Zarządzenie nr 2/2024
Rektora Akademii Teatralnej im. Aleksandra Zelwerowicza
z dnia 11 stycznia 2024 roku

w sprawie wprowadzenia Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie

Na podstawie art. 23 ust. 1 i ust. 2 pkt 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2023, poz. 742 z późn. zm.) oraz § 12 ust. 1 i 2 Statutu Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie, postanawiam co następuje:

§ 1

1. Wprowadzam Politykę ochrony informacji oraz danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie, zwaną dalej „Polityką ochrony informacji", stanowiącą załącznik nr 1 do Zarządzenia.

§ 2

1. Z dniem wejścia w życie niniejszego zarządzenia uchyla się następujące Zarządzenia Rektora Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie:
    a) Zarządzenie 51/2021 z dnia 22 grudnia 2021 roku w sprawie w sprawie wprowadzenia Polityki ochrony danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie.
    b) Zarządzenie nr 46/2022 z dnia 30 grudnia 2022 roku w sprawie zmiany zarządzenia nr 51/2021 z dnia 22 grudnia 2021 roku w sprawie wprowadzenia Polityki ochrony danych osobowych w Akademii Teatralnej im. Aleksandra Zelwerowicza w Warszawie

§ 3

1. Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

/- / Prof. dr hab. Wojciech Malajkat

Załącznik 1

do Zarządzenia nr 2/2024 z dnia 11 stycznia 2024 roku

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

SPIS TREŚCI

§ 1
Postanowienia ogólne

1. Polityka ochrony informacji oraz danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie będącym Administratorem Danych Osobowych (dalej: „ADO") jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu informacji oraz danych osobowych we wszystkich zbiorach i procesach przetwarzania informacji oraz danych osobowych przetwarzanych przez ADO, w tym danych przetwarzanych w systemie informatycznym.
2. Polityka ochrony informacji oraz danych osobowych dąży do realizacji zasad wyrażonych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (dalej KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Danych stanowiących dane osobowe w rozumieniu art. 4 Rozporządzenia 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. ADO 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 informacji oraz danych osobowych określonych w:
    a) Konstytucji Rzeczypospolitej Polskiej,
    b) Rozporządzeniu RODO,
    c) KRI;
    d) innych przepisach wydanych i przyjętych w celu realizacji ochrony danych osobowych w tym aktach wewnętrznych.
5. ADO dąży do realizacji zasad, które wskazują, iż informacje oraz 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. ADO przestrzegając zasad wskazanych w ust. 4 wykazuje ich przestrzeganie („rozliczalność”) m.in. poprzez prowadzoną dokumentacją mającą na celu realizację niniejszej Polityki ochrony danych osobowych.
7. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

§ 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. KRI - ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (dalej KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
3. Informacje – oznaczają wszelkie dane przetwarzane w ramach wypełniania funkcji powierzonych ADO.
4. 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.
5. Zbiór danych osobowych - dane osobowe zgromadzone w usystematyzowany sposób według kryterium rodzaju danych, celu albo osoby/działu przetwarzającej w jednostce.
6. 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.
7. ADO – Administrator Danych Osobowych, Akademia Teatralna im. A. Zelwerowicza w Warszawie a w jego imieniu Rektor.
8. Inspektor Ochrony Danych (dalej „IOD”) – osoba wyznaczona przez ADO, zgodnie z art. 37 Rozporządzenia RODO, odpowiedzialna za zadania określone w § 3 Polityki ochrony danych osobowych.
9. Administrator Systemu Informatycznego (dalej „ASI”) - osoba wyznaczana przez ADO odpowiedzialna za przestrzeganie zasad ochrony informacji oraz danych osobowych w systemie informatycznym i nadzorująca przetwarzanie danych osobowych w systemie informatycznym.
10. 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.

11. Osoby przetwarzające dane osobowe - wszystkie osoby, w tym użytkownicy systemu informatycznego, mające z racji wykonywanych obowiązków dostęp do danych osobowych. Osobą przetwarzającą dane osobowe może być pracownik ADO, a także osoba wykonująca usługi na rzecz ADO na podstawie umowy zlecenia lub innej umowy cywilno-prawnej.
12. Poufność - zapewnienie dostępu do informacji wyłącznie osobom upoważnionym.
13. Integralność - spójność danych osobowych, zapewnienie, że dane nie zostaną zmienione, dodane lub usunięte w nieautoryzowany sposób.

§ 3
Zarządzanie przetwarzaniem i bezpieczeństwem danych osobowych

1. ADO powołuje IOD, który wykonuje zadania wskazane w art. 39 Rozporządzenia RODO do których należy:
    a. informowanie ADO oraz Osób przetwarzających 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 ADO 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 zakresie przetwarzania danych osobowych.
2. W ramach wypełniania obowiązków wskazanych w ust. 1 lit. a IOD:
    a. informuje o zmianach i nowych interpretacjach w dziedzinie danych osobowych w zakresie dotyczącym ADO;
    b. informuje o obowiązkach nałożonych przepisami oraz dokumentami wewnętrznymi na Osoby przetwarzające dane osobowe;
    c. udziela odpowiedzi i konsultacji w zakresie stosowania przepisów dotyczących przetwarzania danych osobowych;
3. W ramach wypełniania obowiązków wskazanych w ust. 1 lit. b IOD:
    a. cyklicznie informuje o zaobserwowanych zagrożeniach w dziedzinie ochrony danych osobowych;
    a. kieruje zapytania dotyczące przetwarzania danych osobowych;
    b. prowadzi audyty planowe według przyjętego harmonogramu;
    c. prowadzi audyty doraźne;
4. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
5. ADO zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
6. ADO wspiera IOD 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.
7. ADO zapewnia, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań, nie został odwoływany ani karany przez ADO za wypełnianie swoich zadań.

8. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
9. IOD może wykonywać inne zadania i obowiązki. ADO zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
10. ADO powierza IOD:
    a. monitoring i aktualizację prowadzonej dokumentacji przetwarzania danych osobowych;
    b. prowadzenie rejestrów czynności przetwarzania danych osobowych i kategorii danych osobowych (o ile jest konieczność prowadzenia danego rejestru)) 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.
11. IOD podlega bezpośrednio wyłącznie Rektorowi ADO.
12. IOD wskazuje po uzgodnieniu z ADO osobę, która będzie pełnić jego obowiązki na czas nieobecności spełniającą wymagania określone w art. 37 Rozporządzenia RODO.
13. 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. zarządzanie zasobem danych osobowych w ramach komórki organizacyjnej;
    b. powiadamianie IOD o zatrudnieniu osoby przy przetwarzaniu danych osobowych w celu wprowadzenia na listę osób upoważnionych oraz przesłania materiałów dotyczących Rozporządzenia RODO.
    c. występowanie z wnioskiem do ASI lub podmiotu odpowiedzialnego za określony system informatyczny o nadanie, zmianę lub cofnięcie uprawnień podległym pracownikom do określonego zasobu danych osobowych przetwarzanego w systemie informatycznym w tym aplikacjach;
    d. bieżącą kontrolę nad realizacją zasad przetwarzania danych osobowych przez podległych pracowników;
    e. zabezpieczenie obszaru przetwarzania danych osobowych w ramach stosowanych zabezpieczeń;
    f. zgłaszanie do IOD zamiaru podjęcia nowych czynności przetwarzania danych osobowych w tym w szczególności zamiaru powierzenia przetwarzania danych osobowych podmiotom zewnętrznym;
    g. zgłaszanie do IOD incydentów przetwarzania danych osobowych;
    h. konsultowanie z IOD podstawy przetwarzania danych osobowych, w tym zasadności dopuszczenia do przetwarzania zbiorów osób i podmiotów trzecich;
    i. realizację procesu udostępniania danych osobowych;
    j. realizację zapisów umów powierzenia przetwarzania danych osobowych;
    k. konsultowanie z ASI oraz IOD minimalnych wymagań dla systemów teleinformatycznych zgodnie z wytycznymi KRI oraz Rozporządzeniem RODO;
14. Dział Kadr jest odpowiedzialny za:
    a. informowanie IOD o wszelkich zmianach kadrowych na stanowiskach na których są przetwarzane dane osobowe;
    b. przygotowanie upoważnień do przetwarzania danych osobowych oraz przekazania informacji umożliwiających IOD wgląd, w proces ich wystawienia,
    c. przechowywanie nadanych upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu poufności w aktach osobowych pracowników.
15. ASI jest odpowiedzialny za zabezpieczenie i prawidłowe funkcjonowanie systemów informatycznych zgodnie z postanowieniami Instrukcji Zarządzania Systemami Informatycznymi stanowiącą Załącznik nr 1.

§ 4
Osoby przetwarzające informacje oraz dane osobowe

1. Dostęp do informacji ograniczony jest wyłącznie do osób, którym jest ona niezbędna do realizacji zadań ADO.
2. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby, którym powierzono przetwarzanie danych osobowych. Osoby, którym wydano pisemne upoważnienie wpisywane są do ewidencji osób upoważnionych, którą aktualizuje IOD (według wzoru ustalonego przez ADO). Upoważnienie może być wydane w formie pisemnej lub poprzez podjęcie innych działań przez ADO.
3. Dział Kadr lub Kierownik komórki organizacyjnej informuje IOD o osobie, która ma zostać dopuszczona do przetwarzania danych osobowych w celu kontroli wystawienia upoważnienia oraz udzielenia osobie upoważnionej niezbędnych informacjami w nadzorowanym przez IOD zakresie. Uprawnienia do systemów informatycznych są nadawane przez ASI na wniosek ADO lub wyznaczonego pracownika (osoby nadzorującej prace osoby upoważnionej).
4. Upoważnienie może być przyznane na czas określony lub do odwołania (wzór upoważnienia oraz odwołania upoważnienia znajduje się odpowiednio w Załączniku nr 4 oraz 4a). Osoba otrzymująca upoważnienie do przetwarzania danych osobowych jest zobowiązana podpisać Oświadczenie o zachowaniu poufności Przetwarzanych Danych Osobowych (wzór oświadczenia znajduje się w Załączniku nr 5). Proces powyższy realizowany jest według Procedury nadawania upoważnień znajdującej się w Załączniku nr 3. Dopuszcza się elektroniczne wnioskowanie o nadanie upoważnienia.
5. ADO odbiera oświadczenia osób przetwarzających dane osobowe o poufności oraz zapoznaniu się z zasadami przetwarzania danych osobowych, w tym konsekwencjach nieprzestrzegania tych zasad.
6. ADO zapewnia szkolenie osób upoważnionych zgodnie z zaproponowanym przez IOD i przyjętym przez ADO każdego roku, planem szkoleń.
7. IOD przeprowadza regularne szkolenia pracowników z zakresu RODO, zgodnie z planem szkoleń. Procedura przeprowadzania szkoleń znajduje się w załączniku nr 10.

§ 5
Obowiązki osób przetwarzających dane osobowe

1. W celu przestrzegania zasad ochrony danych osobowych przez osoby przetwarzające dane osobowe, szczegółowe obowiązki osób przetwarzających dane osobowe zostały określone w odrębnym regulaminie wskazanym w Załączniku nr 2. Osoby przetwarzające dane osobowe są zobowiązane do przestrzegania poufności w zakresie przestrzegania zasad ochrony danych w obowiązującej u ADO dokumentacji w tym procedur, instrukcji lub wytycznych w konkretnej sprawie.
2. Nieprzestrzeganie obowiązków dotyczących ochrony danych osobowych stanowi przedmiot analizy ADO w konsultacji z IOD. ADO podejmuje decyzję o konsekwencjach mających być wyciągniętych wobec osoby naruszającej Politykę ochrony danych osobowych lub inne uregulowania dotyczące przetwarzania danych osobowych.

§ 6
Umowy powierzenia danych osobowych

1. W przypadku powierzenia przetwarzania danych osobowych podmiotom trzecim, powierzenie następuje w drodze umowy powierzenia danych osobowych lub innego równorzędnego dokumentu dopuszczonego przez Rozporządzenie RODO.
2. ADO kieruje się przy wyborze podmiotu przetwarzającego dane osobowe zasadami wskazanymi w art. 28 Rozporządzenia RODO, w szczególności korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa o ochronie danych osobowych i chroniło prawa osób, których dane dotyczą.
3. Umowa powierzenia przetwarzania danych lub inny równorzędny dokument powinien zawierać elementy wskazane w art. 28 Rozporządzenia RODO, potwierdzający gwarancje spełnienia przez podmiot przetwarzający dane osobowe warunków, o których mowa ust. 2. ADO może wprowadzić wzór obowiązującej umowy powierzenia przetwarzania danych, przy czym może być on modyfikowany lub zmieniany w przypadku konieczności.
4. Powierzenie przetwarzania danych osobowych jest konsultowane z IOD.
5. ADO ewidencjonuje umowy powierzenia danych osobowych w sposób przyjęty w jednostce.

§ 7
Udostępnianie danych osobowych odbiorcom

1. Udostępnienie danych osobowych odbiorcom niebędącym podmiotami przetwarzającymi może nastąpić wyłącznie w przypadku istnienia przesłanki legalizującej udostępnienie danych osobowych.
2. Udostępnienie danych osobowych jest konsultowane z IOD.
3. Komórka organizacyjna (lub osoba zajmująca samodzielne stanowisko) udostępniająca dane, odnotowuje ten fakt w przyjęty w jednostce sposób (np. w umowie, rejestrze elektronicznym, wiadomości e-mail).

§ 8
Naruszenia i incydenty

1. Osoby przetwarzające dane osobowe są zobowiązane powiadomić IOD 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) nieupoważnioną modyfikację danych osobowych, kopiowanie lub niszczenie dokumentów zawierających dane osobowe,
   d) inne naruszenie postanowień Rozporządzenia RODO.
3. IOD informuje o zdarzeniu ADO, który informuje w przypadkach wskazanych w Rozporządzeniu RODO Urząd Ochrony Danych Osobowych i osoby, których przetwarzanie danych osobowych zostało naruszone.
4. Szczegółowy tryb postępowania w takim przypadku zawarty jest w Załączniku nr 8.
5. W jednostce prowadzona jest lista naruszeń i incydentów. Na liście umieszcza się także zdarzenia nie mające bezpośredniego negatywnego wpływu na system, ani przetwarzane dane osobowe, ale które mogą potencjalnie zagrażać zgromadzonym danym nawet jeśli nie są danymi osobowymi. Zgłoszeń dokonują osoby odpowiedzialne za zabezpieczenie systemu teleinformatycznego.

