UNIWERSYTET ARTYSTYCZNY
w Poznaniu
SEKRETARIAT REKTORA
Aleje Marcinkowskiego 29
skr. poczt. 191, 60-967 Poznań 9
tel. 61 852-16-31, 852-23-21, fax 61 852-80-91

Zarządzenie nr 98/2017/2018
Rektora Uniwersytetu Artystycznego w Poznaniu
z dnia 19 lipca 2018 r.

---

w sprawie ochrony danych osobowych

Na podstawie art. 66 ust. 1 i 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz.U.2016.1842 t.j. z późn. zm.) oraz § 34 ust.3 Statutu Uniwersytetu Artystycznego w Poznaniu, niniejszym zarządzam, co następuje:

§ 1

1. W dniu 25 maja 2018 roku weszły w życie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.119/1), (dalej jako RODO).
2. W celu dostosowania działalności Uniwersytetu Artystycznego w Poznaniu (dalej jako UAP) do wymogów RODO, ochrona danych osobowych odbywa się na zasadach opisanych w:
   a) Regulaminie Ochrony Danych Osobowych w Uniwersytecie Artystycznym w Poznaniu, stanowiącym załącznik nr 1 do niniejszego zarządzenia,
   b) Polityce Ochrony Danych Osobowych w Uniwersytecie Artystycznym w Poznaniu, stanowiącej załącznik nr 2 do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem wydania z mocą obowiązującą od dnia 25 maja 2018 r.

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
w Poznaniu
prof. dr hab. Wojciech Nowak prof. zw. UAP

Załącznik nr 1 do Zarządzenia nr 98/2017/2018 Rektora UAP z dnia 19 lipca 2018r.

Regulamin Ochrony Danych Osobowych

w

Uniwersytecie Artystycznym w Poznaniu

Spis treści:

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU KOMPUTEROWEGO

W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu komputerowego zobowiązany jest do jego zabezpieczenia przed: zniszczeniem, uszkodzeniem lub kradzieżą. Stwierdzone zniszczenie, uszkodzenie lub kradzież użytkownik ma obowiązek zgłaszać bezpośredniemu przełożonemu.

1. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych osobowych wyświetlanych na monitorach komputerowych.
2. Przed czasowym opuszczeniem stanowiska pracy użytkownik zobowiązany jest zablokować stanowisko komputerowe za pomocą kombinacji klawiszy *WINDOWS + L*.
3. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub mają dostępem do danych osobowych przez Internet zobowiązani są do stosowania personalnych, szyfrowanych połączeń VPN lub Citrix.

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik przetwarzający dane osobowe w systemie informatycznym musi posiadać swój własny indywidualny identyfikator (login) do logowania w domenie Uczelni oraz służbowy adres e-mail (domena uap.edu.pl)
2. Tworzenie kont użytkowników wraz z uprawnieniami odbywa się na podstawie karty obiegowej. Konto tworzy administrator danego systemu informatycznego a uprawnienia do danego modułu ustala z bezpośrednim przełożonym użytkownika.
3. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
4. Zabroniona jest praca kilku użytkowników na wspólnym koncie.
5. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programów nie zweryfikowanych przez Dział IT. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego, w którym przetwarzane są dane osobowe a następnie wyłączyć komputer,
   b) zabezpieczyć stanowisko pracy, w szczególności wydruki oraz nośniki, na których znajdują się dane osobowe.

3 POLITYKA HASEŁ

1. Hasła powinny składać się z minimum ośmiu znaków.
2. Hasła powinny zawierać duże litery, małe litery, cyfry i znaki specjalne.
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy: zapisywać haseł na kartkach i w notesach, naklejać na monitorze komputera, trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła należy to niezwłocznie zgłosić do Działu IT osobiście, telefonicznie lub na adres wsparcieit@uap.edu.pl w celu zablokowania nieautoryzowanego dostępu.
6. Systemy informatyczne wymuszają zmiany haseł co 30 dni.
7. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
8. Niedopuszczalne jest stosowanie tego samego hasła jako zabezpieczenia w dostępie do różnych systemów informatycznych przetwarzających dane osobowe.
9. Nie zaleca się stosowania haseł, w których jeden z członów stanowi imię, nazwisko lub numer miesiąca lub inny możliwy do odgadnięcia klucz.
10. Ze względu na konieczność zachowania bezpieczeństwa danych, zmiana hasła przez Dział IT wymaga osobistego kontaktu ze strony użytkownika. Do weryfikacji tożsamości użytkownika wymagany jest do wglądu dowód osobisty lub inny dokument potwierdzający tożsamość np.: paszport.

4 ZABEZPIECZENIE DOKUMENTÓW I NOŚNIKÓW Z DANYMI OSOBOWYMI

1. Pracownicy są zobowiązani do stosowania tzw. *„Polityki czystego biurka"*. Polega ona na zabezpieczaniu dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub do utylizacji ich w specjalnych pojemnikach. Zasady te opisuje punkt w rozdziale „dobre praktyki".
3. Wycofane z użytku lub uszkodzone nośniki elektroniczne (dyski, pendrive, dyski przenośne, karty pamięci itp.) zawierające dane osobowe należy przekazywać do Działu IT. Zostaną one zniszczone w bezpieczny sposób uniemożliwiający ich odczyt.
4. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np.: na korytarzach, na drukarkach, w pomieszczeniach ogólnodostępnych.
5. Zabrania się wyrzucania niezniszczonych lub przedartych dokumentów z danymi osobowymi na śmietnik.

