Zarządzenie nr 6/2019
Rektora Akademii Teatralnej im. A. Zelwerowicza
z dnia 27 marca 2019 roku

w sprawie zmiany Zarządzenia nr 21/2018 z dnia 24 maja 2018 roku
w sprawie wprowadzenia Polityki ochrony danych osobowych
w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie.

§ 1

1. Wprowadza się następujące zmiany do § 4 nadając mu następujące brzmienie:
   „1. Administrator Danych Osobowych upoważnia osoby przetwarzające dane osobowe do ich przetwarzania w sposób wskazany w Procedurze nadawania upoważnień stanowiącej integralny załącznik do niniejszej Polityki ochrony danych."

2. Wprowadzam następujące zmiany do § 15 ust. 1 oraz dodaje ust. 4 do Polityki ochrony danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie i nadaje mu się następujące brzmienie:
   „1. Integralną częścią niniejszego regulaminu są następujące załączniki:
   a) wzór formularza upoważnienia/odwołania upoważnienia do przetwarzania danych osobowych,
   b) wzór ewidencji osób upoważnionych do przetwarzania danych osobowych,
   c) wzór oświadczenia pracownika (w tym osoby zatrudnionej na innej niż umowa o pracę podstawie prawnej) przetwarzającego dane osobowe,
   d) wzór klauzuli informacyjnej dla pracownika/osoby przetwarzającej dane osobowe
   e) procedura nadawania upoważnień;
   f) procedura reagowania i oceny naruszeń bezpieczeństwa danych osobowych;
   g) procedura udzielania informacji podawanej w przypadku pozyskiwania danych;
   h) procedura realizowania uprawnień osób, których dane są przetwarzane;
   i) procedura opiniowania zagadnień prawnych związanych z danymi osobowymi;
   2. W celu wykonania niniejszej Polityki ochrony danych osobowych wydawane będą dodatkowe dokumenty takie jak procedury, instrukcje czy zarządzenia. W tym celu mogą być prowadzone także listy i wykazy.
   3. W celu wykonania niniejszej Polityki ochrony danych osobowych prowadzone będą w osobnych dokumentach rejestry czynności przetwarzania danych osobowych ewentualnie kategorii danych osobowych.
   4. Wskazana treść wzorów w lit. a) do d) może być modyfikowane w pojedynczych przypadkach, gdy jest to uzasadnione stanem faktycznym."

§2

Pozostałe postanowienia Zarządzenia nr 21/2018 z dnia 24 maja 2018 roku pozostają w mocy.

§3

Pracownika działu Kadr zobowiązuję do zapoznania pracowników z niniejszym zarządzeniem.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

/−/ Prof. dr hab. Wojciech Malajkat

Polityka ochrony danych osobowych
w Akademii Teatralnej im. A. Zelwerowicza w Warszawie

§ 1
Postanowienia ogólne

1. Polityka ochrony danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie (dalej: „Akademia") jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach i procesach przetwarzania danych osobowych przetwarzanych przez Akademię, w tym zbiorach przetwarzanych w systemie informatycznym.
2. Akademii przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 4 Rozporządzenie 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) z dnia 27 Kwietnia 2016 R. (Dz.Urz.Ue.L Nr 119, Str. 1) – dalej Rozporządzenie RODO.
3. Akademia przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli istnieje ku temu podstawa prawna określona w art. 6 lub 9 RODO lub innych regulacjach.
4. Niniejszy dokument ma na celu realizację założeń ochrony danych osobowych określonych w:
    a) Konstytucja Rzeczypospolitej Polskiej,
    b) Rozporządzenie RODO,
    c) innych przepisach wydanych i przyjętych w celu realizacji ochrony danych osobowych w tym aktach wewnętrznych.
5. Akademia dąży do realizacji zasad, które wskazują, iż dane osobowe muszą być:
    a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
    b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
    c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
    d) 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 („prawidłowość");
    e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
    f) 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 („integralność i poufność”).

6. Akademia przestrzegając zasad wskazanych w ust. 4 wykazuje ich przestrzeganie („rozliczalność”) m.in. poprzez prowadzoną dokumentacją mającą na celu realizację niniejszej Polityki ochrony danych osobowych.

§ 2
Definicje

Przez użyte w treści Polityk ochrony danych sformułowania należy rozumieć:

1. Rozporządzenie RODO - Rozporządzenie 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) Z Dnia 27 Kwietnia 2016 R. (Dz.Urz.Ue.L Nr 119, Str. 1).
2. Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); 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.
3. Zbiór danych osobowych - dane osobowe zgromadzone w usystematyzowany sposób według kryterium rodzaju danych, celu albo osoby/działu przetwarzającej w jednostce.
4. Przetwarzanie danych osobowych - 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.
5. Administrator Danych Osobowych - Akademia, a w jego imieniu Rektor.
6. Inspektor danych osobowych – osoba wyznaczona przez Administratora Danych Osobowych odpowiedzialna za zadania określone w § 3 Polityki ochrony danych
7. Administrator Systemu Informatycznego - osoba wyznaczana przez Administratora Danych Osobowych odpowiedzialna za przestrzeganie zasad ochrony danych osobowych w systemie informatycznym i nadzorująca przetwarzanie danych osobowych w systemie informatycznym.
8. System informatyczny - zespół środków technicznych (urządzenia: komputerowe, drukujące, łączności, wraz z okablowaniem i oprogramowaniem), zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieć informatyczna i udostępniane przez nią zasoby.
9. Osoby zatrudnione przy przetwarzaniu danych osobowych - wszystkie osoby, w tym użytkownicy systemu informatycznego, mające z racji wykonywanych obowiązków dostęp do danych osobowych. Osobą zatrudnioną przy przetwarzaniu danych osobowych może być pracownik Akademii, a także osoba wykonująca usługi na podstawie umowy zlecenia lub innej umowy cywilno-prawnej pod warunkiem, iż wykonuje te prace osobiście.
10. Poufność - zapewnienie dostępu do informacji wyłącznie osobom upoważnionym.
11. Integralność - spójność danych osobowych, zapewnienie, że dane nie zostaną zmienione, dodane lub usunięte w nieautoryzowany sposób.