§ 9
Zasady zbierania i przetwarzania danych osobowych

1. Dane osobowe przetwarzane w ADO mogą być pozyskiwane:
   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. W celu realizacji zasad wskazanych w § 1 ust. 5 ustala się następujące postepowanie:
   a) w celu realizacji zasady zgodność z prawem, rzetelność i przejrzystość - przeprowadza się analizę podstawy prawnej przetwarzania danych osobowych, w tym zbierania zgody oraz ustala treść obowiązku informacyjnego zgodnie z postanowieniami art. 12 RODO o przetwarzaniu danych osobowych. Powyższe jest konsultowane z IOD.
   b) w celu realizacji zasady ograniczenia celu przetwarzania - ADO przy podejmowaniu decyzji o przetwarzaniu danych uwzględnia przesłankę ograniczenia celu oraz konsultuje ten proces z IOD.
   c) w celu realizacji zasady minimalizacja danych, osoba odpowiedzialna za dany zbiór określa minimalny zakres danych niezbędny do realizacji celu, uwzględniając przepisy prawne w tym zakresie oraz w razie potrzeby konsultuje go z IOD.
   d) w celu realizacji zasady prawidłowości przetwarzanych danych, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Rozporządzenia RODO, albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia;
   e) w celu realizacji zasady ograniczenia przechowywania danych osobowych, dokonuje się okresowego przeglądu zgromadzonych zasobów zawierających dane osobowe zgodnie z odrębnym dokumentem (instrukcją kancelaryjną) przyjętą w jednostce;
   f) w celu realizacji zasady integralność i poufności danych osobowych stosuje się zabezpieczenia fizyczne, informatyczne oraz organizacyjne opisane w niniejszym dokumencie. W przypadku konieczności udostępnienia dokumentów i danych osobowych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, dokonuje się zmiany tych danych osobowych w sposób zapewniający anonimowość osób, których dane te dotyczą.
   3. W celu realizacji konsultacji z IOD wprowadza się procedurę wskazaną w Załączniku nr 9.

§ 10
Obowiązek informacyjny

1. Kierownicy komórek organizacyjnych 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 IOD prowadzić wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania danych oraz przysługujących im praw. Obowiązek informacyjny prowadzony jest zgodnie z ustaloną z IOD klauzulą informacyjna ich dotyczącą. Klauzula informacyjna zawiera informacje wskazane w art. 12 oraz odpowiednio 13 i 14 Rozporządzenia RODO.
2. Szczegółowy tryb realizacji obowiązku informacyjnego jest zawarty w Załączniku nr 6.

§ 11
Prawa osób, których dotyczą dane osobowe

1. Osobom, których dane przetwarza się w zbiorze danych osobowych ADO, 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 osobowych,
    f) prawo do sprzeciwu wobec przetwarzania danych osobowych.
2. IOD opiniuje zasadność żądania i wraz z komórką organizacyjną w której przetwarzane są dane osobowe udziela odpowiedzi.
3. Szczegółowy tryb realizacji praw osób, których dane są przetwarzane jest zawarty w Załączniku nr 7.

§ 12
Rejestr czynności przetwarzania oraz rejestr kategorii czynności

1. ADO prowadzi rejestr czynności przetwarzania danych osobowych i o ile zachodzi taka konieczność (jednostce powierzono przetwarzanie danych) rejestr kategorii przetwarzania danych.
2. Rejestry są aktualizowane przez IOD na podstawie własnych ustaleń oraz informacji uzyskanych od Osób przetwarzających dane osobowe. Czynności przetwarzania mogą być grupowane w ramach zbiorów danych osobowych wedle kryterium komórki przetwarzającej dane osobowe lub innego przyjętego w ADO kryterium takiego jak kategoria osób lub cel przetwarzania danych.
3. Rejestry zawierają co najmniej elementy, o których mowa w art. 30 ust. 1 oraz 2 RODO.
4. Kierownicy komórek organizacyjnych lub osoby zatrudnione na samodzielnych stanowiskach, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia IOD informacji na temat:
    a) planowanego założenia nowych czynności przetwarzania i zbiorów danych osobowych,
    b) wnoszonych zmian do istniejących czynności przetwarzania i zbiorów danych osobowych,
    c) przypadków powierzenia ADO danych osobowych do przetwarzania przez inny podmiot.

§ 13
Ocena ryzyka i DPiA

1. W celu prawidłowego wyznaczenia poziomu ochrony ADO dokonuje okresowej analizy ryzyka (zgodnie z art. 35 RODO), 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 rozporządzenia RODO oraz chronić prawa osób, których dane dotyczą.
2. Oceny ryzyka dokonuje się nie rzadziej niż raz na 2 lata. W przypadku istotnych zmian przetwarzania danych osobowych przez ADO, analizę ryzyka należy wykonać po ich wprowadzeniu. Ocena ryzyka powinna być wykonywana przez podmiot posiadający wiedzę i doświadczenie w tej

materii. ADO dokonuje wyboru podmiotu, który wykona analizę ryzyka.

3. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować´ wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPiA). Dokonując oceny skutków dla ochrony danych, ADO konsultuje się z IOD. W przypadku braku przesłanek do wykonania DPiA, których oceny istnienia dokonuje IOD, zostaje sporządzana analiza prawna braku takich przesłanek.

§ 14
Zabezpieczenia fizyczne, informatyczne i organizacyjne

1. Zabezpieczenia fizyczne
    a. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, podlega kontroli.
    b. 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.
    c. Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie osobom upoważnionym.
    d. ADO, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
    e. Miejsca przetwarzania danych osobowych wraz z zabezpieczeniami odnotowuje się w odrębnym dokumencie - Lista (ewidencja) miejsc przetwarzania danych osobowych wraz z zabezpieczeniami prowadzona na podstawie Polityki ochrony danych osobowych wskazana w Załączniku nr 13 do niniejszej Polityki ochrony danych osobowych.
    f. Dozwolone jest stosowanie monitoringu, którego szczegóły ustalane są w odrębnym dokumencie po konsultacji z IOD. Wydawanie nagrań z monitoringu jest rejestrowane z uwzględnieniem komu i na jakiej podstawie udostępniono nagranie wraz z datą wydania nagrania. Wzór rejestru znajduje się w Załączniku nr 13a.

2. Zabezpieczenia informatyczne

Zabezpieczenia informatyczne oraz sposób postępowania z środkami informatycznymi został opisany w Załączniku nr 1.

3. Zabezpieczenia organizacyjne

Zabezpieczenia organizacyjne mające na celu stosowanie przepisów RODO zostały opisane w niniejszej dokumentacji i obejmują sposoby oraz procedury postepowania z danymi osobowymi w ADO, szkolenie Osób przetwarzających dane osobowe, zgodnie z planem szkoleń, dokonywanie sprawdzeń zgodnie z planem sprawdzeń oraz korzystanie z procedur mających na celu rzeczywiste uwzględnianie ochrony danych osobowych w funkcjonowaniu jednostki.

§ 15
Kontrola (audyty) przestrzegania przepisów z zakresu bezpieczeństwa danych osobowych

1. ADO może zarządzić przeprowadzenie przez IOD kontroli wewnętrznej dotyczącej przestrzegania zasad i przepisów RODO podczas wykonywania czynności służbowych.

2. Zlecona kontrola ma na celu sprawdzenie czy przetwarzanie danych osobowych odbywa się zgodnie z obowiązującymi przepisami prawa oraz zasadami i dokumentami wdrożonymi w jednostce.
3. Kontrole (audyty) mogą mieć charakter planowy lub doraźny w zależności od okoliczności oraz decyzji ADO.
4. Zasady przeprowadzenia kontroli są opisane w załączniku nr 11.

§ 16
Praca zdalna

1. W uzasadnionych przypadkach ADO może wprowadzić pracę zdalną, jeśli niemożliwe jest wykonywanie obowiązków służbowych przez pracownika w miejscu jej stałego wykonywania.
2. W przypadku wykonywania pracy zdalnej pracownik przestrzega przepisów związanych z bezpieczeństwem danych osobowych jakie są zapisane w niniejszej Polityce ochrony danych osobowych.
3. Szczegóły odnośnie przetwarzania danych osobowych podczas pracy zdalnej są zawarte w załączniku nr 12, który zawiera wytyczne postępowania z danymi osobowymi na czas pracy zdalnej.
4. W przypadku udzielania zdalnego dostępu do baz danych i oprogramowania służącego do przetwarzania danych osobowych ADO stosuje się środki zapewniające poufność i integralność danych.

§ 17
Postanowienia końcowe

1. Integralną częścią niniejszej Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie są Załączniki.
2. W celu wykonania niniejszej Polityki ochrony danych osobowych wydawane mogą być dodatkowe dokumenty takie jak procedury, instrukcje czy zarządzenia. W tym celu mogą być prowadzone także listy i wykazy. Wykaz powyższych dokumentów znajduje się w Załączniku nr 13, który może być uzupełniany przez ADO na wniosek lub po konsultacji z IOD bez konieczności zmiany niniejszej Polityki ochrony danych osobowych, o dokumenty, których prowadzenie okaże się konieczne na gruncie przepisów.
3. W celu wykonania niniejszej Polityki ochrony danych osobowych prowadzone będą w osobnych dokumentach rejestry czynności przetwarzania danych osobowych w jednostce.

Lista załączników:

1. Instrukcja Zarządzania Systemami Informatycznymi – Załącznik nr 1;
2. Regulamin przetwarzania danych osobowych przez osoby upoważnione do przetwarzania danych osobowych w kartotekach i systemach informatycznych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie – Załącznik nr 2;
3. Procedura nadawania upoważnień do przetwarzania danych osobowych – Załącznik nr 3
4. Wzór upoważnienia i odwołania upoważnienia do przetwarzania danych osobowych – Załącznik nr 4;
5. Oświadczenie o zachowaniu poufności Przetwarzanych Danych Osobowych – Załącznik nr 5;
6. Procedura udzielania informacji podawanej w przypadku pozyskiwania danych – Załącznik nr 6;
7. Procedura realizowania uprawnień osób, których dane są przetwarzane – Załącznik nr 7;
8. Procedura reagowania i oceny naruszeń bezpieczeństwa danych osobowych – Załącznik nr 8;

9. Procedura opiniowania zagadnień prawnych związanych z danymi osobowymi – Załącznik nr 9;
10. Procedura szkoleń dla Osób przetwarzających dane osobowe– załącznik nr 10;
11. Procedura kontroli przestrzegania przepisów RODO z zakresu bezpieczeństwa danych osobowych – załącznik nr 11;
12. Wytyczne postępowania z danymi osobowymi na czas pracy zdalnej – załącznik nr 12;
13. Spis rejestrów ewidencji oraz list (ewidencji) prowadzonych na podstawie Polityki ochrony danych osobowych – Załącznik nr 13;
14. Wzór rejestru udostępnienia nagrań z monitoringu – Załącznik nr 13a;

Załącznik nr 1 *do Polityki ochrony danych osobowych*

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie

SPIS TREŚCI

§1
Cel i zakres stosowania instrukcji

1. Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania informacji oraz danych osobowych, przez Administratora Danych Osobowych (ADO) – w celu zabezpieczenia informacji oraz danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych.
3. Za realizację postanowień niniejszej instrukcji, o ile nie jest wskazane inaczej odpowiedzialny jest od strony technicznej Administrator Systemu Informatycznego (ASI) powołany w jednostce. ASI posługuje się w wykonywaniu swoich zadań administratorami oprogramowania i administratorami sprzętu wykorzystywanego u ADO. ASI koordynuje ich działania.
4. W przypadku wskazania w niniejszym dokumencie na użytkownika lub pracownika rozumie się przez to osobę przetwarzającą informacje oraz dane osobowe w rozumieniu definicji zamieszczonej w Polityce ochrony informacji oraz danych osobowych.

§2
Postanowienia ogólne

1. Instrukcja ma na celu realizację przepisów Rozporządzenia 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 (dalej „RODO") w szczególności zasad wyrażonych w art. 5 RODO.
2. Instrukcja ma na celu realizację przepisów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (dalej KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
3. Za priorytet uznano zagwarantowanie zgromadzonym informacjom oraz danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.

§3
Obowiązki w zakresie ochrony informacji oraz danych osobowych

1. Do obowiązków osób zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy:
   a) Podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.
   b) Przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych.
2. Użytkownicy podlegają bieżącym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§4
Obowiązki użytkowników

Do obowiązków użytkowników należy w szczególności:
1) Przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych.
2) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3) Udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania.
4) Uniemożliwienie dostępu do danych osobowych w systemie lub ich podglądu przez osoby nieupoważnione.
5) Informowanie Inspektora Ochrony Danych (IOD) oraz ASI o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.
6) Wykonywania bez zbędnej zwłoki poleceń IOD lub ASI w zakresie ochrony informacji oraz danych osobowych, jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§5
Poziom bezpieczeństwa

1. ADO dąży do stałej zgodności poziomu bezpieczeństwa ustanawianego przepisami KRI oraz RODO.
2. Uwzględniając istotność informacji i kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się środki bezpieczeństwa spełniające co najmniej kryteria wskazane w ust. 4.
3. W przypadku pojawienia się awarii systemu informatycznego mającego wpływ na bezpieczny przepływ informacji oraz danych osobowych wprowadza się procedurę w postaci planu ciągłości działania na wypadek awarii systemu informatycznego stanowiącą załącznik nr 1 do niniejszej Instrukcji.
4. Środki bezpieczeństwa obejmują:
   1) Kontrolę dostępu do pomieszczeń w których zgromadzone są zasoby informatyczne w tym serwerownię. Szczegółowy opis zabezpieczeń fizycznych znajduje się w Polityce ochrony informacji oraz danych osobowych.
   2) W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
   3) Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
      a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator.
      b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
   4) System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
      a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
      b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
   5) Identyfikator użytkownika oraz hasło użytkownika nadawane są zgodnie z zasadami opisanymi w niniejszym dokumencie.

6) Dane osobowe oraz informacje przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
7) W przypadku wykorzystania komputerów przenośnych stosuje się środki ochrony kryptograficznej za których zastosowanie/instalację odpowiada ASI. Użytkownik użytkujący komputer przenośny zawierający dane osobowe zobowiązany jest do zachowania szczególnej ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych.
8) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, które są przeznaczone do likwidacji, przekazania podmiotowi zewnętrznemu, naprawy, pozbawiane są danych osobowych zgodnie z procedurami opisanymi w § 13 oraz 14 niniejszej Instrukcji Zarządzania Systemami Informatycznymi.
9) ASI monitoruje wdrożone zabezpieczenia systemu informatycznego.
10) W celu zapewnienia bezpiecznego przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi ASI sprawuje regularną kontrolę nad tymi procesami. Aktualny stan przepływu tych danych jest zawarty w załączniku nr 2 do niniejszej Instrukcji.
11) Urządzenia i nośniki zawierające dane osobowe nie są przekazywane poza obszar przetwarzania danych poza sytuacjami przekazania ich ASI. W przypadku zajścia konieczności przekazania ich podmiotowi zewnętrznemu, zabezpiecza się w sposób zapewniający poufność i integralność tych danych zgodnie z § 14 niniejszego dokumentu.
12) System informatyczny służący do przetwarzania informacji i danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
13) W przypadku zastosowania logicznych zabezpieczeń obejmują one:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym ADO a siecią publiczną. Kontrolę przepływu informacji realizuje się poprzez zapisywanie logów systemowych możliwych do okresowego wygenerowania przez ASI.
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego ADO. Kontrolę tych działań zapewnia się poprzez stosowaną zaporę firewall i jej ustawienia stosownie do poziomu zagrożeń przez ASI w uzgodnieniu z ADO.

14) Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki kryptograficznej ochrony, poprzez stosowanie protokołu szyfrującego SSL dla poczty wychodzącej.
15) W przypadku przekazywania nośników zawierających dane osobowe podmiotom w przypadkach, gdy są ich odbiorcami, nośniki takie powinny być szyfrowane, a hasło powinno być przekazywane odrębnym kanałem komunikacji. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji IOD bądź ADO.
16) Użytkownicy nie mogą wynosić na zewnątrz firmy wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody ADO.
17) Dane osobowe wynoszone poza ADO muszą być chronione, np.: zaszyfrowane.