Zasady wynoszenia nośników z danymi poza Uczelnię

1. Użytkownicy nie mogą wynosić na zewnątrz wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody bezpośredniego przełożonego.
2. Dane osobowe wynoszone poza Uczelnię winny być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie i przesyłanie dokumentacji papierowej.
4. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
5. W sytuacji przesyłania nośników z danymi osobowymi poza Uczelnię można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą np.: wysłane SMS-em na numer komórkowy adresata,
    c. stosować bezpieczne koperty,
    d. przesyłkę należy przesyłać za potwierdzeniem odbioru.

5 DOSTĘP DO POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE – POLITYKA KLUCZY

1. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe możliwy jest wyłącznie osobom posiadającym upoważnienie do pobierania kluczy. Wykaz opracowuje Inspektor Ochrony Danych a zatwierdza Kanclerz. Zatwierdzony wykaz przekazywany jest do właściwej portierni w zależności od lokalizacji pomieszczeń.
2. Sprzątanie pomieszczeń, w których przetwarzane są dane osobowe powinno odbywać się pod nadzorem osób będących użytkownikami danego pomieszczenia.

6 ZASADY KORZYSTANIA Z INTERNETU PODCZAS PRZETWARZANIA DANYCH OSOBOWYCH

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się instalowania oraz uruchamia nielegalnych programów (programów do których Uczelnia nie posiada praw lub licencji).
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. W opcjach przeglądarki internetowej nie należy włączać autouzupełniania formularzy i zapamiętywania haseł.
6. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np.: na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej, firmy kurierskiej itp.) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Tego typu sytuacje należy zgłaszać niezwłocznie do Obsługi informatycznej..

7. Dział IT nigdy nie wysyła informacji z prośbą o podanie loginów/haseł do jakichkolwiek systemów teleinformatycznych.

7 Zasady korzystania z poczty elektronicznej przy przesyłaniu danych osobowych

1. Przesyłanie danych osobowych z użyciem poczty elektronicznej poza Uczelnię może odbywać się tylko przez osoby do tego upoważnione, wyznaczone przez Kierownika danej jednostki organizacyjnej.
2. W przypadku przesyłania danych osobowych należy wysyłać pliki zaszyfrowane lub spakowane. Pliki powinny być zahasłowane, gdzie hasło powinno być przekazane do odbiorcy telefonicznie lub przez SMS.
3. Przy zabezpieczeniu plików hasłem obowiązuje minimum 8 znaków: duże i małe litery, cyfry lub znaki specjalne.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem odznaczył w wiadomości żądanie potwierdzenia przeczytania wiadomości.

8 Ochrona antywirusowa

1. Komputery, na których przetwarza się dane osobowe mają zainstalowany wielostanowiskowy, licencjonowany program antywirusowy.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany, zainstaluj program antywirusowy", użytkownik zobowiązany jest do poinformowania o tym fakcie Dział IT.

9 Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia bezpośredniego przełożonego lub Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do takich należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka lub ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, użytkowników, utrata / zagubienie danych),
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    b. dokumentacja jest niszczona bez użycia niszczarki,
    c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,

d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
e. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez zgody bezpośredniego przełożonego,
g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
h. telefoniczne próby wyłudzenia danych osobowych,
i. kradzież, zagubienie komputerów lub nośników zawierających dane osobowe,
j. maile zachęcające do ujawnienia identyfikatora lub hasła,
k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
l. hasła do systemów przyklejone są w pobliżu komputera.

10 Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych zadaniach określonych przez Kierownika danej jednostki organizacyjnej,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań służbowych,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

11 Postępowanie dyscyplinarne

1. Przypadki zaniechania obowiązków wynikających z niniejszego regulaminu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

12 Dobre Praktyki w świetle RODO

Zbieranie i przetwarzanie danych osobowych

Dane osobowe przetwarzane w Uczelni powinny być przedmiotem szczególnego traktowania i dbałości. Dotyczy to zarówno danych pracowników i studentów jak i pozostałych danych przetwarzanych w różnych procesach zachodzących w Uczelni. Stanowią one jedno z ważnych aktywów wykorzystywanych w pracy.