§ 3
Zarządzanie przetwarzaniem i bezpieczeństwem danych osobowych

1. Administratorem danych osobowych przetwarzanych w Akademii jest Akademia, reprezentowana przez Rektora Akademii.
2. Rektor Akademii powołuje **Inspektora ochrony danych**, który wykonuje zadania wskazane w art. 39 Rozporządzenia RODO do których należy:
    a. informowanie kierownictwa Akademii oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego Rozporządzenia RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b. monitorowanie przestrzegania Rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
    d. współpraca z organem nadzorczym;
    e. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

    - W ramach wypełniania obowiązków wskazanych w lit. a:
        a. informuje o zmianach i nowych interpretacjach w dziedzinie danych osobowych w zakresie dotyczącym administratora danych osobowych;
        b. informuje o obowiązkach nałożonych przepisami oraz dokumentami wewnętrznymi na pracowników;
        c. udziela odpowiedzi i konsultacji w zakresie stosowania przepisów dotyczących przetwarzania danych osobowych;
    - W ramach wypełniania obowiązków wskazanych w lit. b:
        a. cyklicznie informuje o zaobserwowanych zagrożeniach w dziedzinie ochrony danych osobowych;
        a. cyklicznie kieruje zapytania dotyczące przetwarzania danych osobowych;
        b. prowadzi audyty planowe według przyjętego harmonogramu;
        c. prowadzi audyty doraźne;
3. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
4. Kierownictwo Akademii zapewnia, by Inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
5. Kierownictwo Akademii wspiera Inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 Rozporządzenia RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
6. Kierownictwo Akademii zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega

najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

7. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
8. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. kierownictwo Akademii zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
9. kierownictwo Akademii powierza Inspektorowi danych osobowych:
    a. monitoring i aktualizacja prowadzonej dokumentacji przetwarzania danych osobowych;
    b. prowadzenie rejestrów czynności danych osobowych i kategorii danych osobowych (o ile jest taka potrzeba) zgodnie z uzyskanymi informacjami;
    c. prowadzenie rejestru osób upoważnionych do przetwarzania danych zgodnie z uzyskanymi informacjami;
    d. opiniowanie umów przetwarzania danych osobowych pod kątem Rozporządzenia RODO;
    e. prowadzenie rejestru incydentów;
10. Inspektor danych osobowych podlega bezpośrednio wyłącznie kierownictwa Akademii.
11. kierownictwo Akademii może powołać zastępców Inspektora danych osobowych wspierających go w realizacji zadań;
12. **Kierownicy komórek organizacyjnych** (przez które rozumie się także osoby zajmujące samodzielne stanowiska, o ile odpowiadają one samodzielnie za wybrane obszary przetwarzania danych osobowych) są odpowiedzialni za:
    a. zarządzenie zasobem danych osobowych w ramach komórki organizacyjnej;
    b. występowanie z wnioskiem do Administratora Systemu Informatycznego o nadanie, zmianę lub cofnięcie uprawnień pracownikom do określonego zasobu danych osobowych przetwarzanego w systemie informatycznym w tym aplikacjach;
    c. bieżąca kontrola nad realizacją zasad przetwarzania danych osobowych przez podległych pracowników;
    d. zabezpieczenie obszaru przetwarzania danych osobowych;
    e. zgłaszania do Inspektora danych osobowych zamiaru podjęcia nowych czynności przetwarzania na danych osobowych w tym w szczególności zamiaru powierzenia przetwarzania danych osobowych podmiotom zewnętrznym;
    f. zgłaszania do Inspektora danych osobowych incydentów przetwarzania danych osobowych;
    g. konsultowanie z Inspektorem danych osobowych podstawy przetwarzania danych osobowych w tym zasadności dopuszczenia do przetwarzania zbiorów osób i podmiotów trzecich;
    h. realizację procesu udostępniania danych osobowych;
    i. realizację zapisów umów powierzenia przetwarzania danych osobowych;
13. **Dział Kadr** jest odpowiedzialny za:
    a. informowanie Inspektora danych osobowych o wszelkich zmianach kadrowych na stanowiskach na których są przetwarzane dane osobowe;
    b. przygotowanie upoważnień do przetwarzania danych osobowych do podpisu przez Inspektora danych osobowych lub przekazania mu informacji umożliwiających ich wystawienie,
    c. przechowywanie nadanych upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu poufności (i innych w aktach osobowych pracowników;
14. **Administratorzy Systemu Informatycznego** są odpowiedzialni za zabezpieczenie i prawidłowe funkcjonowanie systemów informatycznych (w tym aplikacji)
    a. prowadzenie aktualnego wykazu systemów informatycznych (w tym aplikacji);

b. prowadzenie aktualnego wykazu osób wraz z loginami do systemów informatycznych i określonych aplikacji;
c. fizyczne nadawanie dostępu do systemu (w tym aplikacji) osobom upoważnionym do przetwarzania danych osobowych na wniosek Kierowników komórek organizacyjnych
d. fizyczne odbieranie lub modyfikację uprawnień do systemów (w tym aplikacji);
e. nadanie identyfikatorów (login) w systemie (w tym aplikacji);
f. nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
g. ustalenia w porozumieniu z Inspektorem danych osobowych, zasad ochrony danych w systemie informatycznym oraz akceptowanie wdrażania rozwiązań przygotowywanych w tym celu;
h. przeciwdziałanie dostępowi osób nieupoważnionych do systemu (w tym aplikacji), w którym przetwarzane są dane osobowe, a także nieautoryzowanych modyfikacji w tym zakresie;
i. informowanie Inspektora danych osobowych o wszelkich incydentach i zdarzeniach w systemie informatycznym mającym wpływ na poufność, integralność i ciągłość przetwarzania danych osobowych;
j. wykonywanie kopii zapasowych systemów (w tym aplikacji), zabezpieczenie ich przechowywania i okresowe sprawdzenie pod kątem odtwarzalności;
k. zgłaszania Inspektorowi danych osobowych informacji niezbędnych do aktualizacji dokumentów dotyczących przetwarzania danych osobowych;
l. tworzenie w porozumieniu z Inspektorem danych osobowych procedur zarządzania kontami użytkowników, procedur wykonywania kopii zapasowych i innych;
m. zapewnienie bezpiecznej wymiany danych w sieci wewnętrznej i nadzór nad przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
n. nadzór nad poprawnym działaniem awaryjnego zasilania urządzeń w szczególności serwerów;
o. składanie do kierownictwa Akademii propozycji zakupu oprogramowania lub sprzętu w celu podniesienia poziomu bezpieczeństwa systemu;
p. opiniowanie bezpieczeństwa stosowanych lub planowanych systemów zabezpieczających system informatyczny w porozumieniu Inspektorem danych osobowych;
q. składanie na wniosek Inspektora danych osobowych wyjaśnień, raportów, sprawozdań w zakresie obowiązków wskazanych w lit. powyżej.

§ 4
Osoby przetwarzające dane osobowe

1. Administrator Danych Osobowych upoważnia osoby przetwarzające dane osobowe do ich przetwarzania w sposób wskazany w Procedurze nadawania upoważnień stanowiącej integralny załącznik do niniejszej Polityki ochrony danych.

§ 5
Obowiązki osób przetwarzających dane osobowe

1. Obowiązki osób przetwarzających dane osobowe zostały określone w odrębnym Regulaminie.
2. Nieprzestrzeganie wskazanych tam obowiązków stanowi przedmiot analizy Administratora Danych Osobowych w konsultacji z Inspektorem Danych Osobowych. Administrator Danych Osobowych

podejmuje decyzję o konsekwencjach mających być wyciągniętych wobec osoby naruszającej Regulamin, o którym mowa w ust. 1

3. Poza Regulaminem Administrator Danych Osobowych może także wydawać procedury i instrukcje obowiązujące osoby przetwarzające dane osobowe.

§ 6
Umowy powierzenia danych osobowych

1. W przypadku powierzenia przetwarzania danych osobowych podmiotom trzecim, niewykonujących przetwarzania osobiście lub wykonujących przetwarzanie danych wspólnie z innymi osobami powierzenie następuje w drodze umowy powierzenia danych osobowych lub innego równorzędnego dokumentu dopuszczonego przez Rozporządzenie RODO.
2. Umowa powierzenia przetwarzania danych lub inny równorzędny dokument powinien zawierać elementy wskazane w Rozporządzeniu RODO.
3. Powierzenie przetwarzania danych osobowych jest konsultowane z Inspektorem Danych Osobowych.
4. Administrator Danych Osobowych ewidencjonuje umowy powierzenia danych osobowych.