§6
Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe zostaje zapewniona poprzez przestrzeganie następujących zasad:
1) Użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie. Dodatkowo stosuje się różny poziom uprawnień do systemu (z podziałem na konto administratora i użytkownika).
2) Użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.
3) Użytkownikom nie wolno we własnym zakresie instalować nowego lub aktualizować już zainstalowanego oprogramowania. Dodatkowo stosuje się środki techniczne uniemożliwiające instalowanie nowego oprogramowania.
4) Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
5) Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.
6) Użytkownikom nie wolno bez uzyskania zgody ASI lub osób przez niego upoważnionych przenosić aplikacji oraz zasobów zlokalizowanych na zasobach sieciowych na dyski lokalne oraz przenośne nośniki danych.
7) Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego jest zabronione bez zgody ASI lub IOD.

§7
Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

Nadawanie i rejestrowanie uprawnień.
1) Z uwagi na różnorodność stosowanych systemów informatycznych, zasobów sprzętowych oraz procesów związanych z przetwarzaniem informacji i danych osobowych do nadawania i rejestrowanie uprawnień ADO stosuje różne procedury postepowania, przy czym zachowuje w tym zakresie generalne zasady opisane poniżej.
2) Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do przetwarzania danych osobowych w tym systemie, zobowiązani są zapoznać z zasadami przetwarzania i ochrony danych osobowych.
3) Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe wiąże się z uprzednim nadaniem mu upoważnienia do przetwarzania danych osobowych i złożeniem przez użytkownika oświadczenia o zachowaniu w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczania. Wzór upoważnienia i oświadczenia stanowi załącznik do Polityki ochrony informacji i danych osobowych.
4) Wniosek o zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe składa do ASI, ADO lub osoba do tego upoważniona przez ADO. Wniosek ten składa się wraz z wnioskiem o przygotowanie upoważnienia i przeprowadzenia szkolenia stanowiskowego do IOD. Wniosek o zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień może zostać złożony w przyjęty u ADO sposób w tym poprzez zgłoszenie e-mail oraz w systemie informatycznym z zachowaniem pewności uprawnienia wnioskodawcy do jego złożenia.
5) Identyfikator oraz dostęp do zasobów sprzętowych i oprogramowania jest rejestrowany w systemie informatycznym przez ASI. System informatyczny umożliwia wygenerowanie powyższych danych w każdym

czasie. Użytkownik z dostępem do danych osobowych jest rejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych przez IOD po nadaniu upoważnienia zgodnie z przyjętą procedurą stanowiącą załącznik do Polityki ochrony informacji i danych osobowych.
6) Identyfikator i zakres dostępu przydziela ASI, zgodnie z poleceniem bezpośredniego przełożonego (kierownika komórki organizacyjnej).
7) ASI lub podlegający mu administrator oprogramowania lub sprzętu przekazuje użytkownikom tymczasowe hasła dostępowe w sposób bezpieczny. W tym celu użytkownicy powinni unikać pośrednictwa osób trzecich lub korzystania do tego celu z niechronionych wiadomości poczty elektronicznej. Dodatkowo ustawienia systemu informatycznego wymuszają zmianę hasła po pierwszym logowaniu do użytkownika, o ile system to umożliwia, w przeciwnym razie ASI instruuje użytkownika o konieczności zmiany hasła.
8) Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach informatycznych należy stosować odpowiednio również w przypadku zmiany uprawnień.
9) Prawa dostępu przyznane użytkownikom, którzy nie są pracownikami etatowymi powinny mieć charakter czasowy i mogą być przyznawane na okres odpowiadający wykonywanemu zadaniu.
10) Dostęp do systemu informatycznego a także do poszczególnych aplikacji i baz danych przetwarzających dane osobowe powinien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.
11) Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez ASI.
12) Rejestracja użytkownika polega na nadaniu identyfikatora wraz z hasłem tymczasowym. Podczas pierwszego logowania, użytkownik dokonuje zmiany hasła na nowe, znane tylko jemu.
13) Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
14) W przypadku osób zatrudnionych na podstawie umowy o prace wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
15) Wykaz użytkowników posiadających upoważnienia do przetwarzania danych osobowych jest zawarty w załączniku nr 1 do niniejszej Instrukcji.

Odebranie uprawnień użytkownikowi.
1) Odebranie uprawnień użytkownika do systemu informatycznego lub jego komponentów (w tym oprogramowania) dokonuje ASI na wniosek kierownika komórki organizacyjnej na którego wniosek je nadano uprawnienia lub ADO.
2) Odebranie uprawnień polega na trwałym lub czasowym zablokowaniu kont użytkownika umożliwiającego dostęp do zasobów sprzętowych i informatycznych (oprogramowania) lub jego komponentów (w tym oprogramowania)).
3) ASI lub podlegający mu administrator oprogramowania lub sprzętu przeprowadzają raz na 6 miesięcy weryfikacje prawidłowości nadanych uprawnień.

§8
Metody i środki uwierzytelnienia

Identyfikator (login).
1) Identyfikator nadaje ASI.
2) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być

przydzielony innej osobie.
3) Identyfikator użytkownika jest unikatowy dla tego użytkownika, przy czym identyfikator użytkownika może służyć mu do logowania do różnych systemów/oprogramowania.

Hasło użytkownika.
1) Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
2) Użytkownicy powinni stosować hasła, które:
a) są łatwe do zapamiętania, a trudne do odgadnięcia.
b) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.).
c) zawierają przynajmniej jedną dużą literę, jedną małą literę, jedną cyfrę lub znak specjalny.
3) Hasła powinny być zmieniane okresowo przy czym odstępy te powinny być ustalane w oparciu o specyfikę użytkowania oprogramowania, dobre praktyki i ogólnie przyjęte standardy; ; ASI lub IOD, w uzasadnionych sytuacjach mogą polecić dokonanie zmiany hasła przez użytkownika.
4) Należy unikać ponownego lub cyklicznego używania starych haseł, o ile system informatyczny na to zezwala.
5) Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
6) Pracownicy są odpowiedzialni za zachowanie w poufności swoich haseł.
7) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).
8) Użytkownik wprowadza swoje hasło w sposób uniemożliwiający innym osobom jego poznanie.
9) W sytuacji, gdy zachodzi podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik natychmiast dokonuje zmiany hasła.
10) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
11) ASI jest odpowiedzialny za usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które jest odpowiedzialny.

Hasło administratora systemu.
Hasła administratora systemu znane jest ASI i zabezpieczone jest u ADO lub możliwe do zresetowania przez kierownictwo ADO u dostawców oprogramowania.

§9
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników

Tryb pracy na poszczególnych stacjach roboczych.
1) Rozpoczęcie pracy na stacji roboczej następuje po włączeniu komputera, a następnie wprowadzeniu indywidualnego identyfikatora i hasła użytkownika.
2) Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
3) Monitory komputerów wyposażone są w wygaszacze ekranu. Zastosowana jest blokada komputerów –

wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
4) W przypadku opuszczenia stanowiska pracy, użytkownik ma obowiązek wylogowania się z systemu lub w inny sposób zablokować stację roboczą. Stanowisko pracy nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim użytkownika.
5) Obowiązuje zakaz robienia kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez ASI lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
6) Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne, po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii, dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
7) Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami ADO, a komputerami przenośnymi użytkowników z wykorzystaniem kryptograficznych środków ochrony danych.
8) Przesyłanie danych osobowych pocztą elektroniczną powinno odbywać się w postaci zaszyfrowanej.
9) Obowiązuje zakaz wynoszenia poza obszar przetwarzania danych na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
10) Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak by zapobiec ich utracie.
11) Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary zasobów sieciowych, a następnie prawidłowym wylogowaniu się przez użytkownika i wyłączeniu komputera.
12) Przed opuszczeniem pokoju należy:
a) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe.
b) schować do zamykanych na klucz szaf wszelkie dokumenty zawierające dane osobowe.
c) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu.
d) zamknąć okna.
13) Opuszczając pokój należy zamknąć za sobą drzwi na klucz.

Tryb pracy na komputerach przenośnych.
W przypadku korzystania z komputerów przenośnych należy stosować się do poniższych zasad:

1) O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.
2) Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu.
3) Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
4) Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.
5) Użytkownicy zmieniają hasła w komputerach przenośnych okresowo przy czym odstępy te powinny być ustalane w oparciu o specyfikę użytkowania oprogramowania, dobre praktyki i ogólnie przyjęte standardy.
6) Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu.
7) Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
8) Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na zasobach sieciowych ADO, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.
9) Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach

przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem ASI, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to administratorowi systemu.
10) Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

§10
Procedury tworzenia kopii zapasowych

I. Wykonywanie kopii zapasowych.

1) Z uwagi na różnorodność stosowanych systemów informatycznych, zasobów sprzętowych oraz procesów związanych z przetwarzaniem informacji i danych osobowych do wykonywania kopii zapasowych ADO stosuje różne procedury postepowania, przy czym zachowuje w tym zakresie generalne zasady opisane poniżej.
2) W systemie informatycznym zapewnia się wykonanie kopii zapasowych zapewniających ciągłość pracy ADO.
3) Kopie zapasowe są wykonywane automatycznie poprzez odpowiednie ustawienia oprogramowania do jego tworzenia. Automatyczne wykonywanie kopii zapasowych odbywa się nie rzadziej niż raz dziennie.
4) Dostęp do kopii bezpieczeństwa posiada wyłącznie ADO oraz ASI, który wydaje kopię zapasową na każde żądanie ADO. Każde wydanie i przyjęcie kopii jest odnotowywane przynajmniej w formie wiadomości elektronicznej.
5) Za tryb i częstotliwość tworzenia kopii zapasowych odpowiada ASI.

II. Testowanie kopii zapasowych.

W celu zapewnienia poprawności wykonywania kopii bezpieczeństwa należy regularnie poddawać testowi wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych. Wyniki testów odnotowywane są w raporcie miesięcznym dostarczanym przez ASI. Testy kopii zapasowych wykonuje się nie rzadziej niż raz na 6 miesięcy.

III. Przechowywanie kopii zapasowych.

Kopie zapasowe przechowuje się w odrębnym pomieszczeniu tak, aby zminimalizować ryzyko ich losowego zniszczenia. Kopii zapasowych nie wykonuje się na nośnikach typu CD, CD-R, CD-R, DVD-R, DVD-RW, taśmy magnetyczne, chyba że w sytuacjach wyjątkowych dopuszczonych przez ASI. Nośniki z takimi danymi są niezwłocznie niszczone po ustaniu ich użyteczności.

IV. Zaangażowanie podmiotu trzecich w wykonywanie kopii zapasowych

1) W przypadku zaangażowania podmiotu trzeciego (dostawcy zewnętrznego usług tworzenia kopii zapasowych, w tym dostawcy rozwiązań chmurowych) innego niż ASI, umowa lub inny dokument regulujący zasady świadczenia usługi będzie określał zasady wykonywania kopii zapasowych, testowanie kopii zapasowych oraz ich przechowywania. Wybór dostawcy i przyjęte zasady wykonywania kopii zapasowych musza zapewniać poziom bezpieczeństwa odpowiadający poziomowi zapewnianemu w tego typu usługach przez wiodących dostawców i zapewniający odpowiedni poziom bezpieczeństwa.

V. Procedura poprawiania i usuwania danych z kopii zapasowych

1) W przypadku otrzymania wniosku do zrealizowania prawa do sprostowania danych lub usunięcia danych na podstawie odpowiednio art. 16 i 17 RODO, postępuje się zgodnie z Procedurą reagowania i oceny naruszeń bezpieczeństwa danych osobowych (Załącznik nr 8 do Polityki Bezpieczeństwa) z uwzględnieniem poniższych zapisów.

2) IOD wraz z kierownikiem działu merytorycznego ustalają w jakich zbiorach znajdują się dane osobowe wnioskodawcy. Następnie IOD wraz z kierownikiem działu merytorycznego oceniają wniosek pod kątem obowiązujących przepisów prawnych i możliwości jego uwzględnienia.
3) Uwzględniając wniosek, kierownik działu merytorycznego lub na jego zlecenie osoba obsługująca system informatyczny, usuwa dane ze zbioru danych używanych na bieżąco. Od tego dnia nadpisywane są automatycznie kopie zapasowe nie posiadające już danych, które uległy wykasowaniu, co skutkować będzie usunięciem danych z kopii zapasowych w terminie nadpisania najstarszej z nich. W przypadkach dysponowania odpowiednimi możliwościami technicznymi i organizacyjnymi wykasowanie danych z kopii zapasowych może zostać przyspieszone i zlecone przez kierownictwo ADO. W takim przypadku za wykasowanie danych odpowiada osoba lub podmiot odpowiedzialny za wykonanie kopii zapasowej.
4) W czasie nadpisywania danych zakazane jest odtwarzanie kopii zapasowych w celu wykorzystania niezmienionych danych podlegających usunięciu. W przypadku konieczności odtworzenia kopii zawierającej dane podlegające sprostowaniu lub usunięciu w innym celu, niezwłocznie po przywróceniu danych z kopii zapasowej, usuwa się dane objęte usunięciu.

§11
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych przez ASI.
2) Oprogramowanie, o którym mowa w pkt 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
3) Do obowiązków ASI należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
4) Użytkownik niezwłocznie powiadamia ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem. Po takim zgłoszeniu następuje odrębne skanowanie systemu przez ASI.
5) Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych, sieć wewnętrzna jest chroniona centralnym urządzeniem sprzętowym z wbudowanym Firewall.

§11[1]
Zasady zabezpieczenia sieci teleinformatycznej przed nieautoryzowanym dostępem

1) ASI odpowiedzialny jest za zabezpieczenie sieci teleinformatycznej przed nieautoryzowanym dostępem z uwzględnieniem poniższych zasad:
   a. ochronę sieci kablowej przed nieautoryzowanym dostępem;
   b. odłączanie nieużywanych gniazd;
   c. zablokowanie nieużywanych portów na przełączniku;
   d. blokowanie portów na podstawie Mac adresu urządzenia;

e. stosowanie sprawnego, z aktualnym oprogramowaniem firewall'a
f. udostępniania sieci z zewnątrz tylko za pośrednictwem VPN w każdym uzasadnionym przypadku;
g. Ochrona antywirusowa na komputerach;
h. Stosowania sprawdzonych polityk bezpieczeństwa w zakresie dostępu do zasobów sieciowych dla Użytkowników;
i. Zabezpieczenie dostępu Wi-Fi przez odpowiedni protokół zabezpieczenia sieci i szyfrowanie. W przypadku użytkowników domowych zalecane jest stosowanie protokołu WPA2 Personal z szyfrowaniem AES oraz WPA3. Nie są zalecane protokoły WPA z szyfrowaniem TKIP i WPA-PSK;
j. regularną zmianę domyślnego hasła administratora, zalecana jest również zmiana loginu.
k. usuwanie naklejki z hasłem z routera;
l. wyłączenie funkcji WPS – czyli Wi-Fi Protected Setup;
m. aktualizowanie oprogramowania routera;
n. filtrowanie adresów MAC (Media Access Control);
o. zainstalowanie oprogramowania antywirusowego na komputerach podłączonych do sieci WiFi, co pomoże zabezpieczyć przed kradzieżą hasła WiFi;
p. zmniejszenie zasięgu Wi-Fi – jeśli w ustawieniach routera możliwe jest ograniczenie zasięgu sieci, tak, żeby nie mogli z niej korzystać osoby postronne;
q. upewnienie się że sieć nie zawiera nieautoryzowanych punktów dostępowych (ang. rogue access point);
r. zablokowanie zdalnego dostępu do routera.