1. Przetwarzanie danych osobowych musi odbywać się na podstawie przepisów prawa lub w oparciu o wyraźną zgodę osoby, której dotyczą. Należy zawsze pamiętać aby przy pozyskiwaniu danych posiadać podstawę prawną ku temu lub posiadać zgodę osoby.
2. Zgodnie z wytycznymi RODO dane osobowe należy zbierać wyłącznie w zakresie niezbędnym do zrealizowania celu, do którego są zbierane. Należy unikać nadmiarowości, gdyż takie działanie stanowi naruszenie zasad oraz może naruszać prawa osoby, której to dotyczy.
3. Należy pamiętać o obowiązku informacyjnym wynikającym z nowych wytycznych; każda osoba, od której pozyskuje się dane osobowe zarówno drogą elektroniczną jak i papierową ma prawo do pełnej informacji co do celu, zakresu przetwarzania powierzonych danych osobowych.
4. Po ustaniu celu przetwarzania danych osobowych, do którego zostały zebrane, danych tych nie należy używać do innych celów niż wskazane w klauzuli zgody.
5. W przypadku zgłoszenia sprzeciwu ze strony osoby, której dane dotyczą należy zaprzestać przetwarzania (jeżeli nie koliduje to z innymi regulacjami prawnymi).Należy również poinformować zainteresowanego o podjętych krokach.
6. W sytuacji, w której dane osobowe będą przekazywane podmiotowi trzeciemu, należy dopilnować aby zawarta została pisemna umowa powierzenia.(nie dotyczy to sytuacji, w których dane osobowe przekazywane są na podstawie regulacji prawnych do podmiotów uprawnionych np. ZUS, Urząd Skarbowy itp.)
7. Zaleca się regularne przeglądy dokumentacji, plików na komputerze pod kątem ich aktualności i celowości przetwarzania. Nośniki z danymi osobowymi, których cel przetwarzania został osiągnięty należy niszczyć w sposób trwały. Dotyczy to zwłaszcza baz danych, które były tworzone do celów organizacji jednorazowych imprez np. warsztatów, spotkań, plenerów itp.
8. Wszelkie wątpliwości należy konsultować z Inspektorem Ochrony Danych

   dostępnym pod adresem iod@uap.edu.pl

Komunikacja marketingowa

1. W przypadku organizowania imprez niecyklicznych, kursów, wydarzeń itp. z użyciem formularza rejestracyjnego zamieszczonego na stronie www Uczelni należy umieścić „checkbox" z obligatoryjną zgodą na przetwarzanie danych osobowych przez osobę chcącą wziąć udział w imprezie. Dane pozyskane w ten sposób muszą być adekwatne do celu. Należy unikać nadmiarowości gromadzonych informacji. Należy również dopełnić obowiązek informacyjny wobec uczestników ww. imprez.

Strona www podczas świąt oraz innych dłuższych przerw w funkcjonowaniu Uczelni

W celu zminimalizowania skutków ewentualnego ataku hackerskiego na stronę www Uczelni zaleca się przełączenie strony w tryb tylko do odczytu.

Niszczenie dokumentów i wydruków z danymi osobowymi

1. Wszelkie wydruki zawierające dane osobowe lub inne dane podlegające ochronie, po upływie ich przydatności powinny być zniszczone w sposób trwały i nieodwracalny z użyciem niszczarki.
2. W przypadku braku niszczarki w jednostce organizacyjnej należy skontaktować się z Działem gospodarczym w celu przekazania wydruków do bezpiecznego zniszczenia.
3. Przekazanie wydruków do bezpiecznego zniszczenia potwierdza się protokołem , którego wzór znajduje się poniżej.

Protokół

Przekazania wydruków do bezpiecznego zniszczenia

W dniu ..... przekazano do bezpiecznego zniszczenia następujące wydruki dostarczone przez .....(nazwa jednostki organizacyjnej)

L.p.	Nazwa	Ilość
1	(Np. wykaz osób będących na urlopach)	(Szacunkowa liczba wydruków)

4. Zgromadzone wydruki należy przekazać specjalistycznej firmie stosującej normę DIN 32757 (dla klasy III tajności) podczas procesu niszczenia. Po procesie zniszczenia dokumentów firma powinna wystawić certyfikat/zaświadczenie.

Zasady upubliczniania danych osobowych w procesie organizacji roku akademickiego.

1. Przy każdym przetwarzaniu danych osobowych w procesie organizacji roku akademickiego należy stosować zasadę adekwatności, zgodnie z którą powinno przetwarzać się tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne aby zrealizować określony cel.
2. Wszelkie informacje dotyczące studentów zaleca się publikować na podstawie ich numeru albumu. Dzięki temu studenci będą w stanie jednoznacznie zidentyfikować się na wszelkich listach lub zestawieniach, a jednocześnie nie będzie możliwości ich identyfikacji przez osoby trzecie.
3. W przypadku publikowania ocen z egzaminów zaleca się przyporządkowywać oceny do numeru albumu. Nie należy podawać wyników egzaminów telefonicznie ze względu na brak możliwości zweryfikowania komu udzielana jest informacja.
4. W przypadku kandydatów na studia nie posiadających jeszcze numeru albumu, zaleca się korzystać z kodu kandydata (nadanego przy rejestracji). Numer ten jest wystarczający do identyfikacji dla kandydata na studia, a przy tym nie pozwala na identyfikację kandydata przez osoby trzecie.
5. Powyższe zalecenia dotyczą upubliczniania informacji w formie tradycyjnej oraz elektronicznej.
6. Wszelkie wątpliwości należy konsultować z Inspektorem Ochrony Danych dostępnym pod adresem iod@uap.edu.pl

Załącznik nr 2 do Zarządzenia
nr 98/2017/2018 Rektora UAP
z dnia 19 lipca 2018r.

Polityka Ochrony Danych Osobowych
w
Uniwersytecie Artystycznym w Poznaniu

1 WSTĘP

Polityka Ochrony Danych Osobowych opisuje zasady ochrony danych osobowych stosowane przez Administratora Danych Osobowych w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Dokument stanowi jeden ze środków organizacyjnych, mających na celu zapewnienie przetwarzania danych osobowych zgodnie z powyższym Rozporządzeniem.

