Załącznik nr 1
do Zarządzenia Rektora nr 14/2018
z dnia 25.05.2018 r.

Polityka ochrony danych osobowych w Akademii Sztuk Pięknych w Warszawie

§ 1

Postanowienia ogólne

1. Polityka ochrony danych osobowych w Akademii Sztuk Pięknych w Warszawie (dalej: „Akademia") jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach i procesach przetwarzania danych osobowych przetwarzanych przez Akademię, w tym zbiorach przetwarzanych w systemie informatycznym.
2. Akademii przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 4 Rozporządzenie Parlamentu Europejskiego I Rady (Ue) 2016/679 Z Dnia 27 Kwietnia 2016 R. W Sprawie Ochrony Osób Fizycznych W Związku Z Przetwarzaniem Danych Osobowych I W Sprawie Swobodnego Przepływu Takich Danych Oraz Uchylenia Dyrektywy 95/46/We (Ogólne Rozporządzenie O Ochronie Danych) z dnia 27 Kwietnia 2016 R. (Dz.Urz.Ue.L Nr 119, Str. 1) – dalej Rozporządzenie RODO.
3. Akademia przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli istnieje ku temu podstawa prawna określona w art. 6 lub 9 RODO lub innych regulacjach.
4. Niniejszy dokument ma na celu realizację założeń ochrony danych osobowych określonych w:
   a) Konstytucja Rzeczypospolitej Polskiej,
   b) Rozporządzenie RODO,
   c) innych przepisach wydanych i przyjętych w celu realizacji ochrony danych osobowych w tym aktach wewnętrznych.
5. Akademia dąży do realizacji zasad, które wskazują, iż dane osobowe muszą być:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
   d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane

dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

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

§ 2

Definicje

Przez użyte w treści Polityk ochrony danych sformułowania należy rozumieć:

1) Rozporządzenie RODO - Rozporządzenie Parlamentu Europejskiego i Rady (Ue) 2016/679 Z Dnia 27 Kwietnia 2016 R. W Sprawie Ochrony Osób Fizycznych W Związku Z Przetwarzaniem Danych Osobowych I W Sprawie Swobodnego Przepływu Takich Danych Oraz Uchylenia Dyrektywy 95/46/We (Ogólne Rozporządzenie O Ochronie Danych) Z Dnia 27 Kwietnia 2016 R. (Dz.Urz.Ue.L Nr 119, Str. 1).
2) Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
3) Zbiór danych osobowych - dane osobowe zgromadzone w usystematyzowany sposób według kryterium rodzaju danych, celu albo osoby/działu przetwarzającej w jednostce.
4) Przetwarzanie danych osobowych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
5) Administrator Danych Osobowych - Akademia, a w jego imieniu Rektor.
6) Inspektor danych osobowych – osoba wyznaczona przez Administratora Danych Osobowych odpowiedzialna za zadania określone w § 3 Polityki ochrony danych
7) Administrator Systemu Informatycznego - osoba wyznaczana przez Administratora Danych Osobowych odpowiedzialna za przestrzeganie zasad ochrony danych osobowych w systemie informatycznym i nadzorująca przetwarzanie danych osobowych w systemie informatycznym.
8) System informatyczny - zespół środków technicznych (urządzenia: komputerowe,

drukujące, łączności, wraz z okablowaniem i oprogramowaniem), zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieć informatyczna i udostępniane przez nią zasoby.

9) Osoby zatrudnione przy przetwarzaniu danych osobowych - wszystkie osoby, w tym użytkownicy systemu informatycznego, mające z racji wykonywanych obowiązków dostęp do danych osobowych. Osobą zatrudnioną przy przetwarzaniu danych osobowych może być pracownik Akademii, a także osoba wykonująca usługi na podstawie umowy zlecenia lub innej umowy cywilno-prawnej pod warunkiem, iż wykonuje te prace osobiście.
10) Poufność - zapewnienie dostępu do informacji wyłącznie osobom upoważnionym.
11) Integralność - spójność danych osobowych, zapewnienie, że dane nie zostaną zmienione, dodane lub usunięte w nieautoryzowany sposób.