§11[2]
Zabezpieczenie stron internetowych administrowanych przez ADO

Podmiot, któremu powierzono stworzenie lub aktualizację strony internetowej zobowiązywany jest do monitorowania i testowania serwisu internetowego pod względem występowania podatności na naruszenie bezpieczeństwa. Administrator wprowadza do umów z podmiotami, którym powierzono aktualizację strony internetowej zapisy o odpowiedzialności za monitorowanie i testowanie serwisu internetowego pod względem występowania podatności wystarczające do jej prawidłowego i bezpiecznego funkcjonowania. Odpowiedzialnym za monitoring i testowanie serwisu jest podmiot, któremu powierzono aktualizację strony internetowej, za umieszczenie odpowiednich zapisów w umowie odpowiedzialny jest ADO.

§11[3]
Zawieranie umów serwisowych IT

Przy zawieraniu umów z podmiotami zewnętrznymi na świadczenie usług serwisowych lub dotyczących obsługi systemów informatycznych należy:

- dokonać oceny konieczności zawarcia umowy powierzenia danych osobowych;

- w przypadku powierzenia przetwarzania danych osobowych przeprowadzić ocenę wybranego podmiotu pod kątem stosowanych zabezpieczeń;

- wprowadzać bezwzględnie zapisy dotyczące poufności;

- w miarę możliwości i potrzeby wprowadzić do zapisów umów kary umowne lub inne zabezpieczenia prawne umożliwiające dochodzenie roszczeń z tytułu naruszenia poufności lub bezpieczeństwa;

§11[4]
Procedura przydzielania dostępu zdalnego

1. Niniejszy paragraf ustanawia zasady nadawania dostępu do infrastruktury informatycznej za pomocą zdalnego połączenia w tym poprzez pulpit zdalny. Połączenie zdalne (pulpit zdalny) oznacza program, platformę lub protokół sieciowy, który pozwala na zdalne połączenie i kontrolę komputera z innego komputera.
2. Dostęp zdalny odbywa się przez zabezpieczone, szyfrowane połączenie typu VPN ustanawiane za osobę odpowiedzialną za dany zasób informatyczny lub ASI.3. Zdalny dostęp do systemów bezpieczeństwa lub modułów zarządzania kontrolą dostępu do systemów może być realizowany wyłącznie za pośrednictwem tzw. serwera przesiadkowego, odpowiednio skonfigurowanego i zarządzanego.
4. Należy korzystać wyłącznie z takich mechanizmów uzyskiwania zdalnego dostępu, jakie zostały autoryzowane przez ASI. Wykorzystywanie innych sposobów zdalnego dostępu jest zabronione.
5. Regularnie monitoruje się przyznane uprawnienia, usuwając niepotrzebne konta dostępowe nie rzadziej niż raz na pół roku.

I. Zarządzanie zdalnym dostępem dla pracowników.

1. Zdalny dostęp przeznaczony dla użytkowników będących pracownikami AT lub wykonującymi pracę osobiście dla AT na podstawie innej umowy niż umowa o pracę.
2. Zdalny dostęp nadawany jest poprzez utworzenie stałego konta dostępowego dla określonego zidentyfikowanego użytkownika.
3. Zdalny dostęp jest nadawany wskazanym w pkt. 1 osobom, które posiadają przypisany do siebie służbowy komputer przenośny.
4. Zdalny dostęp może zostać nadany wskazanym w pkt. 1 osobom, które nie dysponują służbowym komputerem i łączą się z infrastruktura informatyczną za pomocą własnego urządzenia przenośnego za zgodą Kanclerz AT.
5. Wniosek o udzielenie zdalnego dostępu jest składany elektronicznie do osoby odpowiedzialnej za dany zasób informatyczny przez osobę koordynującą pracą użytkownika lub przez Kanclerz AT.
6. Rejestr pracowników posiadających zdalny dostęp do zasobów AT prowadzą osoby odpowiedzialne za dany zasób informatyczny (rejestr może być prowadzony elektronicznie).
7. Uniemożliwia się nadawanie zdalnego dostępu (w tym poprzez wbudowane w oprogramowanie zdalne pulpity, oprogramowanie typu teamviewer) przez innych niż osoby odpowiedzialne za dany zasób informatyczny. Wyłącza się losowe generowanie haseł i inne tego typu mechanizmy umożliwiającym nadanie dostępu użytkownikom systemu z pominięciem osób odpowiedzialnych za dany zasób informatyczny.

II. Zarządzanie zdalnym dostępem dla podmiotów świadczących wsparcie informatyczne osobiście (osoby odpowiedzialne za dany zasób informatyczny).

1. Zdalny dostęp do zasobów teleinformatycznych dla podmiotów świadczących wsparcie informatyczne osobiście jest przeznaczony wyłącznie dla świadczących usługi wsparcia w zakresie rozwiązań teleinformatycznych na podstawie umowy, zamówienia lub porozumienia. Umowy z

osobami świadczącymi wsparcie informatyczne osobiście zawierają klauzulę o zachowaniu poufności oraz spełniają wymogi co do bezpieczeństwa przetwarzania informacji, a w razie przetwarzania danych osobowych postanowienia dotyczące powierzenia przetwarzania danych osobowych. Do osób tych należą ASI i administratorzy poszczególnych systemów (osoby odpowiedzialne za dany zasób informatyczny).
2. Zdalny dostęp w ramach administrowanego systemu jest nadawany przez osobę odpowiedzialną za zasób informatyczny pod kontrolą ASI. Zdalny dostęp może być odebrany przez ASI na wniosek Kanclerz.

III. Zarządzanie zdalnym dostępem dla podmiotów świadczących wsparcie informatyczne w formie innej niż świadczonej osobiście.

1. Zdalny dostęp do zasobów teleinformatycznych dla podmiotów świadczących wsparcie informatyczne jest przeznaczony wyłącznie dla świadczących usługi wsparcia w zakresie rozwiązań teleinformatycznych na podstawie umowy, zamówienia lub porozumienia.
2. Zdalny dostęp do zasobów teleinformatycznych dla podmiotów świadczących wsparcie informatyczne jest przyznawany po podpisaniu stosownej umowy zawierającej klauzulę o zachowaniu poufności oraz po spełnieniu przez podmiot zewnętrzny wymagań bezpieczeństwa AT, a w razie przetwarzania danych osobowych postanowienia dotyczące powierzenia przetwarzania danych osobowych
3. Odpowiedzialność za utrzymanie właściwej kontroli dostępu do zasobów teleinformatycznych na poziomie uprawnień do systemów operacyjnych, baz danych i aplikacji dostępnych w trybie zdalnym spoczywa na osobie odpowiedzialnej za dany zasób informatyczny do którego przydzielany jest dostęp.
4. Uniemożliwia się nadawanie zdalnego dostępu (w tym poprzez wbudowane w oprogramowanie zdalne pulpity, oprogramowanie typu teamviewer) przez innych niż osoby odpowiedzialne za dany zasób informatyczny wskazane w pkt. II powyżej. Wyłącza się losowe generowanie haseł i inne tego typu mechanizmy umożliwiającym nadanie dostępu użytkownikom systemu z pominięciem osób odpowiedzialnych za dany zasób informatyczny.
5. Zdalny dostęp do zasobów teleinformatycznych dla podmiotów świadczących usługi wsparcia teleinformatycznego nie może być przydzielany na dłużej niż na okres trwania umowy.
6. Wniosek o udzielenie zdalnego dostępu, musi być złożony przez podmiot zewnętrzny świadczący usługi do osoby odpowiedzialnej za dany zasób informatyczny wskazanej w pkt. II powyżej do której zostanie przydzielony dostęp zdalny.
7. Rejestr pracowników firm zewnętrznych posiadających zdalny dostęp do zasobów AT prowadzą osoby odpowiedzialne za dany zasób informatyczny (rejestr może być prowadzony elektronicznie).

§12
Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

1) Rozliczalność w systemach teleinformatycznych zapewnia się poprzez dokumentowanie w postaci elektronicznych zapisów w dziennikach systemów (logach), a w programach komputerowych informacji o czasie, osobie i wprowadzanych zmianach, a także poprzez stosowanie indywidualnych loginów i haseł dostępowych.

2) Informacje o logach przechowywane są przez co najmniej dwa lata.
3) W celu zapewnienia kontroli nad rodzajem/typem danych osobowych i sposobem ich przetwarzania w systemach informatycznych, ASI sprawuje nadzór nad oprogramowaniem i systemami informatycznymi użytkowanymi przez ADO.

§13
Udostępniane i likwidacja nośników zawierających dane osobowe

1) W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
a) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi.
b) stosowanie metod kryptograficznych.
c) stosowanie odpowiednich zabezpieczeń fizycznych.
d) stosowanie odpowiednich zabezpieczeń organizacyjnych.
2) W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
3) W przypadku udostępniania danych osobowych odbiorcy danych użytkownik ma obowiązek odnotować komu i kiedy udostępniono poszczególne dane.
4) Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych nie podlegających archiwizacji w odrębnym trybie dla którego cel przetwarzania ustał, ASI lub osoby upoważnione sporządzają protokół, w którym zamieszcza się następujące informacje:
a) datę dokonania likwidacji.
b) przedmiot likwidacji (aplikacja, baza).
c) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.
5) Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują Właściciele zasobów danych osobowych.
6) W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku, gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych.

§14
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1) ASI przed przystąpieniem do naprawy sprzętu komputerowego zobowiązany jest wykonać kopię zapasową danych, a w przypadku przekazania sprzętu komputerowego do zewnętrznego serwisu nie wykonywanego przez ASI, zobowiązany jest do:
a) wykonania kopii danych użytkownika.
b) pozbawienia zapisanych danych w sposób uniemożliwiający ich odzyskanie albo nadzorowania naprawy samodzielnie lub za pośrednictwem pracownika upoważnionego przez ADO.
2) Zakazane jest przekazywanie sprzętu komputerowego do naprawy do zewnętrznych serwisów bez zgody ADO lub osoby upoważnionej przez ADO.

3) Użytkownik komputera jest zobowiązany zgłosić, czy po zwróceniu sprzętu komputerowego z naprawy zostały skopiowane jego dane zgodnie ze stanem sprzed naprawy.
4) W przypadku napraw gwarancyjnych, gdy naprawa odbywa się w biurze użytkownika, przebiega pod nadzorem ASI, który dba, aby osoby nieuprawnione nie miały dostępu do zawartości dysku twardego naprawianego komputera. W przypadku naprawy gwarancyjnej uszkodzonego dysku, można go przekazać do gwaranta w celu wymiany na nowy dopiero po fizycznym zniszczeniu nośnika informacji przez ASI.
5) Jeżeli nie ma możliwości usunięcia lub skopiowania zawartości uszkodzonego dysku, to dysk powinien zostać fizycznie zniszczony przez ASI. Ze zniszczenia dysku sporządza się protokół.
6) Po odebraniu sprzętu komputerowego z naprawy należy zainstalować na dysku twardym standardowy obraz, wykonać jego personalizację dla potrzeb konkretnego użytkownika i skopiować tam jego dane.
7) Procedura wykonywania przeglądów i konserwacji systemu informatycznego, komputerów przenośnych i stacjonarnych:
a) przeglądy i konserwacja systemu i sprzętu dokonywane są na bieżąco. Planowo przegląd i konserwację przeprowadza się raz na pół roku.
b) za bieżące i planowe przeglądy i konserwację systemu oraz sprzętu odpowiada ASI.
c) użytkownik obowiązany jest do prawidłowej eksploatacji powierzonego sprzętu, w sposób zgodny z jego przeznaczeniem. Użytkownik odpowiada za zgłaszanie do ASI usterek uniemożliwiających pracę.

§14[1]
Zasady przeprowadzania zmian, aktualizacji oprogramowania dla zapewnienia bezpieczeństwa informacji

1) W celu wprowadzania zmian w systemach teleinformatycznych dokonuje się aktualizacji jego części składowych w tym w szczególności oprogramowania.
2) Aktualizacje polegają m.in. na wprowadzeniu do systemu poprawek, uaktualnień, nowych funkcjonalności, a także zagwarantowania większego bezpieczeństwa i odporności systemów teleinformatycznych.
3) Administrator wprowadzając aktualizacje, kieruje się przede wszystkim następującymi celami:
   - utrzymaniem wsparcia producenta;
   - naprawa błędów w oprogramowaniu.
   - Ochrona przed złośliwym oprogramowaniem.
   - Ochrona przed kradzieżą tożsamości
   - naprawianiem luk w zabezpieczeniach;
   - uzupełnianie funkcjonalności lub ich rozwój, w celu umożliwienia wykonywania nowych zadań
   - lepszej ochrony zasobów przed niepożądanymi działaniami i atakami.
4) Aktualizacje oprogramowania w zakresie ochrony zasobów oraz naprawy luk w zabezpieczeniach należy robić możliwie szybko po ukazaniu się stosownej poprawki.
5) Przeprowadzając aktualizację uwzględnia się, że poprawki mogą nie być wszechstronnie przetestowane, a co za tym idzie mogą powodować nieprzewidziane zachowanie systemu teleinformatycznego lub oprogramowania. W związku z powyższym przed aktualizacją należy przygotować sobie ścieżkę powrotu do stanu sprzed aktualizacji:
   - przejrzeć fora w poszukiwaniu opinii o implementacji konkretnej poprawki;
   - wykonać pełną kopię systemu, zabezpieczyć dane;
   - o ile to możliwe, wykonać aktualizację na środowisku testowym;
   - monitorować zachowanie systemu po wykonaniu aktualizacji.

§15
Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1) Użytkownik zobowiązany jest zawiadomić IOD oraz ASI, o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności:
a) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła).
b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień.
c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów sieciowych.
d) wykryciu wirusa komputerowego.
e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego.
f) znacznym spowolnieniu działania systemu informatycznego.
g) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe.
h) zmianie położenia sprzętu komputerowego.
i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
2) Do czasu przybycia na miejsce ASI oraz IOD lub wskazanego przez ADO pracownika należy:
a) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców.
b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia.
c) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia.
d) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku.
e) przygotować opis incydentu.
f) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia IOD lub ASI lub osoby przez nich wskazanej.
3) IOD, przy wsparciu ASI, po otrzymaniu zawiadomienia niezwłocznie:
a) przeprowadza postępowanie wyjaśniające zgodnie z procedurą reagowania i oceny naruszeń bezpieczeństwa danych osobowych przyjętą w jednostce (załącznik nr 8 do Polityki ochrony danych osobowych), w celu ustalenia okoliczności naruszenia ochrony danych osobowych i podjęcia stosowanych działań. Podjęcie działań mających zapobiec w przyszłości naruszeniu jest konsultowane z ASI, który wskazuje w szczególności rozwiązania techniczne mające na celu uniknięcie naruszeń w przyszłości.
4) ASI zarządza, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części, o czym informuję IOD.
5) W razie odtwarzania danych z kopii zapasowych ASI upewnia się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
6) ADO po zapoznaniu się z analizą sporządzoną przez IOD i rekomendacji ASI, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego ADO bądź zastosowaniu środków ochrony fizycznej.

7) ASI informuje ADO oraz IOD o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej Instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzeganiu zasad używania oprogramowania antywirusowego, niewłaściwym wykorzystania sprzętu komputerowego lub przetwarzaniu danych w sposób niezgodny z procedurami ochrony danych osobowych.

