UNIWERSYTET ARTYSTYCZNY
im. Magdaleny Abakanowicz
w Poznaniu
Aleje Marcinkowskiego 29
skr. poczt. 191, 60-967 POZNAŃ 9
tel. 61 855 25 21, fax 61 852 80 91
NIP 778-11-28-625

Zarządzenie nr 63/2021/2022
Rektora Uniwersytetu Artystycznego im. Magdaleny Abakanowicz w Poznaniu
z dnia 12 kwietnia 2022 r.

---

w sprawie zmiany zarządzenia nr 98/2017/2018 Rektora Uniwersytetu Artystycznego w Poznaniu z dnia 19 lipca 2018 r. w sprawie ochrony danych osobowych

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym (Dz.U.2021.478 t.j. z późn. zm.) oraz § 23 ust. 1 Statutu Uniwersytetu Artystycznego im. Magdaleny Abakanowicz w Poznaniu, niniejszym zarządzam, co następuje:

§ 1

Zmienia się treść § 1 ust. 2 pkt a) zarządzenia nr 98/2017/2018 Rektora Uniwersytetu Artystycznego w Poznaniu z dnia 19 lipca 2018 r. w sprawie ochrony danych osobowych w ten sposób, że uchyla się dotychczasową treść dokument pn. „Regulamin Ochrony Danych Osobowych w Uniwersytecie Artystycznym w Poznaniu" i nadaje się mu nowe brzmienie, określone w treści załącznika do niniejszego zarządzenia.

§ 2

W pozostałym zakresie zarządzenie nr 98/2017/2018 Rektora Uniwersytetu Artystycznego w Poznaniu z dnia 19 lipca 2018 r. zmienione zarządzeniem nr 34/2021/2022 z dnia 14 stycznia 2022 r., w sprawie ochrony danych osobowych pozostaje bez zmian.

§ 3

Zarządzenie wchodzi w życie z dniem wydania.

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
im. Magdaleny Abakanowicz
w Poznaniu
prof. dr hab. Wojciech Hora

UNIWERSYTET ARTYSTYCZNY
im. Magdaleny Abakanowicz
w Poznaniu
Aleje Marcinkowskiego 29
skr. poczt. 191, 60-967 POZNAŃ 9
tel. 61 855 25 21, fax 61 852 80 91
NIP 778-11-28-625

Załącznik do zarządzenia nr 63/2021/2022 Rektora Uniwersytetu Artystycznego im. Magdaleny Abakanowicz w Poznaniu z dnia 12 kwietnia 2022 r.

Regulamin Ochrony Danych Osobowych

w

Uniwersytecie Artystycznym im. Magdaleny Abakanowicz

w Poznaniu

§ 1.

Zasady bezpiecznego użytkowania sprzętu komputerowego w procesach przetwarzania danych osobowych

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 (np.: studentom, pracownikom innych jednostek organizacyjnych, osobom postronnym) wglądu do danych osobowych wyświetlanych na monitorach komputerowych.
1. Przed czasowym opuszczeniem stanowiska pracy użytkownik zobowiązany jest zablokować stanowisko komputerowe za pomocą kombinacji klawiszy *WINDOWS*  *+ L*.
2. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub mają zdalny dostępem do danych osobowych zobowiązani są do stosowania personalnych, szyfrowanych połączeń VPN, RD (Remote Desktop) lub Citrix . W celu uzyskania zdalnego dostępu należy kontaktować się z Działem IT.

§ 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).
1. Tworzenie kont użytkowników wraz z uprawnieniami odbywa się na podstawie karty obiegowej. Konto tworzy pracownik Działu IT, który ustala z bezpośrednim przełożonym użytkownika uprawnienia do danego modułu.
2. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
3. Zabroniona jest praca kilku użytkowników na wspólnym koncie.
4. Zabroniona jest praca na komputerze innego użytkownika, który jest już na nim zalogowany.
5. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programów niezweryfikowanych przez Dział IT. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej , jak i wskazanych w formie odnośnika internetowego.
6. Po zakończeniu pracy użytkownik zobowiązany jest wylogować się z systemu informatycznego, w którym przetwarzane są dane osobowe, a następnie wyłączyć komputer.

§ 3.

Polityka haseł

1. Hasła powinny składać się z minimum ośmiu znaków.

1. Hasła powinny zawierać duże litery, małe litery, cyfry i znaki specjalne.

2. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
3. 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 widocznym miejscu.
4. 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.
5. Systemy informatyczne wymuszają zmiany haseł co 30 dni.
6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
7. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów informatycznych przetwarzających dane osobowe.
8. Nie zaleca się stosowania haseł, w których jeden z członów stanowi imię, nazwisko lub numer miesiąca lub inny możliwy do odgadnięcia klucz.
9. Ze względu na konieczność zachowania bezpieczeństwa danych, zmiana hasła przez Dział IT wymaga osobistego kontaktu ze strony użytkownika. Do weryfikacji tożsamości użytkownika może być wymagany do wglądu dowód osobisty lub inny dokument potwierdzający tożsamość.

