Załącznik nr 2 do Zarządzenia Rektora nr 23/2018

Polityka Bezpieczeństwa Danych Osobowych Uniwersytetu Muzycznego Fryderyka Chopina

Spis treści

Wstęp

Polityka Bezpieczeństwa Danych Osobowych Uniwersytetu Muzycznego Fryderyka Chopina (dalej: PBDO UMFC) ma na celu ochronę danych osobowych przetwarzanych w Uniwersytecie na podstawie zobowiązań, wytycznych i zaleceń określonych w 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 (ogólne rozporządzenie o ochronie danych – dalej: RODO) oraz krajowych przepisach dotyczących ochrony danych osobowych. Jest jednym z elementów składających się na dokumentację Systemu Zarządzania Bezpieczeństwem Informacji UMFC.

Niniejszy dokument jest aktem wewnętrznego stosowania, wprowadzonym przez Rektora Uniwersytetu.

Wykaz użytych skrótów i terminów

ABI/IOD Administrator Bezpieczeństwa Informacji/Inspektor Ochrony Danych – osoba wyznaczona przez ADO w celu nadzorowania przestrzegania zasad ochrony danych osobowych

ADO Administrator Danych Osobowych – osoba decydująca o celach i środkach przetwarzania danych osobowych – Rektor UMFC

Dostępność zapewnienie, że dostęp do informacji mają osoby uprawnione zawsze, gdy istnieje taka potrzeba

Organ nadzorczy Generalny Inspektor Ochrony Danych Osobowych/Urząd Ochrony Danych Osobowych - organ powołany do ochrony danych osobowych

Integralność zagwarantowanie dokładności i kompletności informacji oraz metod ich przetwarzania – zapewnienie, że dane nie zostały zmodyfikowane w nieautoryzowany sposób

Obszar przetwarzania miejsce, w którym przetwarzane są dane osobowe

PBDO Polityka Bezpieczeństwa Danych Osobowych

Poufność zapewnienie, że informacje nie są udostępniane bądź wyjawiane nieupoważnionym osobom lub podmiotom

RODO Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Rozliczalność zapewnienie, że działania na informacjach mogą być jednoznacznie przypisane danej osobie, umożliwienie jednoznacznej identyfikacji

System teleinformatyczny zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, w tym również za pomocą obrazu i dźwięku

UMFC/Uniwersytet/Uczelnia Uniwersytet Muzyczny Fryderyka Chopina

1. Dane osobowe i zasady dotyczące ich przetwarzania

Dane osobowe są to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer PESEL lub innego numeru identyfikacyjnego, danych o lokalizacji, loginu, identyfikatora internetowego lub szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość.

Dane osobowe w UMFC muszą być przetwarzane zgodnie z zasadami, o których mowa w art. 5 RODO:

1. **Zasada zgodności z prawem, rzetelność i przejrzystość** – przetwarzanie dokonywanej jest zgodnie z prawem, rzetelnie i w sposób przejrzysty, dla osoby, której dane dotyczą,
2. **Zasada ograniczenia celu** – dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
3. **Zasada minimalizacji danych** – zbierane dane są adekwatne, stosowne oraz ograniczone do tego co jest niezbędne do celów, w których są przetwarzane,
4. **Zasada prawidłowości** – dane są zawsze prawidłowe i w razie konieczności uaktualniane,
5. **Zasada ograniczenia przechowywania** – dane przechowywane są przez okres nie dłuższy niż jest to niezbędne do celów, w których są przetwarzane,
6. **Zasada integralności i poufności** – dane przetwarzane są zawsze w sposób zapewniający im bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Środki techniczne i organizacyjne zastosowane w UMFC, mające na celu zapewnienie bezpieczeństwa danym osobowym przetwarzanym w Uniwersytecie, zostały opisane w odrębnym rozdziale PBDO.

2. Administrator Danych Osobowych

Administrator danych osobowych (ADO) decyduje o celach i środkach przetwarzania danych osobowych, jest też odpowiedzialny za przestrzeganie zasad, o których mowa w poprzednim rozdziale. ADO wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia przetwarzania danych w Uczelni zgodnie z zapisami RODO. Rolę i zadania ADO w UMCF wykonuje Rektor Uczelni.

3. Inspektor Ochrony Danych

Uniwersytet Muzyczny Fryderyka Chopina jako instytucja publiczna zobowiązana jest do wyznaczenia Inspektora Ochrony Danych Osobowych (IOD) zgodnie z art.37 pkt 1a 1 RODO[1]. Inspektor ochrony danych włączany jest we wszystkie sprawy dotyczące ochrony danych osobowych, podlega on bezpośrednio Administratorowi Danych Osobowych. Do jego zadań w szczególności należy: informowanie ADO i wszystkich pracowników UMFC o obowiązkach spoczywających na nich w obszarze zapewnienia bezpieczeństwa danych osobowych, monitorowanie przestrzegania zapisów RODO i przyjętych zasad ochrony danych w Uczelni, podejmowanie działań zwiększających świadomość w obszarze ochrony danych, współpraca z organem nadzorczym. IOD pełni też funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych. W UMFC zadania Inspektora Ochrony Danych pełni wyznaczona przez Rektora osoba. Dane kontaktowe IOD zamieszczone są w BIP UMFC.