§15[1]
Rodzaje naruszenia bezpieczeństwa systemu informatycznego („incydenty")

1) ADO w celu szybkiego identyfikowania zagrożenia oraz skutecznego reagowania na incydenty wprowadza definicje i typowy sposób reagowania na naruszenia bezpieczeństwa systemu informatycznego oraz ich oznaczenie. Na podstawie wagi incydentu, a w przypadkach nieudanych prób naruszenia bezpieczeństwa, także na podstawie częstotliwości zagrożenia ich występowania podejmowane są decyzje co do stosowanych rozwiązań zabezpieczających.
2) Incydenty dzieli się na:
- incydenty Cyber;
- incydenty IT
- incydenty RODO

3) Przez naruszenie bezpieczeństwa systemu informatycznego typu cybernetycznego – Cyber- rozumie się naruszenie bezpieczeństwa skutkujące niedostępnością zasobu/serwisu lub nieautoryzowany dostęp do systemu informatycznego. Źródłem takich incydentów jest najczęściej atak pochodzący z sieci internetowej, rzadziej działanie pracownika. Jeżeli w ich wyniku narusza się bezpieczeństwo danych osobowych, incydent taki kwalifikuje się i ocenia również pod kątem przepisów RODO.
4) W przypadku wystąpienia naruszenia bezpieczeństwa systemu informatycznego oznacza się go jako naruszenie typu „Cyber", wskazując dodatkowo jaki typ naruszenia bezpieczeństwa zaistniał uwzględniając podtypy wskazane w pkt. 5) poniżej. Jeżeli incydent dotyczy danych osobowych incydent oznacza się dodatkiem „RODO".
5) Podtypy incydentów Cyber oraz działań podejmowanych w odpowiedzi na nie:

a) **Malware[1].** Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie systemu antywirusowego oraz regularne aktualizowane oprogramowania.
b) **Man in the Middle**[2]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to zapewnienie aktualności certyfikatu bezpieczeństwa i szyfrowanie transmisji danych.
c) **Cross-site scripting**[3]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu: najskuteczniejszym sposobem reakcji jest korzystanie z zaufanego oprogramowania oraz dobrego programu antywirusowego.
d) **Phishing**[4]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to budowanie

[1] zbitka wyrazowa pochodząca od wyrażenia malicious software („złośliwe oprogramowanie"). Wspólną cechą programów uznawanych za malware jest fakt, że wykonują działania na komputerze bez jego zgody i wiedzy użytkownika, na korzyść osoby postronnej.
[2] od sformułowania „człowiekiem pośrodku", jest to typ ataku w ramach którego w transakcji lub korespondencji między dwoma podmiotami (na przykład sklepem internetowym i klientem) bierze udział osoba trzecia. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych. Celem może być również podsłuchanie poufnych informacji oraz ich modyfikacja.
[3] jest to atak, który polega na umieszczeniu na stronie internetowej specjalnego kodu, który może skłonić ich do wykonania działania, którego nie planowali.
[4] atak polegający na próbie pozyskania hasła użytkownika, które służy do logowania się na portalach społecznościowych

świadomości wśród użytkowników oraz edukacja.

e) DDoS (distributed denial of service)[5]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to filtrowanie ruchu dzięki dobrze skonfigurowanemu firewallowi u dostawcy usług internetowych, stosowaniu monitoringu oraz metody honeypot.
f) SQL Injection[6]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to odpowiednie zabezpieczenia na poziomie bazy danych.
g) Ransomware[7]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie aktualnego oprogramowania antywirusowego oraz dokonywanie regularnych aktualizacji systemu.
h) Malvertising[8]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie filtrów blokujących reklamy oraz współpraca z zaufanymi dostawcami;
i) Atak siłowy (brute force)[9]. Typ działań podejmowanych w odpowiedzi na podtyp incydentu to stosowanie odpowiednio mocnych haseł przy czym długość hasła powinna być wyznacznikiem jego siły.

6) incydenty IT, to zdarzenia, występujące w sieci lokalnej i dzieli się je na trzy grupy:
a) awarie sprzętowe, wadliwy sprzęt, przestarzałe i wyeksploatowane urządzenia, przepięcia w sieci zasilającej, klęski żywiołowe.
b) awarie oprogramowania będące skutkiem błędów oprogramowania, których nie wyeliminował producent
c) błędy użytkownika jako działania celowe lub przypadkowe wynikające z nieumiejętności obsługi, pomyłki.

7) Incydenty typu RODO to incydenty Cyber oraz IT jeżeli w ich wyniku narusza się bezpieczeństwo danych osobowych.
8) W celu analizy i zbiorczego zarządzania incydentami odnotowuj ilość i rodzaj incydentów w systemach teleinformatycznych odnotowuje się w okresowych sprawozdaniach i mogą być odnotowywane na podstawie wzoru Załącznika nr 2 do niniejszej Instrukcji lub za pomocą formularza elektronicznego. Incydenty RODO odnotowuje się dodatkowo zgodnie z procedurą wskazaną w Załączniku nr 7 do Polityki ochrony informacji oraz danych osobowych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie. Okresowo (raz na 6 miesięcy lub częściej w razie potrzeby) przeprowadza się ich zbiorczą analizę.

§16
Wymagania dotyczące sprzętu i oprogramowania

1) Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
2) ASI przekazuje IOD listę kluczowych programów użytkowanych przez pracowników jednostki oraz

bądź do serwisów. Po uzyskaniu dostępu, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw.

[5] atak hakerski, mający na celu sparaliżowanie systemu komputerowego albo sieci, poprzez wysłanie sporej ilości zapytań do konkretnego systemu.

[6] atak tego rodzaju polega na uzyskaniu nieuprawnionego dostępu do bazy danych poprzez lukę w zabezpieczeniach aplikacji, na przykład systemu do obsługi handlu internetowego.

[7] celem ataku jest zaszyfrowanie danych użytkownika, a następnie ponowne ich udostępnienie w zamian za opłatę.

[8] atak poprzez użycie nośnika jakim są reklamy internetowe wyświetlane poprzez sieci takie jak Google Adwords. Poprzez reklamy może być zainstalowane złośliwe oprogramowanie na komputerze.

[9] atak opiera się on na niskim poziomie bezpieczeństwa haseł używanych przez pracowników i polega na generowaniu losowych haseł do momentu znalezienia pasującego

dokonuje aktualizacji listy w przypadku zmian użytkowanych programów. Lista zawiera nazwę programu, loginy przypisane do użytkowników. ASI wskazuje IOD powiązania między użytkowanymi programami w zakresie przetwarzanych przez te programy danych osobowych.
3) Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty ASI.
4) Przed wdrożeniem nowego oprogramowania dokonuje się jego oceny pod względem zapewniania funkcjonalności takich jak rozliczalność, integralność i poufność. W ocenie uczestniczy IOD oraz ASI.
5) Przed zainstalowaniem nowego oprogramowania ASI lub inna upoważniona do takich czynności osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
6) Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne
z wymaganiami producenta działanie sprzętu informatycznego.
7) W uzasadnionych przypadkach stosuje się urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
8) Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
9) Należy przechowywać wszystkie poprzednie wersje oprogramowania jako środek utrzymania ciągłości działania.
10) Należy zapewnić ograniczenie dostępu do bibliotek źródłowych programów a dostęp i zmiany odnotowywać.
11) Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.

§17
Postanowienia końcowe

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Każda osoba upoważniona do przetwarzania danych osobowych jest zapoznawana przed dopuszczeniem do przetwarzania danych z niniejszą Instrukcją oraz składa pisemne oświadczenie, potwierdzające znajomość jej treści.
3. Niezastosowanie się do procedur określonych w niniejszej Instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych, może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.
4. ASI odnotowuje wykonane prace i przeglądy dotyczące działań podejmowanych w strukturze teleinformatycznej odzwierciedlający wykonanie w danym miesiącu prace, a także okresowe przeglądy systemu zgodnie z harmonogramem wynikającym z przyjętych dokumentów w tym zakresie. Okresowe sprawozdania mogą być odnotowywane na podstawie wzoru Załącznika nr 2 do niniejszej Instrukcji lub za pomocą formularza elektronicznego.
5. ASI opracowuje i aktualizuje także dodatkową dokumentację (która może być prowadzona elektronicznie lub możliwa do sporządzenia ad hoc na podstawie wyciągów z systemów informatycznych i oprogramowania) której podstawie można określić aktualną i kompletną:
    a. dokumentacje architektury sieci oraz inwentaryzacja linii telekomunikacyjnych;
    b. ewidencje sprzętu i oprogramowania służącego do przetwarzania informacji przekazywanego pracownikowi

c. wykaz użytkowników systemów teleinformatycznych wraz z nadanymi uprawnieniami;
d. ewidencje aplikacji, do których niezbędne jest nadanie uprawnień dodatkowych;
e. wykaz dopuszczonego do użytkowania oprogramowania systemowego i niesystemowego zawierający m.in. informacje o wsparciu przez producenta

6. W odniesieniu do uprawnień do systemu informatycznego na poziomie domeny, aplikacji lub podobnym, przeprowadza się przegląd uprawnień w celu wykrycia nieprawidłowości, w tym nadmiarowych uprawnień lub wykrycia nieaktywnych kont pracowników z aktywnym dostępem raz na 6 miesięcy. Przeglądu dokonuje ASI na podstawie przesłanej przez ADO listy aktualnych pracowników jednostki.
7. Kierownik jednostki zarządza raz do roku audyt w zakresie bezpieczeństwa informacji zgodnie z wymogami § 20 ust. 2 pkt. 14 rozporządzenia KRI.

Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym

PLAN CIĄGŁOŚCI DZIAŁANIA NA WYPADEK AWARII SYSTEMU INFORMATYCZNEGO
w Akademii Teatralnej im. A. Zelwerowicza w Warszawie („procedura")

Cel procedury:

Celem procedury opisanej w niniejszym dokumencie jest minimalizacja zakłóceń w realizacji działalności statusowej Akademii Teatralnej im. A. Zelwerowicza w Warszawie („jednostka") w związku z wystąpieniem zdarzeń mających wpływ na działanie systemu informatycznego w jednostce.

Procedura opisana w niniejszym dokumencie jest powiązana z procedurami dotyczącymi bezpieczeństwa przetwarzania danych osobowych w ten sposób, iż jej uruchomienie oznacza konieczność przeprowadzenia analizy zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych.

Przedmiot procedury:

Przedmiotem procedury jest określenie sposobu działania w razie zaistnienia zdarzeń mających wpływ na działanie systemu informatycznego.

Osoby zgłaszające:

Każdy użytkownik systemu w razie zaistnienia awarii jest zobowiązany do jej zgłoszenia osobom wskazanym w niniejszej procedurze w celu minimalizacji wpływu awarii na funkcjonowanie jednostki.

Typowe rodzaje incydentów:

a. Awaria serwera;
b. Awaria komputera;
c. Awaria urządzeń aktywnych sieci;
d. Awaria infrastruktury sieciowej;
e. Awaria oprogramowania;

- przy czym przez awarie rozumie się stan niesprawności w/w elementów systemu informatycznego uniemożliwiający jego funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie.

Przyczynami powyżej wymienionych zdarzeń mogą być .in..:

a. umyślne lub nieumyślne działania osób zatrudnionych w jednostce;
b. ingerencja osób zewnętrzny.in.m.in. atak hackerski);
c. zdarzenia losowe (zanik zasilania, zalanie)

Osoby odpowiedzialne za realizacje procedury:

O uruchomieniu procedury decyduje
- Rektor lub kanclerz;
- IOD (Inspektor Ochrony Danych Osobowych),
- kierownicy komórek organizacyjnych (po poinformowaniu kierownika jednostki),
- ASI (Administrator Systemu Informatycznego).

Plan działania:

- W razie wystąpienia awarii należy wypełnić wszystkie punkty poniższego planu i sporządzić raport, który stanowi załącznik do niniejszego dokumentu.

LP.	Działanie	Opis działania
1)	Zweryfikować zasadność zgłoszenia od użytkownika	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.
2)	Ustalić źródła awarii	Ustalić, co jest przyczyną awarii: • przerwa w zasilaniu prądem, • brak połączenia z siecią Internet, • wadliwe działanie sprzętu, • wadliwe działanie aplikacji, • wadliwe działanie systemu, na którym uruchomiona jest aplikacja.
3)	Określić skalę awarii	Ustalić, czy awaria powoduje zatrzymanie pracy: • jednego pomieszczenia pracy lub działu • kilku pomieszczeń lub działów • całego budynku • wszystkich budynków
4)	Ustalić, czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.

5)	Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer).
6)	Przygotować serwer zastępczy,	Jako serwer zastępczy można wykorzystać np. Komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.
7)	Podjąć decyzję o terminie odtworzenia maszyny	W razie konieczności należy skontaktować się z właściwymi kierownikami komórek organizacyjnych.
8)	Przywrócić funkcjonowanie aplikacji / systemu	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.
9)	Sprawdzić aplikację / system	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji / systemów zainstalowanych na serwerze.
10)	Uruchomić usługę w systemie informatycznym Teatru	Po uruchomieniu usługi należy powiadomić właściwych kierowników o tym fakcie.

11)	Określić czy awaria/incydent miała wpływ na przetwarzanie danych osobowych	Określić czy dane osobowe przetwarzane w systemie zostały utracone, zmodyfikowane lub udostępnione osobom postronnym. - poinformować Inspektora Ochrony Danych Osobowych o awarii/incydencie mającym wpływ na dane osobowe - dostarczyć raport z podjętych działań Inspektorowi Ochrony Danych Osobowych - zastosować się do wytycznych Inspektora Ochrony Danych Osobowych

W przypadku wystąpienia awarii/incydentu jest on odnotowywany w protokole oraz dzienniku ASI, który jest niezwłocznie dostarczany Inspektorowi Ochrony Danych Osobowych (dopuszczalna jest forma elektroniczna). Protokół oraz Dziennik ASI stanowią odpowiednio załącznik nr 1 do Planu ciągłości działania na wypadek awarii systemu informatycznego oraz 2 do Instrukcji Zarządzania Systemami Informatycznymi.

Miejsce przechowywania kopii zapasowych na wypadek katastrofy

Miejsce przechowywania kopii zapasowych zostało określone w Instrukcji Zarządzania Systemami Informatycznymi oraz wskazane w Załączniku dotyczącym miejsc przetwarzania danych osobowych. Kopie zapasowe na wypadek katastrofy są przechowywane w odległości pozwalającej uniknąć uszkodzeń spowodowanych katastrofą.

Czas przywrócenia ciągłości działania:

Administrator danych osobowych oraz ASI podejmie wszystkie niezbędne działania w celu niezwłocznego przywrócenia działania systemów informatycznych. Przerwa w dostępie do kluczowych funkcjonalności systemu oraz głównych baz danych (klientów oraz pracowników) nie powinien przekroczyć 72 godzin. Jeśli w tym czasie będzie to możliwe przywrócone zostaną w trybie awaryjnym niezbędne do bieżącej pracy funkcjonalności systemu w ciągu 12 godzin.

Realizacja:

W celu realizacji niniejszej procedury administrator danych osobowych (kierownik jednostki) zapewnia środki materialne i osobowe w celu doprowadzenia do zgodności z przep.in.i prawa m.in.:

- kontakt z kluczowymi pracownikami działów, lista z numerami telefonów.
- dostęp do najbardziej aktualnej wersji aplikacji,
- dostęp do aktualnej bazy danych,
- zapewnienie środków dowolnego typu, które w podstawowym zakresie pozwolą na uruchomienie zrealizowanie niniejszej procedury.