DEFINICJE

Administrator danych osobowych (ADO) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub więcej czynników specyficznych dla tej osoby.

Przetwarzanie danych osobowych - dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez ADO, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe.

Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu ADO.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez ADO w celu informowania i doradzania podmiotowi przetwarzającemu oraz pracownikom w zakresie obowiązującego prawa

o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2 Analiza Ryzyka

Za analizę ryzyka odpowiada ADO. Poniższą procedurę stosuje się do przeprowadzenia analizy ryzyka na potrzeby wykazania spełnienia wymagań RODO. W przypadku powołania Inspektora Ochrony Danych, ocena skutków musi być wykonana z jego współudziałem.

2.1 INWENTARYZACJA AKTYWÓW

W celu dokonania analizy ryzyka wymagane jest zinwentaryzowanie zbiorów danych osobowych oraz procesów, które należy zabezpieczyć. Dane te w postaci wykazu rejestru czynności przetwarzania dla procesów zostały wykazane w **załączniku nr 1** i stanowią jego integralną część.

2.2 OCENA PROPORCJONALNOŚCI

W ramach przeprowadzenia oceny proporcjonalności ADO przetwarzający dane osobowe zobowiązany jest do spełnienia wobec nich obowiązków prawnych. W szczególności należy wykazać, że:

1. dane te są przetwarzane legalnie,
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas,
4. wobec tych osób wykonano obowiązek informacyjny wraz ze wskazaniem ich praw oraz opracowano klauzule informacyjne dla powyższych osób,
5. istnieją umowy powierzenia z podmiotami przetwarzającymi. Wykaz podmiotów przetwarzających prowadzony jest zgodnie z **załącznikiem nr 2** – rejestr umów powierzenia.

2.3 2.3 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do możliwych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Przyjęto, że analiza ryzyka przeprowadzana jest dla procesów przetwarzania (np. dla procesu zatrudnienia).

2.3.1 Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Naruszenie (incydent) ochrony danych osobowych - to 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.
3. Zagrożenie - potencjalne naruszenie możliwe do zidentyfikowania.
4. Skutki - rezultaty lub straty wynikające z niepożądanego incydentu.
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie.

2.3.2 Wyznaczenie zagrożeń

1. ADO jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w danym procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio ustalonych aktywów.

2.3.3

2.3.4 Wyliczenie ryzyka dla zagrożeń

1. ADO określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.
2. Skalę prawdopodobieństwa przyjmuje się zakres od 1 do 3.
3. ADO określa Skutki (**S**) wystąpienia incydentów uwzględniając straty finansowe, straty wizerunkowe oraz skutki karne.
4. Skalę skutków przyjmuje się zakres od 1 do 3.
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S

2.3.5 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. ADO porównuje wyliczone ryzyka ze skalą i podejmuje decyzje lub działania
2. Proponowaną skalę ryzyka

Poziom ryzyka	Wartość
ryzyko akceptowalne	1-2
ryzyko akceptujemy lub obniżamy	3-6
ryzyka nie akceptujemy i obniżamy	9

2.3.6 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe.
2. Działania obniżające ryzyko, możliwe do zastosowania:
   a. Przeniesienie –przerzucenie ryzyka (np. ubezpieczenie od odpowiedzialności cywilnej)
   b. Unikanie – eliminacja działań powodujących ryzyko (np. coroczne kontrole instalacji wod.-kan.).
   c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. montaż czujników ppoż. w pomieszczeniach, w których przetwarza się dane osobowe).

3. Wykaz rozwiązań i procedur zawiera **załącznik nr 3** – wykaz zabezpieczeń.
4. Analiza ryzyka stanowi integralną część **załącznika nr 1**.
5. Ponowna analiza ryzyka przeprowadzana jest cyklicznie raz do roku oraz w przypadkach: zmian w procesie przetwarzania, powstania nowych procesów oraz zmian prawnych.
6. Inspektor Ochrony Danych zobowiązany jest do monitorowania wdrożonych zabezpieczeń.

3 UPOWAŻNIENIA

1. Inspektor Ochrony Danych (IOD) nadaje oraz anuluje upoważnienia do przetwarzania danych w zbiorach papierowych oraz systemach informatycznych.
2. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie. Upoważnienie do przetwarzania danych osobowych- **załącznik nr 4**
3. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Ewidencja ma charakter pomocniczy i stanowi **załącznik nr 5** - ewidencja osób upoważnionych.

4 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Instrukcja określa katalog incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych oraz pozostali pracownicy i podwykonawcy zobowiązani są do powiadamiania o incydencie bezpośredniego przełożonego lub Inspektora Ochrony Danych.
2. Do typowych sytuacji mogących prowadzić do incydentów należą np.:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu komputerowego,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np.: niestosowanie zasady „czystego biurka" i „czystego ekranu", upublicznienie hasła dostępu do systemu, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą np.:
    a. zdarzenia losowe takie jak: pożar obiektu lub pomieszczenia, zalanie wodą, zanik, zasilania lub przepięcie w sieci energetycznej, utrata łączności z siecią publiczną)
    b. zdarzenia losowe (awaria serwera, komputerów, błędy oprogramowania, pomyłki użytkowników, zagubienie nośnika z danymi),
    c. działania umyślne (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek danych ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów lub nośników z danymi).
4. W przypadku incydentu Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w ramach którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
    b. inicjuje działania mające na celu zmniejszenie strat w momencie zaistnienia incydentu,
    c. podejmuje działania na rzecz przywrócenia stanu pierwotnego po wystąpieniu incydentu,
    d. podejmuje działania korygujące mające na celu eliminację podobnych incydentów w przyszłości.
5. Inspektor Ochrony Danych dokumentuje naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania z wykorzystaniem dokumentu - formularz rejestracji incydentu - **załącznik nr 6**.
6. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób których dotyczą, Administrator Danych Osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza ten fakt organowi nadzorczemu.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie bezpiecznych zasad przetwarzania danych osobowych w Uniwersytecie Artystycznym w Poznaniu i stanowi osobny dokument - Regulamin Ochrony Danych Osobowych.