§ 7
Udostępnianie danych osobowych odbiorcom

Udostępnienie danych osobowych odbiorcą niebędącymi podmiotami przetwarzającymi może nastąpić wyłącznie w przypadku istnienia przesłanki legalizującej udostępnienie danych osobowych. Udostępnienie danych osobowych jest konsultowane z Inspektorem ochrony danych. Komórka organizacyjna (lub osoba zajmująca samodzielne stanowisko) udostępniająca dane ewidencjonuje ich udostępnienie.

§ 8
Incydenty

1. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane powiadomić Inspektora Danych osobowych o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie.
2. Za zdarzenia naruszające bezpieczeństwo danych osobowych uważa się w szczególności:
   a) nieupoważniony dostęp do danych osobowych,
   b) ujawnienie bądź utrata danych osobowych,
   c) nieupoważniona modyfikacja danych osobowych, kopiowanie lub niszczenie dokumentów zawierających dane osobowe,
   d) inne naruszenie postanowień Rozporządzenia RODO.
3. Inspektor Danych Osobowych informuje o zdarzeniu Administratora Danych Osobowych, który informuje w przypadkach wskazanych w Rozporządzeniu RODO Urząd Ochrony Danych Osobowych i osoby, których przetwarzanie danych osobowych zostało naruszone.
4. Administrator Danych Osobowych może wydać odrębną szczegółową procedurę postępowania w takich przypadkach.

§ 9
Gromadzenie danych osobowych

1. Dane osobowe przetwarzane w Akademii mogą być uzyskiwane:
   a) bezpośrednio od osób, których te dane dotyczą,
   b) z innych źródeł, w granicach dozwolonych przepisami prawa.
2. Przetwarzanie danych osobowych może odbywać się wyłącznie w sytuacjach przewidzianych w art. 6 oraz 9 Rozporządzenia RODO oraz stosownych regulacjach wydanych na tej podstawie.
3. Dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
4. Zbierane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych")
5. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą lub niszczone, chyba że przepis prawa stanowi inaczej.
6. W przypadku konieczności udostępnienia dokumentów i danych osobowych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać zmiany tych danych osobowych w sposób zapewniający anonimowość osób, których dane te dotyczą.
7. W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Rozporządzenia RODO, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 10
Obowiązek informacyjny

1. Kierownicy komórek organizacyjnych Akademii lub osoby zatrudnione na samodzielnych stanowiskach, które zbierają i przetwarzają dane osobowe, są odpowiedzialni udzielić, osobom których dane przetwarzają, wszelkich informacji, o których mowa w art. 13 i 14 Rozporządzenia RODO, oraz z udziałem Inspektora Danych osobowych prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania ich prawach. Obowiązek informacyjny prowadzony jest zgodnie z ustaloną z Inspektorem Danych osobowych klauzulą informacyjna ich dotyczącą. Klauzula informacyjna zawiera informacje wskazane w art. 12 Rozporządzenia RODO.

§ 11
Prawa osób, których dotyczą dane osobowe

1. Osobom, których dane przetwarza się w zbiorze danych osobowych Akademii, przysługuje:
   a) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych,
   b) prawo do żądania sprostowania (poprawienia) danych,
   c) prawo do żądania usunięcia danych osobowych (tzw. „prawo do bycia zapomnianym"),
   d) prawo do żądania ograniczenia przetwarzania danych osobowych,
   e) prawo do przenoszenia danych do Pani/ Pana lub do innego administratora danych,
   f) prawo do sprzeciwu wobec przetwarzania danych osobowych.

2. Inspektor danych osobowych opiniuje zasadność żądania i wraz z komórką organizacyjną w której przetwarzane są dane osobowe udziela odpowiedzi.

§ 12
Czynności przetwarzania i zbiory danych

1. W Akademii prowadzi się rejestr czynności przetwarzania danych osobowych i ewentualnie rejestr kategorii przetwarzania danych. Rejestry są aktualizowane przez Inspektora danych osobowych na podstawie własnych ustaleń oraz informacji uzyskanych od pracowników. Czynności przetwarzania mogą być grupowane w ramach zbiorów danych osobowych wedle kryterium komórki przetwarzającej dane osobowe lub innego przyjętego w Akademii takiego jak kategoria osób lub cel przetwarzania danych.
2. Kierownicy komórek organizacyjnych Akademii lub osoby zatrudnione na samodzielnych stanowiskach, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia Inspektorowi danych osobowych informacji na temat:
   a) planowanego założenia nowych czynności przetwarzania i zbiorów danych osobowych,
   b) wnoszonych zmian do istniejących czynności przetwarzania i zbiorów danych osobowych.

§ 13
Ocena ryzyka

W celu prawidłowego wyznaczenia poziomu ochrony Administrator Danych Osobowych dokonuje okresowej analizy ryzyka, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania. Brana jest ona pod uwagę zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, a na jej podstawie wdraża się odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

§ 14
Zabezpieczenia fizyczne, informatyczne i organizacyjne

1. Dostęp do pomieszczeń Akademii, w których przetwarzane są dane osobowe, podlega kontroli.
2. Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania lub zdania klucza.
3. Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie osobom upoważnionym.
4. Akademia, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
5. W Akademii stosowane są następujące dodatkowe środki techniczne i organizacyjne oraz przedsięwzięcia niezbędne do zapewnienia poufności, integralności przetwarzanych danych osobowych:
   a) środki ochrony fizycznej - urządzenia służące do przetwarzania danych osobowych znajdują się

wyłącznie w pomieszczeniach zabezpieczonych zamkami,

b) dostęp do pomieszczenia, w którym znajdują się urządzenia serwerowe ma tylko Administrator Danych Osobowych oraz Administrator Systemu Informatycznego, a w uzasadnionych przypadkach Inspektor ochrony danych,

c) zbędne dokumenty papierowe zawierające dane osobowe mogą być niszczone wyłącznie w niszczarkach,

d) urządzenia na których znajdują się bazy danych osobowych – serwery powinny być podłączone do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania,

e) sieć lokalna podłączona jest do internetu poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną,

f) codzienne kopie zapasowe są wykonywane automatycznie poprzez odpowiednie ustawienia w systemach informatycznych,

g) okresowo są wykonywane kopie zapasowe na nośniki zewnętrzne.