Administrator Danych Osobowych może wykonać powyższe przy pomocy ASI.

Załącznik nr 1

do Planu ciągłości działania na wypadek awarii/incydentu dotyczącego systemu informatycznego

WZÓR

PROTOKÓŁ AWARII/INCYDENTU W TYM MAJĄCEGO NEGATYWNY WPŁYW NA PRZETWARZANIE INFORMACJI LUB DANYCH OSOBOWYCH (ICH INTEGRALNOŚCI, POUFNOŚCI LUB DOSTĘPNOŚCI)

Nr protokołu …… , dn ……..

1. Termin realizacji czynności: ……..

2. Osoba przeprowadzająca: ……

3. Osoby uczestniczące: ……

4. Opis incydentu:

……

……

……

4.1. WPŁYW NA INTEGRALNOŚĆ/POUFNOŚĆ/DOSTĘPNOŚĆ: TAK/NIE*

5. Podjęte działania:

……

……

……

6. Wnioski i rekomendacje:

……

……

……

Uwagi:

**zaznaczyć odpowiednie*

Podpis osób uczestniczących Podpis przeprowadzającego

Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym

- W Z Ó R –

Data sporządzenia raportu ……

Stan struktury teleinformatycznej

na miesiąc …… 2020 roku

DZIENNIK ASI

Akademia Teatralna im. A. Zelwerowicza w Warszawie

Liczba awarii krytycznych:
Liczba zgłoszeń standardowych (w tym usterki i wsparcie techniczne użytkowników):
Prace administracyjne:
Status backupów:
Dodatkowe prace wdrożeniowe:
Zgłoszone incydenty ochrony danych (PROTOKÓŁ AWARII/INCYDENTU):
Testy kopii zapasowych (styczeń/sierpień):
Nadane/odebrane uprawnienia do systemu:
Skanowanie systemu po zgłoszeniu działania szkodliwego oprogramowania:
Odtworzenie z kopii zapasowej
Aktualizacja listy oprogramowania:
Protokół zniszczenia nośnika:
Planowy przegląd systemu informatycznego (grudzień):
Przegląd logów systemowych (marzec, czerwiec, wrzesień, grudzień)

……

Podpis ASI

Załącznik nr 2 do Polityki ochrony danych osobowych

Regulamin przetwarzania danych osobowych przez osoby upoważnione do przetwarzania danych osobowych w kartotekach i systemach informatycznych w Akademii Teatralnej im. A. Zelwerowicza w Warszawie

1. Osoby przetwarzające dane osobowe są zobowiązane do zachowaniu poufności wszelkich danych osobowych uzyskanych w toku czynności, w tym do nieujawniania danych osobowych osobom, którym nie jest to niezbędne do realizacji ich zadań powierzonych przez Akademii Teatralnej im. A. Zelwerowicza w Warszawie (zwany dalej „ADO").
2. Osoby przetwarzające dane osobowe mają obowiązek zgłaszania zamiaru powierzenia przetwarzania danych osobowych podmiotom trzecim i konsultacji z IOD treści umów powierzenia przetwarzania danych osobowych.
3. Osoby przetwarzające dane osobowe są zobowiązane powiadomić IOD, a w przypadku systemów informatycznych także ASI o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych. Za zdarzenia naruszające bezpieczeństwo danych osobowych uważa się w szczególności:
   - nieupoważniony dostęp do danych osobowych;
   - ujawnienie bądź utrata danych osobowych;
   - nieupoważniona modyfikacja danych osobowych, kopiowanie lub niszczenie dokumentów zawierających dane osobowe;
   - inne naruszenie postanowień Rozporządzenia RODO.
4. Osobom przetwarzającym dane osobowe do przetwarzania danych osobowych zabrania się:
   1) przetwarzania danych osobowych:
      a) które nie są niezbędne do prawidłowego wykonywania obowiązków pracowniczych,
      b) niezgodnie z celem ich przetwarzania.
   2) udostępniania lub umożliwiania dostępu do danych osobowych osobom nieupoważnionym.
   3) niedopełniania obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach.
   4) uniemożliwiania osobie, której dane dotyczą, korzystania z przysługujących jej praw.
5. Osoba przetwarzająca dane osobowe niszczy zbędne dokumenty papierowe zawierające dane osobowe wyłącznie w niszczarkach.
6. Osoba przetwarzająca dane osobowe nie pozostawia bez nadzoru sprzętu i dokumentów mu powierzonych.
7. Osoba przetwarzająca dane osobowe zabezpiecza pomieszczenie, w którym są przetwarzane przez nią dane osobowe, przed wstępem osób nieupoważnionych.
8. Osoba przetwarzająca dane osobowe nie pozostawia w pomieszczeniu bez nadzoru osób nieupoważnionych do przetwarzania danych osobowych.
9. Osoba przetwarzająca dane osobowe, której udostępniono komputer przenośny nie pozostawia go bez nadzoru, korzysta z szyfrowania dysku.
10. Sprzęt komputerowy i oprogramowanie udostępniane są wyłącznie w celach służbowych. Osoby, którym udostępniono sprzęt komputerowy i oprogramowanie są odpowiedzialne za prawidłowe wykorzystywanie sprzętu i oprogramowania zgodnie z tym celem.
11. Osoby przetwarzające dane osobowe nie są uprawnione do instalacji oprogramowania bez wiedzy i zgody osoby odpowiedzialnej za system informatyczny.
12. Osoby przetwarzające dane osobowe odpowiadają w pełni za skutki uruchomienia zainstalowanego przez siebie oprogramowania bez wiedzy osoby odpowiedzialnej za system

informatyczny.

13. Przypadki instalowania i uruchomienia oprogramowania bez wiedzy ASI, w szczególności gdy jego uruchomienie wywołuje działania niedozwolone, traktowane jest jako celowe i świadome działanie Osoby przetwarzającej dane osobowe zmierzające do zwiększenia ryzyka awarii systemów informatycznych.
14. Osoby przetwarzające dane osobowe nie powinny otwierać załączników w poczcie e-mail, co do których mają uzasadnione podejrzenie, co do ich pochodzenia. W takim przypadku powinny skonsultować się z osobą odpowiedzialną za system informatyczny
15. Osoby przetwarzające dane osobowe powinny stosować następujące postępowanie w stosunku do haseł dostępowych do stacji roboczej i aplikacji:
    a) 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).
    b) 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.
    c) 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.
    d) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności i odpowiada za wszystkie działania wykonane z wykorzystaniem osobistego loginu i hasła.
    e) Zabronione jest przekazywanie haseł innym osobom oraz zapisywanie haseł w sposób jawny (np. na karteczkach samoprzylepnych, w komputerze).
    f) w przypadku nadania pierwszego hasła lub zresetowania hasła przez ASI należy je niezwłocznie zmienić.
16. Osoby przetwarzające dane osobowe stosują następujące zasady rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym:
    a) Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
    b) Podczas logowania należy zwracać uwagę na komunikaty systemu (np. czy ktoś nie próbował włamać się do systemu).
    c) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. polityka czystego ekranu.
    d) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
    e) Po zakończeniu pracy, użytkownik zobowiązany jest:
        - wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
        - zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne.
17. Osoby przetwarzające dane osobowe są zobowiązane do następującego korzystania z zasobów Internetu:
    a) Osoby przetwarzające dane osobowe są zobowiązani do korzystania z serwisów internetowych zgodnie z zakresem swoich obowiązków, w celu realizacji zadań służbowych oraz zadań związanych z podnoszeniem kwalifikacji zawodowych.
    b) Zabrania się:
        - korzystania z serwisów zawierających treści niecenzuralne lub w jakikolwiek sposób naruszające prawo;

- korzystania z serwisów niezwiązanych z obowiązkami pracownika, np. oferujących gry internetowe lub losowe, hazard, prywatne aukcje, rozrywkę, fora dyskusyjne, usługi chat;
- kopiowania i wysyłania plików o przeznaczeniu niewynikającym z wykonywanych zadań służbowych, w tym filmów, plików muzycznych, wygaszaczy oraz gier;
- umożliwiania osobom postronnym (w tym rodzinie i znajomym) dostępu do sieci wewnętrznej oraz do sieci Internet przy wykorzystaniu udostępnionej infrastruktury technicznej;
- podłączenia komputera nie służącego do wykonywania obowiązków pracowniczych do sieci wewnętrznej bez uprzedniej pisemnej zgody administratora sieci.

18. Osoby przetwarzające dane osobowe zobowiązane są do zachowania następujących zasad przy korzystaniu z poczty elektronicznej:
    a) użytkownicy nie mogą używać poczty elektronicznej do celów innych niż służbowe.
    b) zabrania się przesyłania dalej otrzymywanych wiadomości niezwiązanych z realizowaną pracą, np. reklam, "łańcuszków szczęścia", wiadomości obraźliwych, humorystycznych, pornograficznych.
    c) wysyłane załączniki, o ile to możliwe, powinny być skompresowane; załączniki zawierające dane osobowe powinny być szyfrowane, a hasło powinno być przekazane w bezpieczny sposób inną drogą np. sms.
    d) każdy użytkownik powinien archiwizować na swoim komputerze otrzymywane i wysyłane wiadomości.
    e) należy zwracać szczególną uwagę na wiadomości z nie znanych źródeł (adresów), w szczególności zawierających jakiekolwiek załączniki; w takich przypadkach użytkownicy nie powinni uruchamiać załączników (plików z rozszerzeniem typu: .exe, .com, .bat, .pif.
19. W celu zapewnienia bezpieczeństwa sieci oraz jej użytkowników zabrania się dokonywania następujących działań:
    a) instalowania oprogramowania o nieznanym działaniu, należy je traktować za potencjalnie szkodliwe.
    b) skanowania sieci informatycznej.
    c) prowadzenia wszelkiego rodzaju ataków ingerujących w działanie lub zasoby komputerów innych użytkowników lub urządzeń w sieci wewnętrznej, a także osób trzecich i urządzeń w Internecie.
    d) naruszania w jakikolwiek sposób bezpieczeństwa serwerów i ich bezawaryjnej pracy.
    e) zabrania się wykorzystywania narzędzi umożliwiających omijanie zabezpieczeń oraz ograniczeń sieci i systemów teleinformatycznych.
20. Wobec Osób przetwarzających dane osobowe naruszających ww. zasady stosowane będą: blokady kont pocztowych, kont WWW i ftp, ograniczenie dostępu do Internetu (z całkowitą blokadą włącznie) oraz konsekwencje przewidziane przez kodeks pracy, kodeks cywilny oraz kodeks karny.
21. Niepodjęcie działań określonych niniejszym Regulaminem w przypadku stwierdzenia naruszenia ochrony danych osobowych stanowi naruszenie obowiązków Osoby przetwarzającej dane osobowe.
22. W celu wprowadzenia szczegółowych zasad wprowadzone mogą być odrębne procedury.

Załącznik nr 3 do Polityki ochrony danych osobowych

PROCEDURA
nadawania upoważnień do przetwarzania danych osobowych

Podmioty realizujące:

1. Administrator Danych Osobowych (ADO);
2. Inspektor Ochrony Danych (IOD);
3. Kierownicy komórki organizacyjnej;
4. Osoba przetwarzająca dane osobowe;

Cel procedury

Celem procedury jest zapewnienie dopuszczenia do przetwarzania danych osobowych wyłącznie osób do tego upoważnionych.

Nadawanie upoważnień

1. Forma i źródło upoważnienia. Upoważnienie do przetwarzania danych osobowych w jednostce nadawane jest przez ADO (lub wyznaczonego pracownika), który decyduje o zakresie nadanych uprawnień. Upoważnienie może wynikać z polecenia ADO (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 ADO w tym stacji roboczych i oprogramowania, w którym są przetwarzane dane osobowe,
   c) z umocowania ustawowego,
   d) umowy wiążącej strony,
   e) zostać wskazane w dokumencie upoważnienia.
2. Dokument upoważnienia. W przypadku wydania dokumentu upoważnienia jest ono podpisywane przez IOD, osobę, której udzielono upoważnienia oraz osobę decydującą o dopuszczeniu do przetwarzania danych osobowych (ADO lub wyznaczony pracownik) przy czym jego zakres wyznacza ADO lub osoba upoważniona poprzez podjęcie określonych w ust. 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 przez ADO lub wyznaczonego pracownika i wynika w szczególności z polecenia 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 ADO udostępnił dane osobowe, osobie je przetwarzającej;

e) przepisu prawa;
f) powierzenia pełnienia określonej funkcji (np. członek komisji ZFŚS);
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 ust. 3 poleceń przetwarzania ADO w tym w szczególności modyfikacji uprawnień do określonych zasobów informatycznych. Upoważnienie wygasa wraz z odwołaniem upoważnienia, ustania stosunku prawnego pomiędzy ADO i osobą upoważnioną, a także zaprzestania pełnienia wyznaczonej funkcji, chyba, że ADO postanowi inaczej.
5. Upoważniony do przetwarzania danych osobowych jest zobowiązany do zachowania poufności złożonego w odrębnym oświadczeniu, w umowie, wyrażone w przepisach prawa (dotyczących tajemnicy zawodowej, obowiązków wobec pracodawcy wynikających z kodeksu pracy) lub inny sposób.
6. Prowadzona jest lista wydanych upoważnień, która zawiera co najmniej następujące dane: imię i nazwisko, stanowisko lub funkcję osoby przetwarzającej, data rozpoczęcia przetwarzania, data zakończenia przetwarzania.

Załącznik nr 4 do Polityki ochrony danych osobowych

WZÓR UPOWAŻNIENIA ORAZ ODWOŁANIA UPOWAŻNIENIA

Upoważnienie do Przetwarzania Danych Osobowych
numer:

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

Pani/Pana
……..
zatrudnioną/ego na stanowisku
……..
(od ……..)

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 danych szczególnych kategorii wskazanych w art. 9 RODO (tzw. danych wrażliwych) lub 10 RODO (dane dotyczące wyroków skazujących i naruszeń prawa),, jeżeli jest to niezbędne w celu wykonywania obowiązków wyznaczonych przez przełożonego.

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 ADO lub osoby wyznaczonej przez ADO

decydującej o wydaniu upoważnienia i jego zakresie

……

zapoznałem się z dokumentem
podpis osoby upoważnionej

.....

zapoznałem się z dokumentem

podpis Inspektora Ochrony Danych

Załącznik nr 4a *do Polityki ochrony danych osobowych*

Odwołanie Upoważnienie numer […] 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 nadawania upoważnienia

……..

podpis ADO lub osoby wyznaczonej przez ADO

Załącznik nr 5 do Polityki ochrony danych osobowych

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 6 do Polityki ochrony danych osobowych

PROCEDURA
udzielania informacji podawanej w przypadku pozyskiwania danych

I. Podmioty realizujące:
1. Administrator Danych Osobowych (ADO);
2. Osoby przetwarzające dane osobowe (zgromadzenie niezbędnych danych oraz techniczna realizacja wniosku, poinformowanie IOD);
3. Inspektor Ochrony Danych (IOD - w zakresie oceny treści obowiązku informacyjnego).

II. Cel: Celem procedury jest prawidłowe wypełnienie przez ADO obowiązków wskazanych w art. 12, 13 oraz 14 RODO oraz przepisach uzupełniających.