§ 3

Zarządzanie przetwarzaniem i bezpieczeństwem danych osobowych

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

- W ramach wypełniania obowiązków wskazanych w lit. a:
  a. informuje o zmianach i nowych interpretacjach w dziedzinie danych osobowych w zakresie dotyczącym administratora danych osobowych;
  b. informuje o obowiązkach nałożonych przepisami oraz dokumentami wewnętrznymi na pracowników;
  c. udziela odpowiedzi i konsultacji w zakresie stosowania przepisów dotyczących przetwarzania danych osobowych;
- W ramach wypełniania obowiązków wskazanych w lit. b:
  a. cyklicznie informuje o zaobserwowanych zagrożeniach w dziedzinie ochrony danych osobowych;
  a. cyklicznie kieruje zapytania dotyczące przetwarzania danych osobowych;
  b. prowadzi audyty planowe według przyjętego harmonogramu;
  c. prowadzi audyty doraźne;

3. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem

ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

4. Kierownictwo Akademii zapewnia, by Inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
5. Kierownictwo Akademii wspiera Inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 Rozporządzenia RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
6. Kierownictwo Akademii zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
7. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
8. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. kierownictwo Akademii zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
9. kierownictwo Akademii powierza Inspektorowi danych osobowych:
    a. monitoring i aktualizacja prowadzonej dokumentacji przetwarzania danych osobowych;
    b. prowadzenie rejestrów czynności danych osobowych i kategorii danych osobowych (o ile jest taka potrzeba) zgodnie z uzyskanymi informacjami;
    c. prowadzenie rejestru osób upoważnionych do przetwarzania danych zgodnie z uzyskanymi informacjami;
    d. opiniowanie umów przetwarzania danych osobowych pod kątem Rozporządzenia RODO;
    e. prowadzenie rejestru incydentów;
10. Inspektor danych osobowych podlega bezpośrednio wyłącznie kierownictwa Akademii.
11. kierownictwo Akademii może powołać zastępców Inspektora danych osobowych wspierających go w realizacji zadań;
12. **Kierownicy komórek organizacyjnych** (przez które rozumie się także osoby zajmujące samodzielne stanowiska, o ile odpowiadają one samodzielnie za wybrane obszary przetwarzania danych osobowych) są odpowiedzialni za:
    a. zarządzenie zasobem danych osobowych w ramach komórki organizacyjnej;
    b. występowanie z wnioskiem do Administratora Systemu Informatycznego o nadanie, zmianę lub cofnięcie uprawnień pracownikom do określonego zasobu danych osobowych przetwarzanego w systemie informatycznym w tym aplikacjach;
    c. bieżąca kontrola nad realizacją zasad przetwarzania danych osobowych przez podległych pracowników;
    d. zabezpieczenie obszaru przetwarzania danych osobowych;
    e. zgłaszania do Inspektora danych osobowych zamiaru podjęcia nowych czynności przetwarzania na danych osobowych w tym w szczególności zamiaru powierzenia przetwarzania danych osobowych podmiotom zewnętrznym;
    f. zgłaszania do Inspektora danych osobowych incydentów przetwarzania danych osobowych;
    g. konsultowanie z Inspektorem danych osobowych podstawy przetwarzania danych osobowych w tym zasadności dopuszczenia do przetwarzania zbiorów osób i podmiotów trzecich;
    h. realizację procesu udostępniania danych osobowych;
    i. realizację zapisów umów powierzenia przetwarzania danych osobowych;

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

§ 4

Osoby przetwarzające dane osobowe

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby posiadające upoważnienie i wpisane do ewidencji prowadzonej przez Inspektora Danych Osobowych (według wzoru ustalonego w Akademii)
2. Dział Kadr informuje Inspektora danych osobowych o osobie, która ma zostać dopuszczona do przetwarzania danych osobowych w celu wystawienia odpowiedniego upoważnienia wraz z niezbędnymi informacjami. Uprawnienia do systemów informatycznych są nadawane przez Administratora Systemów Informatycznych.
3. Wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób oraz obszar przetwarzania danych osobowych, opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznym stanowią załącznik do niniejszej Polityki ochrony danych.
4. Administrator Danych Osobowych wydaje i ewidencjonuje oraz przechowuje imienne upoważnień do przetwarzania danych osobowych oraz dokumentów anulujących upoważnienia. Upoważnienie może zostać wydane na czas określony lub do odwołania. Anulowanie upoważnienia jest konieczne wyłącznie w przypadku uprzedniego wydania upoważnienia na czas do odwołania. Proces powyższy realizowany jest według zasad przyjętych w Akademii.
5. Administrator Danych Osobowych zbiera, ewidencjonuje i przechowuje oświadczenia osób przetwarzających dane osobowe o zachowaniu w tajemnicy oraz ochronie przed dostępem osób nieupoważnionych danych osobowych, z którymi mają styczność oraz o zobowiązaniu do przestrzegania przepisów o ochronie danych osobowych, w tym postanowień niniejszego regulaminu (wzór oświadczenia stanowi załącznik Nr 6 do niniejszego regulaminu). Proces powyższy realizowany jest według zasad przyjętych w Akademii.
6. Brak ważnego upoważnienia, o którym mowa w ust. 1, lub podpisanego oświadczenia, o którym mowa w ust. 2, uniemożliwia powierzenie osobom wykonywania zadań i obowiązków związanych z przetwarzaniem danych osobowych.