6. W Akademii stosowane są następujące środki ochrony w ramach narzędzi informatycznych i innych narzędzi programowych oraz środki ochrony w ramach systemu użytkowego:

a) identyfikator i hasło dostępu do danych na poziomie aplikacji - dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator, użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia,

b) komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem, stosowane jest wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika, stosowana jest blokada hasłem podczas dłuższej nieaktywności użytkownika,

c) na komputerach stosuje się hasło administracyjne oraz hasło użytkownika;

d) hasła są konstruowane w następujący sposób:

- hasło dostępu do stacji roboczej lub oprogramowania powinno składać się z co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
- dokonywać zmiany hasła, w przypadku, gdy nie jest to wymuszone przez system, nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
- hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: imion, nazwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów. Hasło nie może być identyczne z loginem.
- zobowiązana jest do zachowania hasła w poufności, nawet po utracie przez nie ważności i odpowiada za wszystkie działania wykonane z wykorzystaniem osobistego loginu i hasła.
- zabronione jest przekazywanie haseł innym osobom oraz zapisywanie haseł w sposób jawny (np. na karteczkach samoprzylepnych, w komputerze); pierwsze hasło nadane przez administratora danych osobowych jest przekazywane użytkownikowi systemu w sposób uniemożliwiający zapoznanie się z nim osób postronnych i niezwłocznie przez niego zmieniane.

e) wszystkie elementy sieci informatycznej są zabezpieczone hasłami, elementy takie jak routery, drukarki z dyskami, stacje robocze w zakresie hasła administracyjnego i podobne są zabezpieczone przez Administratora Systemów Informatycznych znanemu jemu oraz deponowane w kopercie u kierownictwa Administratora Danych Osobowych;

f) Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

g) W przypadku likwidacji nośników informatycznych zawierających Dane Osobowe lub kopie

zapasowe Systemów Informatycznych służących do przetwarzania Danych Osobowych należy przed ich likwidacją usunąć Dane Osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

h) Nie przechowuje się zbędnych nośników informacji zawierających zbędne Dane Osobowe oraz kopie zapasowe, a także wydruków i innych dokumentów zawierających Dane Osobowe, których przechowywanie nie jest uzasadnione celem ich przetwarzania.

i) Nośniki informacji zawierające Dane Osobowe oraz Kopie Zapasowe, a także wydruki i inne dokumenty zawierające Dane Osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania Danych Osobowych, w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

j) Po upływie użyteczności Danych Osobowych, o ile przepis szczególny nie stanowi inaczej, Dane Osobowe są kasowane lub niszczone tak, aby nie było możliwe ich odtworzenie. Dozwolona jest również ich anonimizacja polegająca na pozbawieniu danych umożliwiających identyfikację określonej osoby fizycznej.

k) W przypadku uszkodzenia lub zużycia nośników informacji zwierających Dane Osobowe są one fizycznie niszczone (we własnym zakresie lub przez podmiot profesjonalnie zajmujący się takimi czynnościami) tak, aby nie było możliwe odczytanie danych osobowych. Ze zniszczenia sporządzany jest raport.

l) Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego stosowane jest oprogramowanie antywirusowe. Oprogramowanie obejmuje każdy element systemu informatycznego wymagający ochrony. Konieczność ochrony poszczególnych elementów systemu informatycznego określa Administrator Systemów Informatycznych.

m) Każdy zbiór wczytywany do komputera, podłączane urządzenie, w tym także wiadomość e-mail, musi być przeskanowany programem antywirusowym.

n) Na każdym stanowisku wyposażonym w dostęp do sieci publicznej (Internet) musi być zainstalowanie oprogramowanie antywirusowe oraz program firewall. Niedopuszczalne jest stosowanie dostępu do sieci publicznej (Internet) bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

o) w przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności Administratora Systemu Informatycznego lub Inspektora danych osobowych.

p) przeglądy techniczne sprzętu komputerowego są dokonywane przy każdej czynności w toku codziennych prac jednakże nie rzadziej niż raz w roku.

q) w systemie informatycznym instalowane są zalecane przez producentów oprogramowania poprawki i uaktualnienia. Poprawki i uaktualnienia służą do wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

r) w przypadku powierzenia określonego składnika systemu informatycznego w postaci programu komputerowego dostarczanego przez licencjodawcę programu komputerowego, postanowienia dotyczące poufności oraz przetwarzania danych osobowych będą regulowane na podstawie umowy licencyjnej lub umowy dotyczącej przetwarzania danych osobowych będącej uzupełnieniem umowy licencyjnej.

§ 15
Postanowienia końcowe

1. Integralną częścią niniejszego regulaminu są następujące załączniki:
    a) wzór formularza upoważnienia/odwołania upoważnienia do przetwarzania danych osobowych,
    b) wzór ewidencji osób upoważnionych do przetwarzania danych osobowych,
    c) wzór oświadczenia pracownika (w tym osoby zatrudnionej na innej niż umowa o pracę podstawie prawnej) przetwarzającego dane osobowe,
    d) wzór klauzuli informacyjnej dla pracownika/osoby przetwarzającej dane osobowe
    e) procedura nadawania upoważnień;
    f) procedura reagowania i oceny naruszeń bezpieczeństwa danych osobowych;
    g) procedura udzielania informacji podawanej w przypadku pozyskiwania danych;
    h) procedura realizowania uprawnień osób, których dane są przetwarzane;
    i) procedura opiniowania zagadnień prawnych związanych z danymi osobowymi;
2. W celu wykonania niniejszej Polityki ochrony danych osobowych wydawane będą dodatkowe dokumenty takie jak procedury, instrukcje czy zarządzenia. W tym celu mogą być prowadzone także listy i wykazy.
3. W celu wykonania niniejszej Polityki ochrony danych osobowych prowadzone będą w osobnych dokumentach rejestry czynności przetwarzania danych osobowych ewentualnie kategorii danych osobowych.
4. Wskazana treść wzorów w lit. a) do d) może być modyfikowane w pojedynczych przypadkach, gdy jest to uzasadnione stanem faktycznym.

Załącznik nr 1
do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

Upoważnienie do Przetwarzania Danych Osobowych
numer:

Na podstawie **art. 29 RODO upoważniam:**

Panią/Pana

zatrudnioną na stanowisku

……

(od ……. r.)

do przetwarzania danych osobowych w zbiorach prowadzonych przez **administratora w zakresie wykonywanych obowiązków wyznaczonych przez przełożonego oraz w systemach informatycznych do których dostęp został Pani/Panu nadany.**

Upoważnienie obejmuje przetwarzanie danych w zbiorach i zakresie niezbędnym w celu prawidłowego wykonywania powierzonych czynności, w tym systemach informatycznych do których został nadany dostęp przez **Administratora**.

Upoważnienie wygasa z chwilą rozwiązania stosunku pracy, czasu pełnienia funkcji lub trwania umowy cywilnoprawnej, a także cofnięcia Upoważnienia przez **Administratora.**

Upoważnienie niniejsze zastępuje dotychczasowo wydane upoważnienie.

Warszawa, dnia …….. r.

.....

podpis osoby upoważnionej do nadawania upoważnienia

Odwołanie Upoważnienia nr …
do przetwarzania danych osobowych

Niniejszym odwołuję upoważnienie do przetwarzania danych osobowych

Pani/Pana

……..

zatrudnioną/ego na stanowisku

…….

(od ……..)

i zobowiązuję do niezwłocznego zaprzestania ich przetwarzania**.**

Warszawa, dnia …….. r.