4. Rejestrowanie czynności przetwarzania danych

Każdy Administrator Danych Osobowych zobowiązany jest zgodnie z art. 30 RODO do prowadzenia rejestru przetwarzania danych osobowych, za które odpowiada. Rejestr zawiera m.in. dane ADO i IOD, cele przetwarzania, opis kategorii osób, których dane dotyczą, opis kategorii danych, kategorie odbiorców danych, planowane terminy usunięcia danych, ogólny opis środków technicznych i organizacyjnych zastosowanych w celu zapewnienia bezpieczeństwa danych.

W UMFC rejestr czynności przetwarzania danych prowadzi i aktualizuje Inspektor Ochrony Danych.

5. Środki organizacyjne i techniczne zastosowane w UMFC w celu zapewnienia bezpieczeństwa i ochrony danych

Zgodnie z art.24 RODO administrator danych wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia, że przetwarzanie będzie odbywało się zgodnie z prawem. Stosowanie środków musi uwzględniać charakter, zakres, kontekst i cele przetwarzania danych a także ryzyko naruszenia praw lub wolności osób, których dane dotyczą. Zastosowane środki muszą zostać wdrożone w sposób umożliwiający ich wykazanie, w razie potrzeb poddawane są przeglądom i aktualizacji.

Środki organizacyjne zastosowane w UMFC mające na celu zapewnienie bezpieczeństwa i ochrony danych osobowych to przede wszystkim:

1. Opracowanie, wdrożenie i stosowanie zapisów niniejszej Polityki Bezpieczeństwa Danych Osobowych,
2. Opracowanie, wdrożenie i stosowanie zapisów Polityki Bezpieczeństwa Systemów Teleinformatycznych (odrębny dokument, związany z niniejszą PBDO),
3. Ciągłe podnoszenie świadomości wszystkich pracowników UMFC w obszarze ochrony danych osobowych,
4. Organizowanie szkoleń z obszaru ochrony danych osobowych dla wszystkich osób mających dostęp do przetwarzania danych

[1] Do dnia 25 maja 2018 roku zadania IOD w UMFC pełni Administrator Bezpieczeństwa Informacji wyznaczony na mocy ustawy z dn. 29.08.1997r. o ochronie danych osobowych (Dz.U.2016.922).

5. Wyznaczenie Inspektora Ochrony Danych.

Środki techniczne zastosowane w UMFC mające na celu zapewnienie bezpieczeństwa i ochrony danych osobowych to przede wszystkim:

1. Nadawanie upoważnień do przetwarzania danych osobowych w celu zapewnienia, że dostęp do danych mają jedynie osoby uprawnione, w określonym zakresie, czasie i celu,
2. Zapewnienie rozliczalności we wszystkich systemach teleinformatycznych poprzez ustalony system nadawania/zmiany/odbioru uprawnień w systemie,
3. Stosowanie fizycznej kontroli dostępu do szaf i pomieszczeń, w których przechowywane są dane,
4. Przestrzeganie zasad „czystego biurka" i „czystego ekranu",
5. Ochrona przed szkodliwym oprogramowaniem (programy antywirusowe),
6. Stosowanie zabezpieczeń nośników danych, sprzętu komputerowego, aplikacji, sieci.

Sposoby wdrożenia i realizacji poszczególnych środków technicznych zastosowanych w UMFC zostały opisane w odrębnych politykach i procedurach.

5.1. Ocena skutków dla ochrony danych

W przypadku gdy dany rodzaj przetwarzania danych ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może spowodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, ADO jeszcze **przed** rozpoczęciem przetwarzania dokonuje oceny skutków dla ochrony danych osobowych. Ocena skutków dotyczy przede wszystkim planowanego przetwarzania z użyciem nowych technologii.

W UMFC ocena skutków dokonywana jest w konsultacji z Inspektorem Ochrony Danych.

5.2. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Administrator danych UMFC uwzględnia ochronę praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych jeszcze przed przystąpieniem do faktycznego przetwarzania danych – już na najwcześniejszym etapie w fazie projektowania, tj. opracowywania, wybierania aplikacji, programów i usług.

