zasad ochrony danych osobowych,
5) Administrator Systemu Informatycznego – informatyk zajmujący się zarządzaniem systemem informatycznym i odpowiadający za jego sprawne działanie, a także kontrolę uprawnień i administrowanie użytkownikami.
6) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Za dane osobowe uważa się również dane osób fizycznych prowadzących działalność gospodarczą,
7) zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje),
8) przetwarzanie danych – operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
9) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur, narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

IV. Odpowiedzialność

1.Do obowiązków Administratora Danych należy w szczególności:
1) podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych,
b) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie Administratora Bezpieczeństwa Informacji,
c) wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych.
d) zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa danych osobowych.
2. Do obowiązków Administratora Bezpieczeństwa Informacji należy nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych przetwarzanych w formie papierowej i elektronicznej. Do obowiązków ABI należy również:
1) nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych,
2) prowadzenie dokumentacji wynikającej z niniejszej Polityki oraz powiązanych z nią instrukcji i procedur,

3) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie oraz przedstawienie Administratorowi Danych zaleceń i rekomendacji dotyczących eliminacji ryzyk ich z powiązanych z nią instrukcji i procedur,

3. Obowiązki Administratora Systemu Informatycznego:

1) operacyjne zarządzanie systemami informatycznymi, w sposób zapewniający ochronę danych osobowych w nich przetwarzanych,

2) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,

3) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,

4) zarządzanie stosowanymi w systemach informatycznych środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.

5) utrzymywanie systemu w należytej sprawności technicznej,

6) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami sprzętu, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

4. Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

1) przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,

2) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,

3) ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,

4) informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe.

V. Zagrożenia

1.Rodzaje zagrożeń naruszających ochronę danych osobowych:

1) zagrożenia losowe:

a) zewnętrzne np. przerwy w zasilaniu energią elektryczną – ich wystąpienie może prowadzić do utraty danych, ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu,

b) wewnętrzne np. niezamierzone pomyłki operatora, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych,

2) zagrożenia zamierzone – świadome i celowe naruszenie ochrony danych. W ramach tej kategorii zagrożeń wystąpić mogą:

a) nieuprawniony dostęp do systemu z zewnątrz,

b) nieuprawniony dostęp do systemu z wewnątrz,

c) nieuprawnione przekazanie danych,

d) bezpośrednie zagrożenie sprzętu np. kradzież, zniszczenie.

2. Sytuacje zakwalifikowane jako naruszenie lub uzasadnienie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to m.in.:
1) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych,
2) niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, przeciążenia napięcia,
3) awaria sprzętu lub oprogramowania, które są celowym działaniem naruszenia ochrony danych osobowych,
4) pogorszenie jakości danych w systemie lub inne odstępstwa od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie,
5) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
6) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia,
7) ujawnienie osobom nieuprawnionym danych osobowych bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych,
8) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych,
9) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa danych (brak blokady komputera przed opuszczeniem stanowiska pracy, pozostawienie dokumentów w drukarce lub kserokopiarce, nie wykonanie kopii zapasowych, ujawnienie haseł do systemu innym pracownikom itp.),
10) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych – otwarte szafy, biurka itp.
3. W przypadku stwierdzenia naruszeń danych osobowych należy podjąć działania zgodne z procedurą postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.

VI. Procedury

1.Procedura określa tryb postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych gromadzonych i przetwarzanych zarówno w zbiorach informatycznych jak i w zbiorach tradycyjnych (papierowych). Procedurę stosuje się także w przypadku gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe.
2.Przez naruszenie bezpieczeństwa danych osobowych rozumie się świadome lub nieświadome niezgodne z przepisami obowiązującego prawa, przetwarzanie (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie oraz usuwanie), doprowadzenie przez swoje działanie do możliwości utraty danych, ich ujawnienie osobom nieupoważnionym lub uszkodzenie systemów informatycznych.
4.Procedura postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych:

1) każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest do niezwłocznego powiadomienia o tym bezpośredniego przełożonego, a następnie Administratora Bezpieczeństwa Informacji.
2) Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Systemów Informatycznych po otrzymaniu powiadomienia:
a) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

b) sprawdza sposób działania programów (w tym obecność wirusów),
c) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
d) sprawdza zawartość zbioru danych osobowych,
e) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,
3) W przypadku stwierdzenia naruszenia zabezpieczeń Administrator Bezpieczeństwa Informacji:
a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbioru danych itp.),
b) w celu powstrzymania lub ograniczenia dostępu do danych osoby nieupoważnionej, podejmuje odpowiednie działania poprzez: fizyczne odłączenie urządzeń i segmentów sieci, wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp, w celu uniknięcia ponownej próby włamania,
c) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyny naruszenia,
d) niezwłocznie przywraca prawidłowy stan działania systemu,
e) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
f) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
4) Raport Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych,
5) Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych, podejmuje niezbędne działania w celu wyeliminowania naruszeń w przyszłości zabezpieczeń danych:
a) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
b) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniechania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe

szkolenia, a wobec osób winnych zaniedbań wnioskuje do Administratora Danych o wyciągnięcie konsekwencji przewidzianych prawem,
c) jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, występuje do Administratora Danych o zawiadomienie organów ścigania.