.....

podpis osoby upoważnionej do odwoływania upoważnień

Załącznik nr 2
do Zarządzenia Rektora Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

Nr	Nazwisko, Imię	Stanowisko	Okres upoważnienia		Uwagi
			Od	Do	

Załącznik nr 3
do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

Oświadczenie o zachowaniu poufności Przetwarzanych Danych Osobowych

Imię i nazwisko:

Ja niżej podpisany/a oświadczam, iż:

- zostałem/am zaznajomiony/a z przepisami dotyczącymi ochrony Danych Osobowych i znana jest mi treść przepisów prawa w tym zakresie, w szczególności Rozporządzenie 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) z dnia 27 Kwietnia 2016 R. (Dz.Urz.Ue.L Nr 119, Str. 1);
- znana mi jest treść dokumentów wewnętrznych obowiązujących w jednostce**;**
- znane są mi również konsekwencje prawne oraz służbowe, jakie ponosi osoba niestosująca się do wymogów określonych we wspomnianych powyżej przepisach i procedurach;
- znany jest mi fakt, iż przetwarzane przeze mnie Dane Osobowe są poufne i chronione i nie mogą być wykorzystywane w celach innych niż powierzone przez jednostkę;

Niniejszym zobowiązuję się do:

- przestrzegania w/w przepisów i procedur obowiązujących w jednostce;
- zachowania w poufności informacji oraz Danych Osobowych nich zawartych;
- wykorzystywania Danych Osobowych wyłącznie w celu wypełnienia obowiązków powierzonych w jednostce;
- nieujawniania Danych Osobowych innym osobom pracującym w jednostce niż te, którym jest to niezbędne do zrealizowania obowiązków powierzonych w jednostce;

.....
podpis osoby składającej oświadczenie

Załącznik nr 4
do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

Obowiązek informacyjny

1. Administrator danych oraz inspektor ochrony danych

Administratorem Pani/Pana danych osobowych jest Akademia Teatralna im. Aleksandra Zelwerowicza w Warszawie, ul. Miodowa 22/24; 00-246 Warszawa, w dalszej części zwany jako „Akademią". Jeśli ma Pani/Pan jakiekolwiek pytania dotyczące sposobu, celów lub zakresu przetwarzania danych osobowych przez Akademię lub pytania dotyczące przysługujących Pani/Panu uprawnień, prosimy o kontakt z Akademią na adres: ul. Miodowa 22/24; 00-246 Warszawa bądź z inspektorem ochrony danych na adres e-mail: patryk.koralewski@at.edu.pl

2. RODO

RODO to Rozporządzenie 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. RODO reguluje kwestie związane z przetwarzaniem danych osobowych i ma zastosowanie od dnia 25 maja 2018 r.

3. Cele oraz podstawy prawne przetwarzania Pani/Pana danych osobowych

Akademia przetwarza Pani/Pana dane osobowe w celu wykonania umowy łączącej Panią/Pana z Akademią (podstawa prawna: art. 6 ust. 1 lit. b RODO) oraz wypełnienia obowiązków nałożonych przepisami prawa art. 6 ust. 1 lit. c RODO. W innych przypadkach Pani/Pana dane osobowe przetwarzane będą wyłącznie na podstawie udzielonej zgody (podstawa prawna: art. 6 ust. 1 lit. a RODO), w celu określonym w treści zgody.

4. Obowiązek podania danych osobowych

Podanie przez Panią/Pana danych osobowych w przypadku wykonania umowy, podanie danych jest warunkiem zawarcia umowy, a w przypadku realizacji obowiązków nałożonych przepisami prawa jest wymogiem ustawowym i jest obligatoryjne. Brak podania przez Panią/Pana wymaganych danych osobowych może stanowić przeszkodę uniemożliwiającą zawarcie umowy. W zakresie, w jakim dane osobowe są zbierane na podstawie zgody, podanie danych osobowych jest dobrowolne.

5. Informacje o odbiorcach Pani/Pana danych osobowych

Pani/Pana dane osobowe mogą być udostępniane następującym odbiorcom bądź kategoriom odbiorców danych:

1. organom władzy publicznej oraz podmiotom wykonującym zadania publiczne lub działającym na zlecenie organów władzy publicznej, w zakresie i dla celów wynikających z obowiązujących przepisów prawa,

2. podmiotom wspierającym Akademię w realizacji jego procesów biznesowych i operacyjnych, w tym podmiotom przetwarzającym dane osobowe w imieniu Akademii,

6. Okresy przetwarzania danych osobowych

Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji celów przetwarzania wskazanych w pkt. 3 powyżej, tj. przez okres:

a. obowiązywania umowy łączącej Panią/Pana z Akademią,
b. wypełniania obowiązków prawnych ciążących na Akademii, w tym obowiązków związanych z przechowywaniem danych, np. dla celów sprawozdawczości finansowej,
c. realizacji przez Akademię jej prawnie uzasadnionych interesów, w szczególności przez przewidziane w odrębnych przepisach okresy przedawnienia roszczeń,
d. do czasu wycofania zgody – o ile przetwarzanie odbywa się na podstawie wyrażonej przez Panią/ Pana zgody.

7. Profilowanie oraz zautomatyzowane podejmowanie decyzji

Pani/ Pana dane osobowe nie będą podlegały profilowaniu. Akademia nie będzie podejmowała zautomatyzowanych decyzji w przetwarzaniu danych osobowych.

8. Prawa osoby, której dane dotyczą

W związku z przetwarzaniem Pani/Pana danych osobowych przez Akademię, przysługują Pani/Panu następujące prawa:
a. prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych,
b. prawo do żądania sprostowania (poprawienia) danych,
c. prawo do żądania usunięcia danych osobowych (tzw. „prawo do bycia zapomnianym"),
d. prawo do żądania ograniczenia przetwarzania danych osobowych,
e. prawo do przenoszenia danych do Pani/ Pana lub do innego administratora danych,
f. prawo do sprzeciwu wobec przetwarzania danych osobowych.

W powyższych uprawnień może Pani/Pan skorzystać:
a. składając wniosek w naszej siedzibie,
b. przesyłając wniosek na adres: ul. Miodowa 22/24; 00-246 Warszawa,
c. przesyłając wniosek drogą mailową na adres: patryk.koralewski@at.edu.pl

Zakres każdego z powyższych uprawnień oraz sytuacje, w których Pani/Pan może z nich skorzystać, są określone przepisami prawa. Możliwość skorzystania z niektórych z ww. uprawnień może być uzależniona m.in. od podstaw prawnych, celu lub sposobu ich przetwarzania.

9. Prawo do cofnięcia zgody na przetwarzanie danych osobowych

W zakresie, w jakim udzielona została przez Panią/Pana zgoda na przetwarzanie danych osobowych, przysługuje Pani/Panu prawo do cofnięcia tej zgody. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

10. Prawo wniesienia skargi do organu nadzorczego

W przypadku uznania, że przetwarzanie przez Akademię Pani/Pana danych osobowych narusza przepisy obowiązującego prawa, może Pani/Pan wnieść skargę do organu nadzorczego – Urzędu Ochrony Danych Osobowych.

11. Przekazywanie danych osobowych do podmiotów spoza Europejskiego Obszaru Gospodarczego („EOG") lub organizacji międzynarodowych

Akademia nie planuje przekazywać Pani/Pana danych osobowych do podmiotów spoza EOG ani do organizacji międzynarodowych.