6 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być przeszkolona i zapoznana z zasadami ochrony danych osobowych w Uniwersytecie Artystycznym w Poznaniu
2. Za przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych.
3. Po szkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, **załącznik nr 8** - oświadczenie poufności.

7 PLAN CIĄGŁOŚCI DZIAŁANIA

Plan ciągłości działania stanowi **załącznik nr 9**.

8 INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Instrukcja zarządzania systemami informatycznymi stanowi integralną cześć Regulaminu Ochrony Danych Osobowych. Zapisy te znajdują się w punktach: 1,2,3,4. Ponadto materiały instruktażowe znajdują się na stronie www Uczelni oraz dostępne są u administratora danego systemu.

9 WYKAZ ZABEZPIECZEŃ

Wykaz zabezpieczeń stosowanych przez Administratora Danych osobowych stanowi **załącznik nr 3** - wykaz zabezpieczeń.

10 OBOWIĄZEK INFORMACYJNY

Administrator Danych dopełnia obowiązku informacyjnego wobec pracowników, studentów oraz innych osób, których dane posiada za pomocą komunikatów skierowanych do właściwych grup osób przekazywanych w sposób tradycyjny lub/i za pomocą poczty elektronicznej.

Załącznik nr 1 do Polityki Ochrony Danych Osobowych w UAP

Część I

Rejestr czynności przetwarzania dla: *nazwa procesu*
Administrator: Uniwersytet Artystyczny w Poznaniu
Utworzono:.....
Zmodyfikowano:.....
IOD .....

1	Opis kategorii osób, których dane dotyczą	
2	Cele przetwarzania	
3	Kategorie danych osobowych	
4	Współadministratorzy	
5	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	
6	Przekazanie do państwa trzeciego lub organizacji międzynarodowej	
7	Dokumentacja odpowiednich zabezpieczeń dla przekazania do państwa trzeciego lub organizacji międzynarodowej (wg Art. 49 ust. 1 akapit 2)	
8	Planowane terminy usunięcia poszczególnych kategorii danych	

9	Czynności przetwarzania	
10	Nazwa Systemu / Aplikacji	
11	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	
12	Czy dane zostały zebrane na podstawie zgody?	
13	Czy obowiązek informacyjny został spełniony wobec podmiotu danych?	
14	Podstawa prawna przechowywania danych	
15	Czy powierzono przetwarzanie danych innemu podmiotowi?	
16	Nazwa i dane kontaktowe podmiotu przetwarzającego	
17	Podstawa prawna przechowywania danych dla podmiotu przetwarzającego	

Część II

Wykaz zbiorów oraz osób biorących udział w procesie

Nazwa zbioru		
Wykaz osób przetwarzające dane	Imię i nazwisko	Data nadania upoważnienia do przetwarzania
Zakres przetwarzania		
Lokalizacja zbioru		
Forma zbioru		

Opracował:.....

Część III

Wykaz aktywów wykorzystywanych w procesie: *nazwa procesu*

AKTYWA	PODAKTYWA	Tak	Nie
1. Informacje			
	dane osobowe		
	dane dostępowe (loginy, hasła)		
	polityki bezpieczeństwa		
	umowy, dokumentacja papierowa		
	inne		
2. Programy i systemy operacyjne	**OPROGRAMOWANIE**		
	systemy operacyjne		
	oprogramowanie użytkowe (pakiety biurowe, oprogramowanie antywirusowe)		
	inne		
3. Infrastruktura IT	**SPRZĘT KOMPUTEROWY**		
	serwery (fizyczne i wirtualne)		
	stacje robocze (PC, laptopy)		
	Drukarki, skanery, kopiarki		
	inne		
	NOŚNIKI DANYCH		
	elektroniczne nośniki z danymi		
	inne		
	SIEĆ		
	usługi sieciowe (DNS, DHCP, VPN)		
	Okablowanie strukturalne		
	urządzenia aktywne		
	urządzenia pasywne		
	inne		
4. Infrastruktura dodatkowa	**Pomieszczenia i wyposażenie**		

	serwerownia		
	punkty dystrybucyjne sieci		
	pomieszczenia przetwarzania danych (elektronicznych i papierowych)		
	studzienki i kanały telekomunikacyjne		
	rozdzielnie elektryczne		
	kamery monitoringu		
	klimatyzator		
	zasilacze UPS		
	System ppoż. (w tym gaśnice)		
	System alarmowy		
	inne		