VII. Obszar przetwarzania danych osobowych

1.Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia w budynku Filharmonii przy ul. Piłsudskiego 60 w Jeleniej Górze. Do takich pomieszczeń zalicza się w szczególności:
1) pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych,
2) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe,
3) pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia elektroniczne, nośniki informacji oraz kopie zapasowe zawierające dane osobowe.
2. Szczegółowy wykaz obszarów przetwarzania danych osobowych określa załącznik nr 1 do niniejszej Polityki.
3. Za jego prowadzenie i bieżącą aktualizację odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

VIII. Wykaz zbiorów danych osobowych

1.Dokumentacja zbiorów danych osobowych prowadzona jest przez Administratora Bezpieczeństwa Informacji, której wzór stanowi załącznik nr 2 do niniejszej Polityki.
2. Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń należących do obszaru przetwarzania danych osobowych.

IX Opis struktury zbiorów danych osobowych

1.Dokumentacja zbiorów danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji, której wzór stanowi załącznik nr 3 do niniejszej Polityki.
2. Wskazane w załączniku nr 3 zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach.

3. Zawartość pól informacyjnych występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają Administratora Danych do przetwarzania danych osobowych.

X. Sposób przepływu danych pomiędzy poszczególnymi systemami

1.Dokumentacja systemów informatycznych służących do przetwarzania danych osobowych powinna zawierać opis współpracy z innymi systemami informatycznymi oraz sposób przepływu pomiędzy systemami, z którymi współpracuje.

2. Administrator Systemów Informatycznych zobowiązany jest do prowadzenia aktualnej dokumentacji opisującej sposób przepływu danych osobowych pomiędzy systemami.

XI. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1.Dane osobowe chronione są przy zastosowaniu następujących zabezpieczeń niezbędnych dla zapewnienia poufności, integralności i rozliczalności danych osobowych:

a) budynek i wszystkie pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed dostępem osób nieuprawnionych,,

b) klucze do pomieszczeń, w których przetwarzane są dane osobowe pobierane są i zdawane na portierni u pracowników ochrony. Prowadzona jest ewidencja wydawanych kluczy.

c) osoby nieupoważnione do przetwarzania danych osobowych mogą przebywać w obszarach przetwarzania danych osobowych wyłącznie za zgodą Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych,

b) dane osobowe przechowywane w wersji tradycyjnej (papierowej) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych. Klucze należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych,

c) zbiory danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii zapasowych,

d) transmisja danych osobowych poprzez publiczną sieć telekomunikacyjną jest zabezpieczona środkami kryptograficznej ochrony danych,

e) w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemów informatycznych, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło,

f) hasła do uwierzytelniania w systemach informatycznych służących do przetwarzania danych osobowych są zmieniane co najmniej raz na 30 dni

g) stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją,

h) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,

2. Szkolenie z zakresu ochrony danych osobowych dla nowo przyjmowanych pracowników przeprowadza Administrator Bezpieczeństwa Informacji.

XII. Przeglądy i aktualizacje polityki bezpieczeństwa

1.Polityka bezpieczeństwa podlega przeglądowi pod katem aktualności i przestrzegania nie rzadziej niż raz na dwa lata. Przeglądu dokonuje Administrator Bezpieczeństwa Informacji.

2. Polityka bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:

- likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru,
- zmiany lokalizacji zbioru,
- zmiany przepisów prawa dotyczących ochrony danych osobowych, wymagającej aktualizacji polityki.

3. Aktualizacji Polityki Bezpieczeństwa dokonuje Administrator Bezpieczeństwa Informacji.

4. Zatwierdzenia zaktualizowanej Polityki Bezpieczeństwa dokonuje Administrator Danych.

załącznik nr 1
do Polityki Bezpieczeństwa

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar przetwarzania danych osobowych

Lp.	Nazwa zbioru	Budynek/adres	Pomieszczenie
Lp.	**Nazwa zbioru**	**Budynek/adres**	**Pomieszczenie**
1.	Kontrahenci Filharmonii	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	134,135,136,137,302,306,402, 404,406
2.	Deklaracje ZUS	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	135,136
3.	Listy płac	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	134,135,136,404
4.	Zajęcia komornicze	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	134,135,136,404
5.	Deklaracje podatkowe	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	134,135,136,406
6.	Listy zasiłkowe	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	134,135,136,404
7.	Karty wynagrodzeń	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	134,135,136
8.	Dane meldunkowe	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	Portiernia,137
9.	Baza adresów e-mail	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	136,137,302,306,402,406
10.	Dane ofertowe	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	136,137,302,304,306,402,404, 406
11.	Dane osobowe pracowników	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	136
12.	Karty wypożyczeń instrumentów muz.	Filharmonia Dolnośląska, ul. Piłsudskiego60 58-500 Jelenia Góra	137

---

podpis Administratora Danych

załącznik nr 2
do Polityki Bezpieczeństwa

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

l.p	Zbiór danych	System informatyczny	Lokalizacja	uwagi
1.	Pracownicy	- Optima - Płatnik - Pakiet MS Office	Budynek Filharmonii	
2.	Melomani	- Pakiet MS Office - Newsletter (CMS) - Aplikacja mobilna - System sprzedaży biletów	Budynek Filharmonii	
3.	Kontrahenci	- Optima	Budynek Filharmonii	
4.	Monitoring	- Monitoring wizyjny	Budynek Filharmonii	
5.	Zakładowy Fundusz Świadczeń Socjalnych	–	Budynek Filharmonii	
6.	Pracownicza Kasa Zapomogowo-Pożyczkowa	–	Budynek Filharmonii	

……..
podpis Administratora Bezpieczeństwa Informacji

s