Wybór produktu uwzględnia kwestie związane z ochrona danych, które będą w nim przetwarzane, uwzględniając przede wszystkim zasadę minimalizacji danych (przetwarzamy tylko te dane, które są niezbędne do osiągniecia celu przetwarzania), a także ich pseudonimizację („szyfrowanie" danych w celu uniemożliwienia identyfikacji osoby) . Stosowanie zasady domyślnej ochrony danych ma na celu zapewnienie, że przetwarzane są tylko te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Domyślna ochrona danych odnosi się do ilości zbieranych danych, zakresu ich przetwarzania, okresu przechowywania oraz ich dostępności.

Zasada uwzględniania ochrony danych osobowych w fazie projektowania oraz zasada domyślnej ochrony danych brana jest pod uwagę w przetargach publicznych.

6. Prawa osób, których dane dotyczą

Osoba, której dane dotyczą posiada następujące prawa:

1. Prawo dostępu do swoich danych oraz uzyskania na ich temat informacji
2. Prawo do sprostowania danych
3. Prawo do usunięcia danych („prawo do bycia zapomnianym”)
4. Prawo do ograniczenia przetwarzania
5. Prawo do przenoszenia danych
6. Prawo do sprzeciwu wobec przetwarzania danych (w tym profilowania, o ile takie jest dokonywane)

Egzekwowanie powyższych praw nie może niekorzystnie wpływać na prawa i wolności innych osób, jak również korzystanie z poszczególnych może wywoływać inne określone skutki prawne, w zależności od celu ich przetwarzania (np. prawo do usunięcia danych w przypadku cofnięcia zgody na ich przetwarzanie w kontekście zatrudnienia lub posiadania statusu studenta oznacza brak możliwości realizacji przez ADO określonego celu wobec osoby jakim jest zatrudnienie lub umożliwienie ukończenia studiów).

O posiadanych prawach osoby są informowane przed przystąpieniem zbierania danych zgodnie z przyjętymi procedurami w UMFC, w zależności od kategorii danych i celu ich przetwarzania.

7. Zgłaszanie naruszeń ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych, które skutkuje bądź może skutkować ryzykiem naruszenia praw i wolności osób, zgodnie z art. 33 RODO ADO bez zbędnej zwłoki, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza ten fakt organowi nadzorczemu. Naruszenia są dokumentowane, dokumentacja dotycząca naruszeń przechowywana jest u IOD.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych są one bez zbędnej zwłoki zawiadamiane o zaistnieniu takiego naruszenia (art. 34 RODO).

Szczegóły dotyczące zgłaszania naruszeń zostały opisane w procedurze stanowiącej załącznik nr 2 do PBDO.

Wykaz załączników

Załącznik nr 1 – Procedura dotycząca nadawania uprawnień w systemach teleinformatycznych i nadawania upoważnienia do przetwarzania danych osobowych

Załącznik nr 2 – Procedura zgłaszania naruszeń ochrony danych

Załącznik nr 1
do Polityki Bezpieczeństwa Danych Osobowych
UMFC

Procedura dotycząca nadawania uprawnień do systemów teleinformatycznych i nadania upoważnienia do przetwarzania danych osobowych w UMFC

w celu zapewnienia kontroli nad nadawaniem/zmianą i odbiorem upoważnień i uprawnień pracownikom i osobom wykonującym zadania na rzecz UMFC na każdym etapie zatrudnienia (nowych osób oraz osób już zatrudnionych, którym zmienia się zakres upoważnienia np. w przypadku zmiany jednostki organizacyjnej, przedłużenia umowy, zmiany zakresu obowiązków i in.) wprowadzony zostaje system obiegu wniosku o nadanie upoważnienia i uprawnień w systemach użytkowanych w UMFC:

1. Wniosek o nadanie upoważnienia do przetwarzania danych osobowych w poszczególnych systemach (tradycyjnych i/lub teleinformatycznych) użytkowanych w UMFC składa Kierownik jednostki organizacyjnej, do której został przydzielony pracownik,
2. We wniosku należy wskazać imię i nazwisko osoby, której wniosek dotyczy, stanowisko, okres na jaki zostaje zatrudniona (lub ma wykonywać czynności z zakresu wniosku), zakres niezbędnych do przyznania uprawnień na danym stanowisku, poprzedni login, o ile taki był wcześniej nadawany. Wzór wniosku stanowi załącznik do niniejszej procedury.
3. Wniosek może być przekazany drogą elektroniczną lub dostarczony w formie wydruku,
4. Upoważnienie do przetwarzania danych osobowych nadaje Administrator Danych Osobowych – Rektor UMFC,
5. Po nadaniu upoważnienia wniosek przekazywany jest do Działu Informatyki celem nadania loginu (o ile nie był wcześniej nadany) oraz uprawnień w poszczególnych systemach teleinformatycznych – zgodnie z wnioskiem,
6. W przypadku konieczności nadania uprawnień do systemów informatycznych innej jednostki organizacyjnej niż jednostka „macierzysta", niezbędne jest uzyskanie zgody Kierownika tej jednostki organizacyjnej, do której zasobów powinny zostać przyznane uprawnienia lub złożenie odrębnego wniosku przez tego Kierownika. W wyjątkowych sytuacjach szerszy dostęp może być nadany za zgodą ADO (np. dla pracowników sekretariatów Rektora, Prorektorów, Kanclerza, Działu Informatyki),
7. Wniosek powinien zawierać tylko te zbiory danych i systemy informatyczne, do których dostęp jest **niezbędny** pracownikowi do wykonywania powierzonych mu zadań.
8. Pracownicy Działu Informatyki realizują wniosek w zakresie nadania uprawnień do systemów oraz tworzą konta nowym użytkownikom systemu – najpóźniej na drugi dzień roboczy od otrzymania formularza, „włączają" systemy zgodnie z nadanymi uprawnieniami w formularzu.
9. Oryginał upoważnienia przechowywany jest w aktach osobowych pracownika, kopia przekazywana jest pracownikowi,
10. Upoważnienia dla osób, dla których nie są prowadzone akta osobowe, przechowywane są w Dziale Kadr w odrębnym segregatorze.

Załącznik nr 2
do Polityki Bezpieczeństwa Danych Osobowych
UMFC

Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych, zgłaszania naruszeń organowi nadzorczemu oraz zawiadamiania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych w UMFC

Naruszenie ochrony danych osobowych (incydent/zdarzenie) to sytuacja, która doprowadza lub może doprowadzić m.in. do ujawnienia, udostępnienia, nieautoryzowanej modyfikacji, zmiany, usunięcia lub innej niepożądanej operacji na danych osobowych zagrażającej ich bezpieczeństwu. Naruszenia mogą dotyczyć danych osobowych przetwarzanych w formie tradycyjnej (papier), w systemie teleinformatycznym a także słownie.

1. Wszelkie zauważone naruszenia ochrony danych osobowych należy zgłaszać osobiście, telefonicznie lub drogą mailową Inspektorowi Ochrony Danych Osobowych (ABI) i/lub Kierownikowi Działu Informatyki.
2. Sytuacje, które stanowią lub mogą stanowić naruszenie ochrony danych osobowych podlegające zgłoszeniu jak w pkt.1 to m.in.:

    1. Podejrzenie próby włamania do pomieszczenia, w którym przechowywane są dane osobowe,
    2. Obecność podejrzanych osób w pomieszczeniach bez nadzoru pracownika UMFC,
    3. Dokumentacja zawierająca dane osobowe znaleziona w koszu na śmieci (zniszczenie bez użycia niszczarki),
    4. Otwarte pomieszczenia/szafy/szuflady w których przechowywane są dane osobowe,
    5. Udostępnianie danych osobowych w formie papierowej, elektronicznej i ustnej,
    6. Telefoniczne próby wyłudzenia danych osobowych lub innych informacji prawnie chronionych,
    7. „podejrzane” wiadomości mailowe: zachęcające do ujawnienia lub wymuszające, podanie loginu i/lub hasła, kliknięcia w nieznany link,
    8. Kradzież komputerów, mobilnych nośników danych (płyt CD, pendrive, dysków) na których przechowywane były dane osobowe,
    9. Przechowywanie w widocznych miejscach haseł do systemów teleinformatycznych,
    10. Ujawnienie wirusa komputerowego lub nietypowe działanie komputerów,
    11. Przechowywanie w widocznych miejscach kluczy do szaf i szuflad,
    12. Inne niewymienione wyżej sytuacje zagrażające bezpieczeństwu danych osobowych.

3. Każde zgłoszenie jest rejestrowane przez IOD i weryfikowane pod kątem jego skutków,
4. W każdym przypadku podejmowane są działania adekwatne do zaistniałej sytuacji – prewencyjne, naprawcze lub doskonalące istniejące w UMFC procedury,
5. W przypadku naruszenia ochrony danych osobowych skutkujących naruszeniem praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

Zgłoszenie zawiera charakter naruszenia, przybliżoną liczbę osób, których dane dotyczą, imię i nazwisko oraz dane kontaktowe IOD, opis możliwych konsekwencji naruszenia, opis zastosowanych środków w celu zminimalizowania jego ewentualnych skutków,

6. Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, osoba, której dane dotyczą bez zbędnej zwłoki jest zawiadamiana o naruszeniu jej danych.
7. Zawiadomienie osoby, której dane dotyczą powinno zawierać opis charakteru naruszenia, dane IOD, możliwe konsekwencje naruszenia oraz zastosowane lub proponowane środki zaradcze dotyczące naruszenia.