Część IV

Analiza ryzyka dla procesu: *nazwa procesu*

P-Prawdopodobieństwo incydentu (skala od 1 do 3), S-Skutki wystąpienia incydentu (skala od 1 do 3), R-Ryzyko wystąpienia incydentu (skala od 1 do 9), Formuła: R=P*S

Zagrożenie	Opis zagrożenia	P	S	R	Zabezpieczenie
Phishing, cybersquatting	- Mail z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub informowanie o próbie włamania na konto) do „podróbki" strony, np. bankowej i w rezultacie przejęcie hasła - Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www				**Procedura:** - Szkolenia personelu - Regulamin ODO **Zabezpieczenie:** - Systemy antywirusowy - blokada dostępu do określonych stron
Nakłanianie do wykonania czynności	-mail z dyspozycją przelewu wysłany do Kwestury lub Kancelarii -Fax lub mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur				**Procedura:** - szkolenia personelu - regulamin ODO
Instalacja szkodliwego oprogramowania oraz działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink (mail z fakturą do opłacenia, mail z DHL o przesyłce, mail z rzekomym pismem urzędowym). W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci Działające szkodliwe oprogramowanie może wywołać różnorodne skutki: - Przejęcie konta pocztowego do wysyłki spamu - Użycie przejętych komputerów do np.kopania kryptowalut - Użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu do systemów i plików				**Procedura:** - szkolenia personelu - regulamin ODO **Zabezpieczenie:** - systemy antywirusowy i antyspamowy - blokada dostępu do określonych stron

	- Użycie przejętych komputerów do uzyskania pełnego dostępu do wewnętrznej sieci i kopiowania danych i baz danych (kradzież) Szkodliwe oprogramowanie: Wirusy i trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika. Backdoory - Instalują się z maili lub z hiperlinków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza. Keyloggery - Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi. Exploity / exploitpaki - Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.				
Podrzucone nośniki danych	Atakujący pozostawia w pomieszczeniu specjalnie przygotowany nośnik z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).				**Procedura:** - Szkolenia personelu - Regulamin ODO **Zabezpieczenie:** - Blokada portów USB na stacjach roboczych - Dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive
Ataki telefoniczne	-Intruz podający się za „naszego pracownika" prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego				**Procedura:** - Szkolenia personelu - Regulamin ODO
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force) : - do serwera z aplikacjami - do aplikacji www (np. do Wordpress-a) - do serwera poczty - do systemu Windows na stacjach roboczych				**Procedura:** - Szkolenia personelu - Automatyczne, okresowe wymuszanie zmiany haseł o określonej złożoności
Słabe hasła	- Ujawnianie haseł - Nieprawidłowe przechowywanie (karteczki, pliki) - Stosowanie domyślnych haseł producenta				**Procedura:** - Szkolenia personelu - Automatyczne, okresowe wymuszanie zmiany haseł o określonej Złożoności

	- Stosowanie słownikowych lub popularnych haseł, np.: qwerty, 12345678 - Stosowanie jednego hasła do kilku systemów				**Zabezpieczenia:** - hasło zawiera duże, małe litery cyfry lub znaki specjalne - częstotliwość zmiany hasła – 30 dni - mechanizm wymuszenia zmiany hasła
Atak ransomeware	Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Odszyfrowanie wymaga zapłaty określonej sumy pieniędzy.				**Procedura:** - Szkolenia personelu - Regulamin ODO **Zabezpieczenia:** - Systemy antywirusowy i antyspamowy - Kopie bezpieczeństwa kluczowych danych zabezpieczone przed szyfrowaniem przez ransomeware (np.utrzymywanie obrazów-kopii wirtualnych serwerów) - blokada dostępu do określonych stron
Eskalacja uprawnień	- Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych - Przejęcie uprawnień administratora				**Procedura:** - Nadawania uprawnień do systemów przetwarzających dane osobowe w porozumieniu z bezpośrednim przełożonym danej jednostki organizacyjnej **Zabezpieczenia:** -Okresowe przeglądy logów i uprawnień - Monitorowanie logowania na konta administracyjne
Atak DOS / DDOS	Atak dotyczy głownie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapełnienia dysku.				**Procedura:** - Okresowy przegląd stron internetowych pod kątem aktualizacji **Zabezpieczenia:** - Firewall - Mechanizm captcha (kod z obrazka do przepisania w formularzu)
Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do: - Pomieszczeń biurowych - Archiwum - Serwerowni Może skutkować: - dostępem do danych w wersji papierowej - dostępem do plików - kradzieżą komputerów lub/i nosników				**Procedury:** - kontrola dostępu **Zabezpieczenia:** - kontrola wydawania kluczy - portiernia - praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych - rozmieszczenie komputerów i drukarek ograniczające dostęp osób nieupoważnionych - zabezpieczenie dostępu do pomieszczeń (drzwi zamykane na klucz) - zabezpieczenie dostępu do serwerowni (drzwi zamykane na klucz)