Załącznik nr 5
do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

PROCEDURA
nadawania upoważnień

Podmioty realizujące

1. Administrator danych osobowych (Administrator lub ADO);
2. Inspektor Danych Osobowych (IOD);
3. Pracownik.

Cel procedury

Celem procedury jest zapewnienie dopuszczenia wyłącznie osób, które powinny przetwarzać danedo przetwarzania osób,

Nadawanie upoważnień

1. **Forma i źródło upoważnienia.**Upoważnienie do przetwarzania danych osobowych w jednostce nadawane jest przezAdministratora (lub wyznaczonego pracownika, w tym IOD), który decyduje o zakresie nadanych uprawnień. Upoważnienie może wynikać z każdego polecenia Administratora (polecenie przetwarzania danych), które w wyraźny i jasny sposób umocowuje osobę upoważnioną do działania i przetwarzania danych osobowych. Nadanie upoważnienia, a tym samym polecenie przetwarzania danych, może przyjąć formę lub wynikać z:
   a) polecenia (w dowolnej formie) do wykonania czynności wymagających przetwarzania danych osobowych (polecenie przetwarzania danych),
   b) przyznania dostępu do zasobów informatycznych Administratora w tym stacji roboczych i oprogramowania, w którym są przetwarzane dane osobowe;
   c) z umocowania ustawowego,
   d) umowy wiążącej strony,
   e) zostać sformalizowane w dokumencie upoważnienia,
2. **Dokument upoważnienia.**W przypadku wydania osobnego dokumentu upoważnienia jest ono podpisywane przez IOD, przy czym jego zakres wyznacza Administrator poprzez podjęcie określonych w pkt. 3 działań. Rozliczalność zapewniona zostanie poprzez prowadzenie odrębnych list upoważnień (może być powadzone w jednej liście lub w związku z prowadzeniem innej listy np. umów powierzenia)
3. **Zakres upoważnienia do przetwarzania danych.**Zakres upoważnienia określany jest wydawanymi poleceniami przetwarzania Administratora. Polecenie przetwarzania danych osobowych wynika w szczególności z:
   a) nadania uprawnień do określonych zasobów informatycznych (programów lub ich modułów służących przetwarzaniu danych osobowych oraz przypisania uprawnień w zasobie informatycznym);
   b) umowy (o pracę, zlecenie, dzieło etc.) określającej zakres obowiązków osoby, która przetwarza dane osobowe;
   c) opisu stanowiska pracy;
   d) celu w jakim Administratorudostępnił dane osobowe, osobie je przetwarzającej;
   e) przepisu prawa;
   f) powierzenia pełnienia określonejfunkcji (członek komisji ZFŚS, członek zarządu);
   g) indywidualnego polecenia (np. polecenia służbowego)w tym wyrażonego w formie elektronicznej,
   h) ustanowionych procedur i instrukcji obowiązującej w jednostce dotyczących rozstrzygania spraw.
4. Zakres upoważnienia lub jego modyfikacja może następować poprzez zmianę wskazanych w pkt. 3 poleceń Administratora w tym w szczególności modyfikacji uprawnień do określonych zasobów informatycznych. Upoważnienie wygasa wraz z odwołaniem upoważnienia, ustania stosunku prawnego pomiędzy Administratorem i osobą upoważnioną, a także zaprzestania pełnienia wyznaczonej funkcji, chyba, że Administrator postanowi inaczej.
5. Upoważniony do przetwarzania danych osobowych jest zobowiązany do zachowania poufności złożonego wodrębnym oświadczeniu, wumowie, wyrażone wprzepisach prawa (dotyczących tajemnicy zawodowej, obowiązków wobec pracodawcy wynikających z kodeksu pracy) lub inny sposób.

Załącznik nr 6
do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

PROCEDURA
reagowania i oceny naruszeń bezpieczeństwa danych osobowych

Podmioty realizujące:

1. Inspektor Ochrony Danych (IOD).
2. Administrator Systemów Informatycznych (ASI).
3. Administratora Danych Osobowych (ADO).
4. Pracownik.

Naruszenie

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Wszczęcie postępowania i działania

Inspektor Ochrony Danych na podstawie zgłoszenia podejmuje działania mające na celu:

- ograniczenie do minimum negatywnych skutków zdarzenia;
- wyjaśnienie okoliczności zdarzenia;
- sporządzenie raportu z podjętych czynności;
- zgłoszenia (w przypadkach naruszeń skutkujących ryzykiem naruszenia praw lub wolności osób fizycznych) Prezesowi Urzędu Ochrony Danych Osobowych, Administratorowi Danych (w przypadku przetwarzania danych w imieniu innego podmiotu – w roli procesora);
- zgłaszania (w przypadku naruszeń może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych) osoby/osób, których dane uległy naruszeniu;
- poinformowania kierownictwa jednostki o stwierdzonym naruszeniu w celu podjęcia stosowanych działań naprawczych.

Inspektor Ochrony Danych w ramach powyższych działań ma prawo do podejmowania wszelkich dopuszczalnych prawem działań, w szczególności:

- żądania wyjaśnień od osób zatrudnionych przez Administratora Danych Osobowych;
- nakazania przerwania pracy przy przetwarzaniu danych osobowych;
- żądania podjęcia niezwłocznych działań przez ASI.

W przypadku naruszenia bezpieczeństwa danych osobowych działania, określonych w niniejszej procedurze powinny mieć pierwszeństwo przed innymi poleceniami.

Postępowanie

1. **Stwierdzenie naruszenia**. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, każdy pracownik, który stwierdzi naruszenie ma obowiązek zgłoszenia tego faktu Inspektorowi Ochrony Danych Osobowych niezwłocznie i stosować się do jego wskazówek.
2. **Analiza.** W przypadku wykrycia przez Administratora naruszenia ochrony danych osobowych dokonuje sie analizy pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych wynikiem, której może być stwierdzenie naruszenia lub incydentu.
3. **Naruszenie**. W przypadku stwierdzenia, iż jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (**naruszenie**),
    a. naruszenie nie wymaga zgłaszania Prezesowi Urzędu Ochrony Danych Osobowych,
    b. naruszenie nie wymaga zgłaszania osobie, której dane osobowe naruszono,

c. ocenę prawdopodobieństwa uzasadnia się i udokumentowuje, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze
d. naruszenie zostaje wpisane do ewidencji naruszeń (oznaczając jako „naruszenie").