§ 5

Obowiązki osób przetwarzających dane osobowe

1. Obowiązki osób przetwarzających dane osobowe zostały określone w odrębnym Regulaminie.
2. Nieprzestrzeganie wskazanych tam obowiązków stanowi przedmiot analizy Administratora Danych Osobowych w konsultacji z Inspektorem Danych Osobowych. Administrator Danych Osobowych podejmuje decyzję o konsekwencjach mających być wyciągniętych wobec osoby naruszającej Regulamin, o którym mowa w ust. 1
3. Poza Regulaminem Administrator Danych Osobowych może także wydawać procedury i instrukcje obowiązujące osoby przetwarzające dane osobowe.

§ 6

Umowy powierzenia danych osobowych

1. W przypadku powierzenia przetwarzania danych osobowych podmiotom trzecim, niewykonujących przetwarzania osobiście lub wykonujących przetwarzanie danych wspólnie z innymi osobami powierzenie następuje w drodze umowy powierzenia danych osobowych lub innego równorzędnego dokumentu dopuszczonego przez Rozporządzenie

RODO.
2. Umowa powierzenia przetwarzania danych lub inny równorzędny dokument powinien zawierać elementy wskazane w Rozporządzeniu RODO.
3. Powierzenie przetwarzania danych osobowych jest konsultowane z Inspektorem Danych Osobowych.
4. Administrator Danych Osobowych ewidencjonuje umowy powierzenia danych osobowych.

§ 7

Udostępnianie danych osobowych odbiorcom

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

§ 8

Incydenty

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

§ 9

Gromadzenie danych osobowych

1. Dane osobowe przetwarzane w Akademii mogą być uzyskiwane:
   a) bezpośrednio od osób, których te dane dotyczą,
   b) z innych źródeł, w granicach dozwolonych przepisami prawa.
2. Przetwarzanie danych osobowych może odbywać się wyłącznie w sytuacjach przewidzianych w art. 6 oraz 9 Rozporządzenia RODO oraz stosownych regulacjach wydanych na tej podstawie.
3. Dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
4. Zbierane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych")
5. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być

przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą lub niszczone, chyba że przepis prawa stanowi inaczej.

6. W przypadku konieczności udostępnienia dokumentów i danych osobowych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać zmiany tych danych osobowych w sposób zapewniający anonimowość osób, których dane te dotyczą.
7. W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Rozporządzenia RODO, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 10

Obowiązek informacyjny

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

§ 11

Prawa osób, których dotyczą dane osobowe

1. Osobom, których dane przetwarza się w zbiorze danych osobowych Akademii, przysługuje:
   a. prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych,
   b. prawo do żądania sprostowania (poprawienia) danych,
   c. prawo do żądania usunięcia danych osobowych (tzw. „prawo do bycia zapomnianym"),
   d. prawo do żądania ograniczenia przetwarzania danych osobowych,
   e. prawo do przenoszenia danych do Pani/ Pana lub do innego administratora danych,
   f. prawo do sprzeciwu wobec przetwarzania danych osobowych.
2. Inspektor danych osobowych opiniuje zasadność żądania i wraz z komórką organizacyjną w której przetwarzane są dane osobowe udziela odpowiedzi.