					oraz brak oznaczenia miejsca - zabezpieczenie dokumentacji w pomieszczeniach (zamknięte niemetalowe szafy) - system alarmowy - ochrona fizyczna obiektu - monitoring wizyjny w obrębie obiektu i otoczeniu
Kradzież lub zagubienie sprzętu i nośników	Kradzież lub zagubienie: - laptopów - pendrive - dysków zewnętrznych				**Procedury:** - Regulamin użytkowania komputerów przenośnych **Zabezpieczenia:** - Szyfrowanie laptopów - Stosowanie szyfrowanych nośników przenośnych
Udostępnianie danych osobom nieupoważnionym przez sieć publiczną	- dostęp do danych osobowych poprzez stronę www bez logowania się - udostępnianie plików zaindeksowanych przez roboty na skutek braku komend chroniących katalogi webowe przez taką indeksacją				**Procedura** - Regulamin ODO **Zabezpieczenia** - Uwierzytelnianie dostępu do zasobów - Blokada robotów - aktualizacje oprogramowania stron www
Awarie i uszkodzenia elementów IT	Awarie: - dysków - stacji roboczych - urządzeń sieciowych/routerów - drukarek				**Zabezpieczenia:** - redundancja serwera - macierz RAID - plan ciągłości działania - sukcesywne wycofywanie z eksploatacji sprzętów starszych niż 5 lat
Błąd lub awaria oprogramowania	Awarie: - programu kadrowo-płacowego - poczty - aplikacji www (np. wordpressa)				**Zabezpieczenia:** - Wirtualizacja serwera obsługującego program kadrowo-płacowy - aktualizacje oprogramowania stron www oraz serwera pocztowego
Pożar	- Pożar w pomieszczeniu lub obiekcie - Pożar serwerowni				**Procedury:** - Zabezpieczenia techniczne **Zabezpieczenia:** - gaśnice w pomieszczeniach lub ich najbliższym sąsiedztwie - system PPOŻ
Zalanie	- Zalanie serwerowni - Zalanie pomieszczeń - Zalanie archiwum Np.: powódź, zalanie z pękniętych rur wod.-kan., CO)				**Procedury:** Zabezpieczenia techniczne **Zabezpieczenia:** - składowanie dokumentacji papierowej na podwyższeniu - digitalizacja najważniejszych dokumentów archiwalnych
Przegrzanie	wysoka temperatura w serwerowni				**Procedury:** - Zabezpieczenia techniczne **Zabezpieczenia:** - klimatyzacja w serwerowni

Awaria zasilania	- przerwy w dostawie zasilania - skoki napięcia - przepięcia w sieci				**Procedury:** - Zabezpieczenia techniczne **Zabezpieczenia:** - UPS podtrzymujący zasilanie serwera - UPS na kluczowych elementów systemu IT - UPS centralny podtrzymujący zasilanie w segmencie B oraz w nowym budynku dydaktycznym
Nieuprawniona modyfikacja lub usunięcie danych osobowych	- niezamierzone lub pomyłkowe zmodyfikowanie lub usunięcie danych - sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji				**Procedury:** Instrukcja zarządzania systemem informatycznym **Zabezpieczenia:** - Rozliczalność operacji - systemy zapisują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych itp - każdy użytkownik systemu posiada swój indywidualny login
Nieprawidłowe postępowanie przy niszczeniu nośników z danymi	- wyrzucenie uszkodzonych nośników bez ich zniszczenia - wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym - wyrzucenie niezniszczonych płyt CD/DVD i innych nośników				**Procedury:** - regulamin postępowania z nośnikami danych **Zabezpieczenia:** - niszczarki o podwyższonym standardzie - niszczenie/czyszczenie nośników przed utylizacją - firma niszcząca dokumenty
Nieprzestrzeganie procedur	- świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka				**Procedury:** - Szkolenia personelu - Regulamin ODO - postępowanie dyscyplinarne
brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy przy powierzaniu przetwarzania danych osobowych				**Zabezpieczenia:** - Umowa powierzenia - Pisemne upoważnienia dla podmiotu współpracującego z jasnymi warunkami bezpiecznej pracy z danymi powierzonymi
Awaria łącza ISP	Krytyczne dla usług wymagających „Internetu"				**Zabezpieczenie:** - Redundancja łączy

Załącznik nr 2 do Polityki Ochrony Danych Osobowych w UAP

Rejestr umów powierzenia

Lp	Nazwa Administratora	Kategoria osób których dane dotyczą	Numer umowy	Zakres czynności przetwarzania