4. **Incydent.** W przypadku stwierdzenia, iż jest prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (**incydent**):
   a. naruszenie wymaga zgłaszania Prezesowi Urzędu Ochrony Danych Osobowych;
   b. ocenę prawdopodobieństwa uzasadnia się i udokumentowuje, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze;
   c. naruszenie zostaje wpisane do ewidencji naruszeń (oznaczając jako „naruszenie");
   d. przeprowadza się ocenę pod kątem konieczności jej zgłoszenia osobie, której dane dotyczą (zgodnie z pkt. 7 poniżej) i podejmuje na tej postawie stosowne, kroki.
5. **Informowanie Prezesa Urzędu Ochrony Danych Osobowych o incydencie.** Incydent należy zgłosić Prezesowi Urzędu Ochrony Danych Osobowych w terminie 72 godzin od stwierdzenia naruszenia. W przypadku przetwarzania danych osobowych w imieniu Administratora danych osobowych (jako procesor) Incydent należy zgłosić Administratorowi w terminie przewidzianym w umowie z Administratorem.
6. **Zgłoszenie.** Zgłoszenie musi obejmować, co najmniej, następujące elementy:
   a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d. opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
      - jeżeli, i w zakresie, w jakim, informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
      - zgłoszenia dokonuje Administrator danych osobowych we współpracy z Inspektorem Ochrony Danych.
7. **Informowanie osoby, której danych dotyczy Incydent.** Incydent należy zgłosić osobie, której dane dotyczą w przypadku stwierdzenia, iż Incydent może powodować wysokie ryzyko naruszenia praw lub wolności tej osoby. Zgłoszenia należy dokonać bez zbędnej zwłoki.
8. **Zawiadomienie.** Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia zdanych osobowych oraz zawiera przynajmniej informacje i środki:
   a. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   b. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   c. opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
      - zgłoszenia dokonuje Administrator danych osobowych we współpracy z Inspektorem Ochrony Danych.
9. **Wyjątki.** Zawiadomienie, o którym mowa w powyżej, nie jest wymagane, w następujących przypadkach:
   a. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
   c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załącznik nr 7
d do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

PROCEDURA
udzielania informacji podawanej w przypadku pozyskiwania danych

Podmioty realizujące

1. Administrator danych osobowych (Administrator lub ADO);
2. Wyznaczani pracownicy (zgromadzenie niezbędnych danych oraz techniczna realizacja wniosku, poinformowanie IOD);
3. Inspektor danych osobowych (także „IOD" - w zakresie oceny treści obowiązku informacyjnego).

Cel:

Dane mogą być zbierane przez Administratora:

a. od osoby, której dane dotyczą;
b. w sposób inny niż od osoby, której dane dotyczą;

W zależności od sposobu zbierania danych przez Administratora osobie przysługują następujące informacje:

1. w przypadku zbierania danych od osoby, której dane dotyczą, Administrator podaje;
    a. **Dane.** Swoją tożsamość i dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
    b. **Dane IOD**. Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
    c. **Cele.** Cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
    d. **Interes prawny.** Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
    e. Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
    f. Gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.
    g. Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
    h. Informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
    i. Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
    j. Informacje o prawie wniesienia skargi do organu nadzorczego;
    k. Informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
    l. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Zmiana celu. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż

cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

Dysponowanie danymi. Nie udziela się powyższych informacji, gdy i w zakresie, w jakim, której dane dotyczą, dysponuje już tymi informacjami.

Termin udzielenia informacji. Informacji należy udzielić podczas ich zbierania.

2. W przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, Administrator podaje:
    a. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
    b. gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
    c. cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
    d. kategorie odnośnych danych osobowych;
    e. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
    f. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia;
    g. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
    h. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
    i. informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
    j. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
    k. informacje o prawie wniesienia skargi do organu nadzorczego;
    l. źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
    m. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

    Termin udzielenia informacji.
    a. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
    b. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;
    c. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

    Zmiana celu. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych

informacji.

Wyjątki. Powyższe nie ma zastosowania, gdy i w zakresie, w jakim:

a. osoba, której dane dotyczą, dysponuje już tymi informacjami;
b. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
c. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;
d. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Procedura postępowania w sprawie udzielenia obowiązku informacyjnego.

2. W przypadku pozyskiwania danych osobowych należy, każdą taką sytuację skonsultować z IOD, dostarczając mu wszelkich informacji koniecznych do określenia zakresu obowiązku informacyjnego. W szczególności dane o celu przetwarzania danych, podmiotom, którym dane będą udzielane, termin przetwarzania danych, planowany sposób zbierania danych.
3. IOD określa zakres, treść i sposób spełnienia obowiązku informacyjnego i przedstawia kierownictwu jednostki.
4. Za techniczne spełnienie żądania odpowiada Administrator danych osobowych oraz wyznaczony przez niego pracownik/pracownicy.
5. Treść obowiązku informacyjnego odnotowuje się w ewidencji.

Załącznik nr 8
do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

PROCEDURA
realizowania uprawnień osób, których dane są przetwarzane

Osobie, której dane są przetwarzane przysługują następujące prawa:

a. prawo do dostępu do danych osobowych;
b. prawo do sprostowania danych;
c. Prawo do usunięcia danych („prawo do bycia zapomnianym");
d. Prawo do ograniczenia przetwarzania;
e. Prawo do przenoszenia danych;
f. Prawo do sprzeciwu.

Podmioty realizujące:

1. Administrator danych osobowych (Administrator lub ADO);
2. Wyznaczani pracownicy (zgromadzenie niezbędnych danych oraz techniczna realizacja wniosku, poinformowanie IOD);
3. Inspektor danych osobowych (także „IOD" - w zakresie oceny jakie prawo i w jakim zakresie przysługuje osobie).

Procedura realizacja praw.

1. W przypadku zgłoszenia żądania dotyczącego prawa do sprostowania danych, osoba otrzymująca zawiadomienie, kieruje zapytanie, o to czy dane określonej osoby są przetwarzane przez jednostkę oraz przesyła informację do IOD.
2. IOD ocenia uprawnienie do spełnienia żądania oraz określa zakres udzielonej odpowiedzi i spełnienia żądania.
3. IOD lub wyznaczony pracownik w jego imieniu, udziela odpowiedzi na treść żądania, podmiotowi, który zgłosił pytanie.
4. Za techniczne spełnienie żądania odpowiada Administrator Danych Osobowych oraz wyznaczony przez niego pracownik/pracownicy.
5. Spełnienie żądania odnotowuje się w ewidencji spełnienia żądań. Uzasadnienie jej prowadzenia wynika z do konieczności ustalenia, dochodzenia lub obrony roszczeń.

Sposób realizacji praw

Komunikacja. Komunikacja w sprawach realizacji praw, osoby, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (w szczególności, gdy informacje są kierowane do dziecka).

Forma. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

Potwierdzenie tożsamości: Osoba udzielająca informacji ustnie powinna na podstawie zgromadzonych danych zapytać się o co najmniej dwie dane dotyczące osoby pytającego np. numer PESEL, imię ojca, dane adresowe, adres e-mail na który wysyłane są mu informacje. Brak takiego potwierdzenia uniemożliwia udzielenie odpowiedzi.

Odmowa: Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej praw. W przypadkach, o których mowa w art. 11 ust. 2 RODO, Administrator nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać prawa jej przysługujących(art. 15–22 RODO), chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

Termin. Administrator bez zbędnej zwłoki – a w każdym razie **w terminie miesiąca** od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem dotyczących jej praw(na podstawie art. 15–22 RODO).

Przedłużenie terminu. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

Niepodjęcie działań. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Opłaty. Komunikacja i działania podejmowane w celu realizacji praw (na mocy art. 15-22 i 34 RODO) są wolne od opłat.

Opłaty – wyjątek. Jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator może:

a. pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
b. odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Administratorze.