III. Procedura postępowania w sprawie udzielenia obowiązku informacyjnego.
1. W przypadku pozyskiwania danych osobowych wyznaczony pracownik odpowiedzialny za dany proces konsultuje z IOD konieczność i treść obowiązku informacyjnego, 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.
2. IOD określa zakres, treść i sposób spełnienia obowiązku informacyjnego i przedstawia kierownictwu jednostki.
3. Za techniczne spełnienie żądania odpowiada ADO oraz wyznaczony przez niego pracownik/pracownicy.

IV. Sposób zbierania danych i realizacji obowiązku informacyjnego

1. Dane mogą być zbierane przez ADO:
   a. od osoby, której dane dotyczą;
   b. w sposób inny niż od osoby, której dane dotyczą.

V. W zależności od sposobu zbierania danych przez ADO osobie, której dane dotyczą udziela się następujących informacji:

1. W przypadku zbierania danych od osoby, której dane dotyczą, ADO 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 IOD;
   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 ADO 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 ADO 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.

2. Zmiana celu. Jeżeli ADO 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.

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

4. Termin udzielenia informacji. Informacji należy udzielić podczas ich zbierania.

5. W przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, ADO 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 IOD;
   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 ADO lub przez stronę trzecią;
i. informacje o prawie do żądania od ADO 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.

6. 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.

7. Zmiana celu. Jeżeli ADO 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.

8. Wyjątki. Powyższe nie ma zastosowania, 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 ADO 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 ADO, 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.

Załącznik nr 7 do Polityki ochrony danych osobowych

PROCEDURA
reagowania i oceny naruszeń bezpieczeństwa danych osobowych

I. Podmioty realizujące:

1. Inspektor Ochrony Danych (IOD).
2. Administrator Systemu Informatycznego (ASI).
3. Administrator Danych Osobowych (ADO).
4. Osoba przetwarzająca dane osobowe.

II. 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.

III. Wszczęcie postępowania i działania

1. IOD na podstawie zgłoszenia podejmuje działania mające na celu:
   - ograniczenie do minimum negatywnych skutków zdarzenia;
   - wyjaśnienie okoliczności zdarzenia;
   - sporządzenie raportu z podjętych czynności;
   - zgłoszenie (w przypadkach naruszeń skutkujących ryzykiem naruszenia praw lub wolności osób fizycznych) Prezesowi Urzędu Ochrony Danych Osobowych, ADO (w przypadku przetwarzania danych w imieniu innego podmiotu – w roli procesora);
   - zgłoszenie (w przypadku naruszeń powodujących wysokie ryzyko naruszenia praw lub wolności osób fizycznych) osobie/osobom, których dane uległy naruszeniu;
   - poinformowania kierownictwa jednostki o stwierdzonym naruszeniu w celu podjęcia stosowanych działań naprawczych.

2. IOD w ramach powyższych czynności ma prawo do podejmowania wszelkich dopuszczalnych prawem działań, w szczególności:
   - żądania wyjaśnień od osób zatrudnionych przez ADO;
   - nakazania przerwania pracy przy przetwarzaniu danych osobowych;
   - żądania podjęcia niezwłocznych działań przez ASI.

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

IV. Postępowanie

1. Stwierdzenie naruszenia. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, każdy Osoba przetwarzająca dane osobowe, która stwierdzi naruszenie ma obowiązek niezwłocznego zgłoszenia tego faktu IOD niezwłocznie i stosować się do jego wskazówek.

2. Analiza. W przypadku wykrycia przez ADO naruszenia ochrony danych osobowych dokonuje się analizy pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych, wynikiem której może być stwierdzenie naruszenia lub incydentu. Analiza jest wykonywana zgodnie z dokumentem „Data breach severity methodology 1.0" sporządzonym przez European Union Agency of Network and Information Secutity (ENISA).
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 zgłoszenia 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 „incydent"");
    d. przeprowadza się ocenę pod kątem konieczności zgłoszenia osobie, której dane dotyczą (zgodnie z ust. 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 maksymalnie 72 godzin od stwierdzenia jego zaistnienia. W przypadku przetwarzania danych osobowych w imieniu ADO (jako procesor) Incydent należy zgłosić ADO w terminie przewidzianym w umowie z ADO.
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 IOD 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 ADO 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 ADO we współpracy z IOD.

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 osoby należy opisać jasnym i prostym językiem zawierającym charakter naruszenia danych osobowych oraz:
    a. zawierać imię i nazwisko oraz dane kontaktowe IOD 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 ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

- zgłoszenia dokonuje ADO we współpracy z IOD.

9. Wyjątki. Zawiadomienie, o którym mowa w powyżej, nie jest wymagane, w następujących przypadkach:

a. ADO 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. ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o których mowa w pkt. a;
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.

10. Zagrożenia mogące powodować naruszenie ochrony danych
    a. zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
    b. zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, ADO, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
    c. zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.
11. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:
    a. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
    b. niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,
    c. awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
    d. pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
    e. jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
    f. nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
    g. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
    h. nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
    i. ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
    j. praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
    k. ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
    l. podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,

m. rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).
n. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Załącznik nr 8 do Polityki ochrony danych osobowych

PROCEDURA
realizowania uprawnień osób, których dane są przetwarzane

I. 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.

II. Podmioty realizujące:

1. Administrator Danych Osobowych (ADO);
2. Osoba przetwarzająca dane osobowe (zgromadzenie niezbędnych danych oraz techniczna realizacja wniosku, poinformowanie IOD);
3. Inspektor Ochrony Danych (IOD - w zakresie oceny jakie prawo i w jakim zakresie przysługuje osobie).

III. Procedura realizacji praw.

1. W przypadku zgłoszenia żądania dotyczącego prawa do sprostowania danych, osoba otrzymująca zawiadomienie, kieruje zapytanie do ADO, 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 ADO oraz wyznaczony przez niego pracownik/pracownicy;
5. Spełnienie żądania odnotowuje się w ewidencji prowadzonej przez ADO. Uzasadnienie jej prowadzenia wynika z konieczności ustalenia, dochodzenia lub obrony roszczeń.

IV. Sposób realizacji praw:

1. **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).

2. **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.

3. **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.

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

6. 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 ADO 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.

7. Niepodjęcie działań. Jeżeli ADO 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.

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

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

10. Żądanie dodatkowych informacji co do tożsamości. Bez uszczerbku dla art. 11 RODO, jeżeli ADO 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.

11. Wytyczne w sprawie udzielania odpowiedzi.

I. Prawo dostępu do danych osobowych

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od ADO 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 przetwarzanych 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 ADO 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. ADO 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, ADO 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.

II. Prawo sprostowania danych. Osoba, której dane dotyczą, ma prawo żądania od ADO 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.

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

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

III. Prawo do usunięcia danych - prawo do bycia zapomnianym.

1. Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych, a ADO 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 ADO;
f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

2. Jeżeli ADO 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 ADO przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by ci ADO usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Ust. 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 ADO, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;
   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 RODO, 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.

ADO informuje o usunięciu danych osobowych, którego dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

IV. Prawo do ograniczenia przetwarzania.

1. Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania w następujących przypadkach:

   a. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO 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. ADO 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 ADO 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 ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

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

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

V. 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 ADO, oraz ma prawo przesłać te dane osobowe innemu ADO bez przeszkód ze strony ADO, 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, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez ADO bezpośrednio innemu ADO, 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 ADO.

4. Prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

VI. 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. ADO 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.

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.

VII. 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.

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.

VIII. 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.

IX. 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. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
   a. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO;
   b. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega ADO 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.3 lit. a) i c), ADO wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony ADO, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
5. Decyzje, o których mowa w ust. 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) RODO i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Załącznik nr 9 do Polityki ochrony danych osobowych

PROCEDURA
opiniowania zagadnień prawnych związanych z danymi osobowymi

Podmioty realizujące:

1. Administrator Danych Osobowych (ADO);
2. Kierownicy komórek organizacyjnych
3. Inspektor Ochrony Danych (IOD);
4. Osoba przetwarzająca dane osobowe

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

Procedura jest stosowana w zakresie nie regulowanym przez inne procedury obowiązujące u ADO, w szczególności dotyczy opiniowania 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. organizowania 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. Ostateczna decyzja 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.

Załącznik nr 10 do Polityki ochrony danych osobowych

PROCEDURA
szkoleń dla osób przetwarzających dane osobowe

Podmioty realizujące:

1. Administrator Danych Osobowych (ADO);
2. Kierownicy komórek organizacyjnych;
3. Inspektor Ochrony Danych (IOD);
4. Osoba przetwarzająca dane osobowe.

Cel. Celem procedury jest przeprowadzenie dla pracowników jednostki szkoleń z tematów związanych z bezpieczeństwem danych osobowych.

Procedura jest stosowana w zakresie nieuregulowanym przez inne procedury obowiązujące u ADO. Procedura ma na celu kształtowanie świadomości pracowników na temat bezpiecznego przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa oraz ma uzmysławiać pracownikom jakie zagrożenia mogą pojawić się w związku z nieprawidłowym przetwarzaniem danych osobowych.

Procedura przeprowadzenia szkolenia.

1. Szkolenia są przeprowadzane na podstawie przyjętego planu szkoleń przygotowanego przez IOD, który zatwierdza ADO. Plan szkoleń jest corocznie dołączany do Polityki ochrony danych osobowych i został wskazany w Załączniku nr 13. Plan zawiera proponowane ogólne opisy oraz terminy szkoleń, które mogą ulec zmianie na wniosek IOD i za aprobatą ADO lub na podstawie samodzielnej decyzji ADO.
2. ADO ma prawo odstąpić od przeprowadzenia szkolenia przyjętego w planie szkoleń na podstawie swojej decyzji, o czym informuję IOD.
3. Zagadnienia, które mają być tematem szkolenia przygotowuje IOD i przedstawia propozycję danego szkolenia do ADO celem akceptacji.
4. IOD przedstawia również proponowany przebieg i czas trwania szkolenia celem uzyskania aprobaty ADO.
5. Po uzyskaniu akceptacji tematu i czasu szkolenia, IOD przesyła informację o terminie i zakresie szkolenia do kierowników komórek organizacyjnych, których pracownicy mają wziąć udział w szkoleniu.
6. Kierownicy komórek organizacyjnych przesyłają do IOD listę pracowników, którzy wezmą udział w szkoleniu.
7. W dniu szkolenia zgłoszeni pracownicy podpisują listę obecności, potwierdzając swoje stawiennictwo na szkolenie. W przypadku, gdy któryś z zgłoszonych pracowników nie stawi się na szkolenie, kierownik jednostki powinien wyjaśnić przyczynę jego nieobecności IOD oraz ADO.
8. Pracownik, który nie stawił się na szkolenie bez podania uzasadnionej przyczyny może ponieść konsekwencje o charakterze służbowym, zgodnie z regulaminami/procedurami obowiązującymi w jednostce ADO.
9. Szkolenie jest prowadzone przez IOD lub wyznaczoną przez niego osobę posiadającą wystarczające kompetencje i wiedzę z zakresu tematycznego, którego dotyczy szkolenie.

10. Po zakończeniu szkolenia IOD przesyła informacje do ADO na temat frekwencji, czego potwierdzeniem jest sporządzona lista obecności oraz relacjonuje przebieg szkolenia.
11. ADO może zarządzić przeprowadzenie szkolenia nie ujętego w planie szkoleń, jeśli wymaga tego sytuacja związana z przetwarzaniem danych osobowych w jednostce.
12. W przypadku decyzji przeprowadzenia szkolenia nie ujętego w planie szkoleń, ADO przekazuje tę informację do IOD, który przygotowuje program szkolenia zgodnie z zakresem przedstawionym przez ADO. Po przygotowaniu programu szkolenia IOD przedstawia go ADO celem akceptacji.
13. IOD przedstawia ADO proponowany termin przeprowadzenia szkolenia nie ujętego w planie szkoleń, zgodnie z posiadanymi przez siebie możliwościami czasowymi realizacji takiego szkolenia.
14. Odnośnie szkoleń nie ujętych w planie szkoleń, proces ich realizacji przebiega identycznie jak podczas zaplanowanych szkoleń, zgodnie z pkt. 5-10 niniejszej procedury.

Załącznik nr 11 do Polityki ochrony danych osobowych

PROCEDURA
kontroli przestrzegania przepisów RODO z zakresu bezpieczeństwa danych osobowych

Podmioty realizujące:

1. Administrator Danych Osobowych (ADO);
2. Administrator Systemu Informatycznego (ASI);
3. Kierownicy komórek organizacyjnych;
4. Inspektor Ochrony Danych (IOD);
5. Osoba przetwarzająca dane osobowe

Cel. Celem procedury jest sprawdzenie przestrzegania przez pracowników zasad bezpieczeństwa przetwarzania danych obowiązków podczas wykonywania czynności służbowych.

Procedura jest stosowana w zakresie nieuregulowanym przez inne procedury obowiązujące u ADO. Procedura ma na celu zapewnienie prawidłowego funkcjonowania przepisów RODO w jednostce oraz wykrycie ewentualnych błędów oraz zagrożeń związanych z niewłaściwym przetwarzaniem danych osobowych.

Procedura przeprowadzenia kontroli.

1. Kontrola jest przeprowadzana na zlecenie ADO, który składa taki wniosek do IOD. Kontrola może dotyczyć wybranego elementu przetwarzania danych osobowych lub obejmować pełne spektrum obszaru związanego z bezpieczeństwem danych osobowych.
    a) kontrola może mieć charakter cykliczny, jeśli tak stanowią zapisy Polityki ochrony danych osobowych. W takim przypadku IOD występuję do ADO z wnioskiem o wszczęcie takiej kontroli, na co najmniej tydzień przed zaplanowanym terminem kontroli,
    b) IOD ma prawo wystąpić samodzielnie do ADO z wnioskiem o przeprowadzenie kontroli, jeśli posiada uzasadnione przesłanki, że mogło nastąpić naruszenie bezpieczeństwa danych osobowych lub istnieje możliwość, że takie naruszenie może się pojawić.
2. Po otrzymaniu wniosku o przeprowadzenie kontroli od ADO, IOD dokonuje analizy zagadnień, które mają zostać skontrolowane. Po zamknięciu procesu analizowania IOD przedstawia listę zagadnień, które będą podlegać kontroli. W zależności od obszaru, który będzie podlegał kontroli lista zagadnień może dotyczyć takich elementów jak:
    - dokumentacja papierowa lub elektroniczna,
    - wiadomości e-mail,
    - aplikacje i programy elektroniczne,
    - miejsca przetwarzania danych osobowych,
    - wywiady z kierownikami/pracownikami.
3. IOD przedstawia listę zagadnień kontrolnych ADO w celu ustalenia terminu przeprowadzenia kontroli. Po ustaleniu terminu IOD przystępuje do procesu przeprowadzenia kontroli.