REKTOR
UNIWERSYTETU ARCHEOLOGII
W Pozn
prof. dr hab. W

Załącznik nr 3 do Polityki Ochrony Danych Osobowych w UAP

Wykaz zabezpieczeń

Zabezpieczenie	Opis zabezpieczenia	Rodzaj zabezpieczenia
Regulamin ODO dla pracowników	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami wewnętrznymi dotyczącymi ochrony danych osobowych	Zabezpieczenia organizacyjne
Szkolenia pracowników	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami ogólnymi dotyczącymi ochrony danych osobowych	Zabezpieczenia organizacyjne
Kontrole wewnętrzne	Przeprowadzane są wewnętrzne kontrole zgodności przetwarzania danych osobowych z regulacjami wewnętrznymi	Zabezpieczenia organizacyjne
kontrola dostępu	Kontrolowane wydawanie kluczy od pomieszczeń, w których przetwarza się dane osobowe	Zabezpieczenia fizyczne
Dostęp do pomieszczeń i sprzętu	ograniczenie dostępu do pomieszczeń osobom nieupoważnionym, chyba że w obecności osoby upoważnionej	Zabezpieczenia fizyczne
Zabezpieczenie pomieszczeń	drzwi zamykane na klucz	Zabezpieczenia fizyczne
Zabezpieczenie serwerowni	drzwi zamykane na klucz, brak oznaczenia przeznaczenia pomieszczenia	Zabezpieczenia fizyczne
Zabezpieczenie dokumentacji	zamknięte niemetalowe szafy, zamknięte metalowe szafy	Zabezpieczenia fizyczne
Systemy alarmowe	system alarmowy	Zabezpieczenia fizyczne
Ochrona fizyczna obiektu	firma ochroniarska	Zabezpieczenia fizyczne
System ppoż.	system w obiekcie, gaśnice	Zabezpieczenia techniczne
Monitoring wizyjny	monitoring wizyjny w obrębie obiektu i otoczeniu	Zabezpieczenia techniczne
Klimatyzacja	klimatyzacja w serwerowni	Zabezpieczenia techniczne
UPS	Zastosowano UPS-y podtrzymujące zasilanie serwerów, oraz na kluczowych elementach infrastruktury IT	Zabezpieczenia techniczne
Systemy antywirusowy	Zastosowano systemy antywirusowe na stacjach roboczych	Zabezpieczenia informatyczne
System antyspamowy	Zastosowano system antyspamowy na serwerze pocztowym	Zabezpieczenia informatyczne
Firewall	Zastosowano firewall do ochrony dostępu do sieci komputerowej	Zabezpieczenia informatyczne
UTM	Zastosowano UTM do ochrony dostępu do sieci komputerowej	Zabezpieczenia informatyczne
Szyfrowanie transmisji	Zastosowano szyfrowanie połączeń zdalnych (VPN)	Zabezpieczenia informatyczne
Redundancja	Zastosowano macierze dyskowe	Zabezpieczenia informatyczne
Rozliczalność operacji	aplikacje posiadają mechanizmy odnotowywania wykonywania operacji na danych osobowych.	Zabezpieczenia informatyczne
Personalizacja użytkowników	użytkownik dokonujący zmian, każdy użytkownik posiada swój indywidualny login	Zabezpieczenia informatyczne
Postępowanie z nośnikami	Wdrożono procedurę postępowania z nośnikami wycofanymi z użycia	Zabezpieczenia organizacyjne
Zarządzanie uprawnieniami	Zastosowano zasadę minimalizacja uprawnień	Zabezpieczenia informatyczne
Uwierzytelnianie użytkowników	Zastosowano wymuszanie zmiany hasła, ustalono długość i składnię hasła,	Zabezpieczenia informatyczne

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
w Poznaniu
prof. dr hab. Wojciech [illegible] prof. zw. UAP

A.

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA*

do przetwarzania danych osobowych
w systemach informatycznych lub w zbiorach w wersji papierowej

Z dniem.....upoważniam/anuluję upoważnienie*

Panią/Pani/Pana*.....

zatrudnionej/zatrudnionego w ..... do przetwarzania danych osobowych

w procesie.....do zbioru.....

w zakresie: (WG) wglądu, (W) wprowadzania, (M) modyfikacji, (U) usuwania, (A) archiwizacji, (U) udostępniania innym podmiotom, oraz koniecznym do wykonywania obowiązków pracowniczych

Upoważnienie dotyczy również przetwarzania danych osobowych w systemie informatycznym:

.....

B.

.....

Poznań, dnia..... (pieczątka i podpis IOD)

Ewidencja użytkownika w systemie informatycznym

Nazwa systemu.....

Identyfikator użytkownika.....

Zakres uprawnień użytkownika (dostęp do modułów).....

Data zarejestrowania w systemie:.....

Data wyrejestrowania użytkownika:.....

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
W POZNANIU
prof. dr hab. Wojciech Nora prof. zw. UAP

*niepotrzebne skreślić

Ewidencja osób upoważnionych w procesie: *Nazwa procesu*

Lp	Imię i Nazwisko	Zakres upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia

Aktualizacja:.....

Opracował.....

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
w Poznaniu
prof. dr hab. Wojciech Kata prof. zw. UAP

Załącznik nr 6 do Polityki Ochrony Danych Osobowych w UAP

Formularz rejestracji incydentu

Data naruszenia/ incydentu	Opis i okoliczności naruszenia/ incydentu	Osoby objęte naruszeniem/ incydentem	Skutki naruszenia/ incydentu	Podjęte działania	Data rozpoczęcia wdrożenia działań

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
W POZNANIU
prof. dr hab. Wojciech Nowicki prof. zw. UAP

Załącznik nr 8 do Polityki Ochrony Danych Osobowych w UAP

Poznań, dnia.....

Imię i nazwisko:

.....

Jednostka organizacyjna:

.....

Oświadczenie o poufności

Oświadczam, iż zapoznano mnie z wewnętrznymi przepisami dotyczącymi ochrony danych osobowych obowiązujących w Uniwersytecie Artystycznym w Poznaniu.

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez ADO zadaniach,
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez ADO,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez ADO,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą,modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez ADO za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....

podpis oświadczającego

Załącznik nr 9 do Polityki Ochrony Danych Osobowych w UAP

Plan ciągłości działania

Dysponentami informacji w zakresie planu ciągłości działania są:

- Pracownicy Działu IT
- Inspektor Ochrony Danych

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
W POZNANIU
prof. dr hab. Wojciech Flora prof. zw. UAP