§ 12

Czynności przetwarzania i zbiory danych

1. W Akademii prowadzi się rejestr czynności przetwarzania danych osobowych i ewentualnie rejestr kategorii przetwarzania danych. Rejestry są aktualizowane przez Inspektora danych osobowych na podstawie własnych ustaleń oraz informacji uzyskanych od pracowników. Czynności przetwarzania mogą być grupowane w ramach zbiorów danych

osobowych wedle kryterium komórki przetwarzającej dane osobowe lub innego przyjętego w Akademii takiego jak kategoria osób lub cel przetwarzania danych.

2. Kierownicy komórek organizacyjnych Akademii lub osoby zatrudnione na samodzielnych stanowiskach, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia Inspektorowi danych osobowych informacji na temat:
   a) planowanego założenia nowych czynności przetwarzania i zbiorów danych osobowych,
   b) wnoszonych zmian do istniejących czynności przetwarzania i zbiorów danych osobowych.

§ 13

Ocena ryzyka

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

§ 14

Zabezpieczenia fizyczne, informatyczne i organizacyjne

1. Dostęp do pomieszczeń Akademii, w których przetwarzane są dane osobowe, podlega kontroli.
2. Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania lub zdania klucza.
3. Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie osobom upoważnionym.
4. Akademia, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
5. W Akademii stosowane są następujące dodatkowe środki techniczne i organizacyjne oraz przedsięwzięcia niezbędne do zapewnienia poufności, integralności przetwarzanych danych osobowych:
   a) środki ochrony fizycznej - urządzenia służące do przetwarzania danych osobowych znajdują się wyłącznie w pomieszczeniach zabezpieczonych zamkami,
   b) dostęp do pomieszczenia, w którym znajdują się urządzenia serwerowe ma tylko Administrator Danych Osobowych oraz Administrator Systemu Informatycznego, a w uzasadnionych przypadkach Inspektor ochrony danych,
   c) zbędne dokumenty papierowe zawierające dane osobowe mogą być niszczone wyłącznie w niszczarkach,
   d) urządzenia na których znajdują się bazy danych osobowych – serwery powinny być podłączone do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania,
   e) sieć lokalna podłączona jest do internetu poprzez router spełniający jednocześnie

funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną,

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

g) okresowo są wykonywane kopie zapasowe na nośniki zewnętrzne.

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

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

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

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

d) hasła są konstruowane w następujący sposób:

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) zobowiązana jest do zachowania hasła w poufności, nawet po utracie przez nie ważności i odpowiada za wszystkie działania wykonane z wykorzystaniem osobistego loginu i hasła.

e) zabronione jest przekazywanie haseł innym osobom oraz zapisywanie haseł w sposób jawny (np. na karteczkach samoprzylepnych, w komputerze); pierwsze hasło nadane przez administratora danych osobowych jest przekazywane użytkownikowi systemu w sposób uniemożliwiający zapoznanie się z nim osób postronnych i niezwłocznie przez niego zmieniane.

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

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

g) W przypadku likwidacji nośników informatycznych zawierających Dane Osobowe lub kopie zapasowe Systemów Informatycznych służących do przetwarzania Danych Osobowych należy przed ich likwidacją usunąć Dane Osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

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

i) Nośniki informacji zawierające Dane Osobowe oraz Kopie Zapasowe, a także wydruki i inne dokumenty zawierające Dane Osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania Danych Osobowych,

w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

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

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

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

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

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

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

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

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

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

§ 15

Postanowienia końcowe

1. Integralną częścią niniejszego regulaminu są następujące załączniki:
   1) wzór formularza upoważnienia/odwołania upoważnienia do przetwarzania danych osobowych,
   2) wzór oświadczenia pracownika (w tym osoby zatrudnionej na innej niż umowa o pracę podstawie prawnej) przetwarzającego dane osobowe,
   3) wzór klauzuli informacyjnej dla pracownika/osoby przetwarzającej dane osobowe;
   4) lista dokumentów przyjętych w jednostce.

2. W celu wykonania niniejszej Polityki ochrony danych osobowych wydawane będą dodatkowe dokumenty takie jak procedury, instrukcje czy zarządzenia. W tym celu mogą być prowadzone także listy i wykazy (każdorazowo umieszczane na liście o której mowa w ust. 1 pkt. 4 powyżej).
3. W celu wykonania niniejszej Polityki ochrony danych osobowych prowadzone będą w osobnych dokumentach rejestry czynności przetwarzania danych osobowych w jednostce.