4. Podczas przeprowadzenia kontroli IOD ma prawo dostępu do wszelkich dokumentów/aplikacji/wiadomości e-mail/miejsc przetwarzania związanych z przetwarzaniem danych osobowych, chyba że ADO zabroni dostępu do danego elementu ze względu na inne przepisy prawne lub regulaminy/procedury wewnętrzne.
5. W przypadku dokonywania kontroli związanej z wiadomościami e-mail lub aplikacjami/programami elektronicznymi IOD ma prawo wystąpić do ASI o niezbędną pomoc oraz o umożliwienie dostępu do obszarów, którymi ASI zarządza w ramach czynności służbowych.
6. Podczas przeprowadzenia kontroli wszyscy kierownicy/pracownicy komórki organizacyjnej, których dotyczy proces kontrolny mają obowiązek współpracować z IOD w ramach czynności kontrolnych.
7. Na żądanie IOD kierownicy/pracownicy komórki organizacyjnej mają obowiązek przedstawić wskazane dokumenty papierowe lub elektroniczne oraz umożliwić IOD dostęp do miejsc przetwarzania danych osobowych.
8. Jeśli będzie to konieczne IOD ma prawo przeprowadzić wywiad kontrolny z kierownikiem/pracownikiem komórki organizacyjnej w celu ustalenia procesu przetwarzania danych osobowych na danym stanowisku pracy lub w danej komórce organizacyjnej. Termin wywiadu IOD uzgadnia z danym kierownikiem komórki organizacyjnej, aby nie spowodować zakłóceń w funkcjonowaniu pracy danej komórki organizacyjnej. Termin wywiadu musi być jednakże wyznaczony w ramach czasowych, które zostały przyjęte do przeprowadzenia kontroli we wniosku kontrolnym zatwierdzonym przez ADO, zgodnie z pkt. 3.
9. Po zakończeniu wszystkich czynności kontrolnych związanych z sprawdzeniem dokumentów papierowych i elektronicznych, sprawdzeniu aplikacji/programów elektronicznych oraz wiadomości e-mail, kontrolą miejsc przetwarzania danych osobowych oraz przeprowadzeniem wywiadów z kierownikami/pracownikami, IOD przystępuje do analizy pozyskanych materiałów kontrolnych.
10. Podczas etapu dokonywania analizy uzyskanych materiałów kontrolnych IOD ma prawo zwrócić się do ASI lub kierownika/pracownika komórki organizacyjnej o dodatkowe wyjaśnienia lub złożyć prośbę o uzupełnienie dodatkowych dokumentów, których IOD nie uzyskał lub o których istnieniu nie wiedział podczas czynności kontrolnych. ASI lub kierownik/pracownik komórki organizacyjnej mają obowiązek udzielić wyjaśnień lub przesłać wymagane dokumenty w trybie niezwłocznym, tzn. w ciągu 24h od złożenia prośby przez IOD o wyjaśnienia lub przesłanie/udostępnienie dokumentu.
11. Udzielenie niepełnych/nieprawdziwych informacji lub celowe zatajenie informacji oraz nie udostępnienie dokumentu podczas procesu kontrolnego przeprowadzanego przez IOD, może skutkować dla kierownika/pracownika komórki organizacyjnej konsekwencjami natury służbowej w ramach instrumentów prawnych posiadanych przez ADO.
12. IOD po zakończeniu procesu analizy uzyskanych materiałów kontrolnych przygotowuje raport z kontroli i przedstawia sporządzony dokument ADO. Raport jest sporządzany na podstawie uzyskanych przez IOD podczas kontroli informacji, więc w przypadku braku danych dokumentów lub wyjaśnień złożonych przez kierownika/pracownika komórki organizacyjnej może nie zawierać w pełni wyczerpujących konkluzji.
13. W przypadku zaistnienia nowych okoliczności, które nie zostały ujawnione podczas czynności kontrolnych, IOD ma prawo zwrócić się do ADO o dokonanie dodatkowej kontroli obejmującej obszar, który jest związany z ujawnionymi okolicznościami.
14. W przypadku, gdy przygotowany raport końcowy zawiera wnioski/oceny wskazujące na potrzebę wprowadzenia zmian lub ujawnione zostały błędy w zakresie przetwarzania danych osobowych, IOD ma obowiązek przedstawić ADO rozwiązania w obszarach, które wymagają zmian w zakresie bezpieczeństwa danych osobowych.
15. ADO wydaje końcową decyzję odnośnie wdrożenia zmian, których wprowadzenie jest sugerowane przez IOD na podstawie zakończonego procesu kontrolnego.

Załącznik nr 12 do Polityki ochrony danych osobowych

Wytyczne postępowania z danymi osobowymi na czas pracy zdalnej

ADO podejmuje decyzje, które zadania są niezbędne w celu zachowania ciągłości działania jednostki na czas trwania pracy zdalnej i decyduje o możliwości przetwarzania danych osobowych poza siedzibą jednostki.

Wszelkie wynoszone dokumenty i nośniki danych, a także sprzęt wykorzystywany poza obszarem przetwarzania danych osobowych, muszą być odpowiednio zabezpieczone w sposób zapewniający:

- Zabezpieczenie przed kradzieżą, utratą lub zniszczeniem – zasada dostępności danych;
- Uniemożliwienie zmiany treści danych/zawartości dokumentów lub nośników przez osobę nieupoważnioną – zasada integralności danych;
- Zabezpieczenie treści danych/zawartości dokumentów lub nośników przed osobami nieuprawnionymi – zasada poufności.

W szczególności:

Dokumenty.

- Dokumenty w formie papierowej powinny być umieszczane w koszulkach lub foliach, a następnie twardych i zamykanych teczkach aktowych, zabezpieczających przed uszkodzeniami fizycznymi;
- Dokumenty w formie papierowej powinny być podczas transportu pod opieką osoby, której zostały wydane. Nie mogą być pozostawiane bez opieki także w zamkniętym samochodzie;
- Dokumenty w formie papierowej powinny być przetrzymywane w miejscu wykonywania pracy poza siedzibą jednostki w sposób bezpieczny i uniemożliwiający wgląd do nich także członkom rodziny.

Urządzenia i nośniki elektroniczne (m.in. pendrive, CD-ROM).

- Nośniki powinny być podczas transportu pod opieką osoby, której zostały wydane. Nie mogą być pozostawiane bez opieki także w zamkniętym samochodzie;
- Nośniki powinny być przetrzymywane w miejscu wykonywania pracy poza siedzibą jednostki w sposób bezpieczny i uniemożliwiający wgląd do nich także członkom rodziny;
- Nośniki w miarę możliwości powinny być szyfrowane.

Prywatne komputery i urządzenia.

- Korzystanie z prywatnych komputerów i urządzeń powinno być ograniczone do minimum, jeśli nie istnieje taka potrzeba należy ograniczyć zapisywanie plików, wiadomości e-mail na prywatnych dyskach i komputerach;
- Zabezpieczenia na prywatnych komputerach i urządzeniach powinny w miarę możliwości obejmować antywirusy oraz firewalle;
- Hasła nie powinny być przechowywane/zapisywane, a jedynie wpisywane w celu logowania do sytemu.

Transport (przenoszenie, przewożenie).

1. Dokumenty papierowe, nośniki elektroniczne, urządzenia przenośne mogą być transportowane wyłącznie w zamkniętej torbie/plecaku/walizce/skrzyni uniemożliwiających łatwe poznanie ich zawartości. Niedozwolone jest ich przenoszenie w zewnętrznych kieszeniach ubrań, reklamówkach, worka foliowych lub torbach nieposiadających zamknięcia, a także w inny sposób mogący skutkować uszkodzeniem, zniszczeniem, zalaniem (np. ze względu na warunki atmosferyczne). Torba/plecak/walizka/skrzynia musi przez cały czas znajdować się pod bezpośrednią kontrolą użytkownika i w zasięgu jego wzroku;
2. W przypadku transportowania dużej ilości dokumentów w formie papierowej i/lub kilku elektronicznych urządzeń przenośnych (tj. takiej ich ilości, która nie zmieści się w jednej torbie/plecaku/walizce/skrzyni), powinno odbywać się to w asyście innej osoby (osób) upoważnionych (upoważnionej), przy użyciu stosownej liczby toreb/plecaków/walizek/skrzyń zapewniających odpowiednie zabezpieczenie dokumentów i elektronicznych urządzeń przenośnych;
3. Zaleca się przewożenie znacznej ilości dokumentów papierowych lub elektronicznych urządzeń przenośnych przy wykorzystaniu floty samochodów służbowych lub pomocy pracowników korzystających ze zgodą pracodawcy z samochodów prywatnych do celów służbowych;
4. W przypadku korzystania ze środków komunikacji publicznej/taksówek, należy zachować szczególną ostrożność;
5. Niedopuszczalne jest przekazywanie torby / plecaka / walizki / skrzyni, zawierającej dokumenty lub elektroniczne urządzenia przenośne w bezpośrednie władanie osób postronnych ani informowanie tych osób o ich zawartości;
6. Niedopuszczalne jest pozostawienie torby / plecaka / walizki / skrzyni bez nadzoru, np. w szatni, depozycie, samochodzie.

Przechowywanie.

1. Dokumenty i elektroniczne urządzenia przenośne, które zostały wyniesione poza obszar przetwarzania, muszą być przechowywane w miejscu odpowiednio zabezpieczonym przed dostępem osób nieupoważnionych lub osób trzecich, a także uszkodzeniami fizycznymi;
2. Niedopuszczalne jest pozostawienie dokumentów i elektronicznych urządzeń przenośnych bez nadzoru w prywatnych mieszkaniach osób trzecich, recepcjach, oddawanie w depozyt, itp.;
3. Niedopuszczalne jest przechowywanie środków dostępu do dokumentów i/lub elektronicznych urządzeń przenośnych (np. kluczy do toreb, haseł dostępu do komputera, PIN-u do telefonu) bezpośrednio przy dokumentach i/lub sprzęcie.

Korzystanie.

1. Dokumenty papierowe, nośniki i urządzenia elektroniczne powinny być przygotowane do pracy (wyjmowane z teczek, uruchamiane) wyłącznie na czas pracy i niezwłocznie chowane, wyłączane (wygaszane, szyfrowane) po zakończeniu pracy;
2. Po ustaniu konieczności przetwarzania danych osobowych, należy je niezwłocznie trwale zniszczyć lub usunąć z elektronicznego urządzenia przenośnego lub stacjonarnego nie będącego własnością administratora;
3. W przypadku korzystania z prywatnych elektronicznych urządzeń przenośnych i stacjonarnych, będących własnością użytkownika, przez osoby inne niż użytkownik, należy założyć osobne, zahasłowane profile na tych urządzeniach, ograniczające nieupoważnionym osobą – w tym członkom rodziny – dostęp do zasobów służbowych przechowywanych na tych urządzeniach. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec

domowników i osób bliskich, identyfikator oraz hasło do profilu, o którym mowa w zdaniu poprzedzającym i ponosi za to odpowiedzialność;
4. Niedopuszczalne jest współdzielenie służbowego elektronicznego urządzenia przenośnego z osobami nieuprawnionymi, a także zapoznawanie ich z treścią dokumentacji;
5. Niedopuszczalne jest korzystanie na służbowym elektronicznym urządzeniu przenośnym z niezabezpieczonych, publicznych sieci Wi-Fi. Nie zaleca się korzystania z takich sieci na prywatnym elektronicznym urządzeniu przenośnym;
6. Niedopuszczalne jest samodzielne instalowanie na służbowym elektronicznym urządzeniu przenośnym jakichkolwiek programów czy aplikacji ani łączenie ich z innymi niezależnymi i niezabezpieczonymi urządzeniami elektronicznymi;
7. Niedopuszczalne jest korzystanie z dokumentacji i elektronicznych urządzeń przenośnych w bezpośredniej obecności osób nieuprawnionych, w sposób naruszający zasady określone powyżej lub stwarzających ryzyko takiego naruszenia. Szczególną ostrożność należy z zachować w środkach komunikacji publicznej.

Incydenty.

W przypadku utraty / zniszczenia / zagubienia dokumentów lub elektronicznych urządzeń przenośnych lub wystąpienia innych okoliczności stwarzających ryzyko naruszenia ochrony danych osobowych, w związku z przetwarzaniem danych osobowych poza obszarem przetwarzania, należy zawiadomić o tym fakcie kierownictwo jednostki oraz IOD.

Załącznik nr 13 *do Polityki ochrony danych osobowych*

SPIS OBOWIĄZUJĄCYCH REJESTRÓW, EWIDENCJI, LIST I INNYCH DOKUMENTOW SPORZĄDZONYCH W JEDNOSTCE W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

Lista aktualna na dzień: […]
Rejestry oraz listy (ewidencje) prowadzone przez IOD na podstawie Polityki ochrony danych osobowych:

Podstawowe rejestry i listy:

1. Rejestr czynności przetwarzania danych osobowych (obejmującym wykaz zbiorów oraz oprogramowanie do jego przetwarzania);
2. Rejestr kategorii przetwarzania danych osobowych (brak zdarzeń uzasadniających konieczność prowadzenia na dzień aktualności niniejszej listy)
3. Lista (ewidencja) osób upoważnionych do przetwarzania danych prowadzona na podstawie procedury nadawania upoważnień;
4. Lista (ewidencja) obowiązków informacyjnych prowadzona na podstawie procedury udzielania informacji podanej w przypadku pozyskiwania danych wraz z treścią obowiązków informacyjnych;
5. Lista umów powierzenia prowadzona na podstawie Polityki ochrony danych osobowych;
6. Lista (ewidencja) miejsc przetwarzania danych osobowych wraz z zabezpieczeniami prowadzona na podstawie Polityki ochrony danych osobowych.
7. Lista incydentów realizowana na podstawie procedury reagowania i oceny naruszeń bezpieczeństwa danych

Dokumenty uzupełniające:

8. Szkolenie stanowiskowe – dokument aktualizowany w miarę potrzeb przez IOD w uzgodnieniu z ADO;
9. Wzór umowy powierzenia przetwarzania danych osobowych;
10. Analizy prawne zagadnień opiniowanych przez IOD w tym konieczności prowadzenia określonych rejestrów;
11. Instrukcja wraz z Oświadczeniem i obowiązkiem informacyjnym COVID – widownia Teatru;
12. Specyfikacja techniczna zawierająca wymagania minimalne dla systemów informatycznych
13. Zarządzeniem Rektora nr 1/2019 z dnia 3 stycznia 2019 ZASADY DOSTĘPU DO UCZELNI OSÓB NIEPOSIADAJĄCYCH KARTY DOSTĘPOWEJ DO BUDYNKU AKADEMII TEATRALNEJ

Dokumenty sporządzane okresowo:

14. Plan sprawdzeń – dokument aktualizowany corocznie przez IOD w uzgodnieniu z ADO – raz do roku wraz z notatkami ze sprawdzenia;
15. Plan szkoleń – dokument aktualizowany corocznie przez IOD w uzgodnieniu z ADO – raz do roku;
16. Całościowa analiza ryzyka przetwarzania danych osobowych – raz na dwa lata – dotyczy całości przetwarzania danych osobowych

Dokumenty do wdrożenia w przypadku wystąpienia zdarzenia uzasadniającego ich prowadzenie:

17. Lista realizacji uprawnień (wniosków) osób, których dane są przetwarzane prowadzona na podstawie procedury realizowania uprawnień osób, których dane są przetwarzane (brak zdarzeń uzasadniających konieczność prowadzenia na dzień aktualności niniejszej listy);
18. Lista realizacji wniosków o udostępnienie danych osobowych (brak zdarzeń uzasadniających konieczność prowadzenia na dzień aktualności niniejszej listy);
19. Lista wydanych nagrań monitoringu zawierających pomiot, któremu wydano nagranie, datę wydania oraz podstawę wydania.

Wzór rejestru udostępnienia nagrań z monitoringu

Lp.	Data udostępnienia	Nagranie z dnia i godziny.	Podstawa udostępnienia *(Wniosek, żądanie) oraz podmiot, któremu udostępnia się dane*	Uwagi