Żądanie dodatkowych informacji co do tożsamości. Bez uszczerbku dla art. 11 RODO, jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie dotyczące jej praw (art. 15–21 RODO), może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Wytyczne w sprawie udzielania odpowiedzi

Prawo dostępu do danych osobowych

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   a. cele przetwarzania;
   b. kategorie odnośnych danych osobowych;
   c. informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d. w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e. informacje o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f. informacje o prawie wniesienia skargi do organu nadzorczego;
   g. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
   h. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. **Państwa trzecie.** Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.
3. **Kopia danych.** Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.
4. **Koszty kolejnych kopii.** Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.
5. **Ograniczenie.** Prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych.

Prawo sprostowania danych. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Administrator informuje o sprostowaniu, którego dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Prawo do usunięcia danych - prawo do bycia zapomnianym.

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, **jeżeli** zachodzi jedna z następujących okoliczności:
   a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. **6 ust. 1 lit. a)** lub art. 9 **ust. 2 lit. a)** RODO, **i** nie ma innej podstawy prawnej przetwarzania;
   c. osoba, której dane dotyczą, wnosi sprzeciw na mocy **art. 21 ust. 1 RODO** wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy **art. 21 ust. 2** wobec przetwarzania;
   d. dane osobowe były przetwarzane niezgodnie z prawem;
   e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;
   f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. **8 ust. 1**.

2. Jeżeli Administrator upublicznił dane osobowe, ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować Administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by Administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Punkt 1 i 2 powyżej nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
   a. do korzystania z prawa do wolności wypowiedzi i informacji;
   b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
   c. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z **art. 9 ust. 2 lit. h)** oraz **i)** i **art. 9 ust. 3** RODO;
   d. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
   e. do ustalenia, dochodzenia lub obrony roszczeń.

Administrator informuje usunięciu danych osobowych, którego dokonał, każdego odbiorcę, któremu ujawniono

dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Prawo do ograniczenia przetwarzania.

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania w następujących przypadkach:
   a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
   b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   c. Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   d. osoba, której dane dotyczą, wniosła sprzeciw na mocy **art. 21 ust. 1 RODO** wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Ograniczenie przetwarzania danych osobowych polega na tym, iż dane, których dotyczy można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

Administrator informuje o ograniczeniu przetwarzania, którego dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Prawo do przenoszenia danych.

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane osobowe innemu Administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe, jeżeli:
   a. przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO;
   b. przetwarzanie odbywa się w sposób zautomatyzowany.

2. Wykonując prawo do przenoszenia danych na mocy, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu Administratorowi, o ile jest to technicznie możliwe.
3. Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku dla art. **17 RODO**. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.
4. Prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

Prawo do sprzeciwu.

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na **art. 6 ust. 1 lit. e)** lub **f) RODO**, w tym profilowania na podstawie tych przepisów.
2. Administratorowi nie wolno przetwarzać danych w stosunku do których służy prawo sprzeciwu po jego wniesieniu, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do sprzeciwu - marketing bezpośredni. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

Prawo do sprzeciwu – badania naukowe, historyczne i statystyczne. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie.

1. **Decyzje.** Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
2. Osoba, które dane dotyczą ma prawo sprzeciwu do przetwarzania jej danych polegających na profilowaniu.
3. Punkt1 powyżej nie ma zastosowania, jeżeli ta **decyzja**:
   a. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem;
   b. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;
   c. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
4. W przypadkach, o których mowa w ust. 2 lit. a) i c), Administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony Administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
5. Decyzje, o których mowa w pkt. 3, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1 RODO, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Załącznik nr 9
do Zarządzenia Rektora Akademii Teatralnej im. A. Zelwerowicza w Warszawie
nr 21/2018 z dnia 24 maja 2018, zmienionego Zarządzeniem nr 6/2019 z dnia 27 marca 2019 r.

PROCEDURA
opiniowania zagadnień prawnych związanych z danymi osobowymi

Podmioty realizujące

1. Administrator danych osobowych (Administrator lub ADO);
2. Kierownicy jednostki organizacyjnej;
3. Inspektor Danych Osobowych (IOD);
4. Pracownik.

Cel. Celem procedury jest informowanie o obowiązkach wynikających z przepisów dotyczących ochrony danych osobowych oraz doradzanie ADO, kierownikom jednostki organizacyjnej i pracownikom w tych kwestiach.

Procedura jest stosowana w zakresie nie regulowanym przez inne procedury obowiązujące u ADO, w szczególności dotyczy opiniowanie zagadnień prawnych dotyczących przetwarzania danych osobowych oraz opiniowania umów pod kontem przetwarzania danych osobowych.

Procedura opiniowania zagadnień prawnych.

1. Każdy osoba, która ma uzasadnione wątpliwości co zgodności przetwarzania danych osobowych z przepisami prawa ma prawo i obowiązek zwrócenia się z wnioskiem do IOD z zapytaniem dotyczącym przetwarzania danych osobowych, które dotyczą w szczególności:
   a. opiniowania zagadnień prawnych;
   b. opiniowania umów;
   c. zbierania danych osobowych, podstaw prawnych w szczególności wyrażania zgody;
   d. wprowadzania nowych procesów (czynności) przetwarzania danych osobowych;
   e. organizowanie konkursów i promocji;
   f. udostępniania danych osobowych;
   g. powierzenia danych osobowych na podstawie art. 28 RODO;
   h. wprowadzania nowych systemów informatycznych w celu przetwarzania danych osobowych;
   i. wprowadzenia nowych sposobów zabezpieczania miejsc fizycznych i środków informatycznych.
2. IOD pełni rolę opiniującą i doradczą w tym zakresie. Ostateczną decyzję w zakresie zastosowania się do jego wytycznych i opinii należy do ADO lub umocowanego do tego pracownika.
3. IOD odpowiada na pytanie, o ile analogiczny problem nie był już przez niego wyjaśniany.
4. Wniosek składany jest na adres e-mail IOD lub formie tradycyjnej (papierowej) i powinien zawierać następujące informacje:
   a. zapytanie oraz opis stanu faktycznego dotyczącego przetwarzania danych osobowych;
   b. dotychczasowe postępowanie w tego typu sprawach, o ile występowało;
   c. sugestię rozwiązania problemu z uwzględnieniem specyfiki działania określonej komórki organizacyjnej lub dotychczasową praktykę w tym zakresie (o ile przewiduje się zastosowanie konkretnych rozwiązań).
5. Po otrzymaniu wniosku IOD formułuje odpowiedz na piśmie (dozwolona jest forma elektroniczna), niezwłocznie, przy czym nie dłużej niż w terminie 7 dni roboczych od uzyskania wszystkich niezbędnych informacji dotyczących wniosku i przedstawia je osobie wnioskującej oraz podaje do wiadomości kierownictwu.
6. Na żądanie IOD udzielane są mu dodatkowe wyjaśnienia lub dostarczane dokumenty pozwalające na weryfikację przedstawionego zagadnienia z przepisami prawa.
7. Udzielenie niepełnych, nieprawdziwych lub niewyczerpujących informacji IOD może prowadzić do wydania nieprawidłowej odpowiedzi, za co IOD nie ponosi odpowiedzialności. Stąd też w przypadku jakiejkolwiek wątpliwości co do przyjętego za podstawę rozwiązania stanu faktycznego, osoba otrzymująca odpowiedź powinna zgłosić te wątpliwości lub uwagi do IOD.