§ 4.

Zabezpieczenie dokumentów i nośników z danymi osobowymi

1. Pracownicy są zobowiązani do stosowania „Polityki czystego biurka", która stanowi odrębny dokument stanowiący jedno z zabezpieczeń organizacyjnych przetwarzania danych osobowych w uczelni.
1. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków zawierających dane osobowe lub inne dane podlegające ochronie w niszczarkach. W przypadku większej ilości dokumenty/wydruki należy umieszczać w specjalnych pojemnikach. Szczegółowy opis postępowania w takich przypadkach zawiera „Instrukcja niszczenia wydruków oraz nośników elektronicznych zawierających dane osobowe". Instrukcja stanowi odrębny dokument, będący jednym z zabezpieczeń organizacyjnych przetwarzania danych osobowych w uczelni.
2. Wycofane z użytku lub uszkodzone nośniki elektroniczne (dyski, pendrive, dyski przenośne, karty pamięci itp.) zawierające dane osobowe lub inne dane podlegające ochronie należy przekazywać do Działu IT. Zostaną one zniszczone w bezpieczny sposób uniemożliwiający ich odczyt. Szczegółowy opis postępowania w takich przypadkach zawiera „Instrukcja niszczenia wydruków oraz nośników elektronicznych zawierających dane osobowe". Instrukcja stanowi odrębny dokument, będący jednym z zabezpieczeń organizacyjnych przetwarzania danych osobowych w uczelni.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np.: na korytarzach, na drukarkach, w pomieszczeniach ogólnodostępnych.
4. Zabrania się wyrzucania niezniszczonych lub przedartych dokumentów z danymi osobowymi na śmietnik.

§ 5.

Zasady wynoszenia nośników oraz zasady wysyłania drogą elektroniczną poza Uczelnię

1. Użytkownicy nie mogą wynosić na zewnątrz dokumentów zawierających dane osobowe oraz wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody bezpośredniego przełożonego.
1. Nośniki elektroniczne zawierające dane osobowe wynoszone poza Uczelnię muszą być

zaszyfrowane (szyfrowane dyski, zahasłowane pliki).

2. W przypadku wysyłania danych osobowych drogą elektroniczną (za pomocą poczty e-mail) należy stosować następujące zasady bezpieczeństwa:
   a. adresat powinien zostać powiadomiony o planowanym wysłaniu wiadomości,
   b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą np.: wysłane SMS-em na numer komórkowy adresata lub przekazane telefonicznie.
   c. Jako hasła można także użyć informacji, która powinna być znana tylko odbiorcy
   d. przy zabezpieczeniu plików hasłem obowiązuje minimum 8 znaków: duże i małe litery, cyfry lub znaki specjalne.
   e. zaleca się, aby użytkownik podczas przesyłania danych osobowych drogą elektroniczną odznaczył w wiadomości żądanie potwierdzenia przeczytania wiadomości.
   f. należy zwracać szczególną uwagę na poprawność adresu odbiorcy.

4. W przypadku dokumentów w formie papierowej zawierających dane osobowe (wydruki, skoroszyty, itp.) należy je zabezpieczyć przed zagubieniem lub kradzieżą oraz uniemożliwić wgląd w nie przez osoby niepowołane. Należy również dochować wszelkiej staranności podczas transportu.

5. W przypadku wysyłania dokumentów z danymi osobowymi drogą pocztową należy stosować bezpieczne koperty a przesyłkę należy nadawać za zwrotnym potwierdzeniem odbioru. Należy również zwracać szczególną uwagę na poprawność adresu odbiorcy.

§ 6.

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 uprawnienie do pobierania kluczy. Szczegółowy opis postępowania z kluczami zawiera odrębny dokument „Zasady postępowania z kluczami do pomieszczeń w budynkach" będący jednym z zabezpieczeń organizacyjnych przetwarzania danych osobowych w uczelni.

2. Sprzątanie pomieszczeń, w których przetwarzane są dane osobowe powinno odbywać się nadzorem osób będących użytkownikami danego pomieszczenia.

§ 7.

Zasady korzystania z Internetu podczas przetwarzania danych osobowych

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
1. Zabrania się instalowania oraz uruchamia nielegalnych programów (programów do których Uczelnia nie posiada praw lub licencji).
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
3. 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).
4. W opcjach przeglądarki internetowej nie należy włączać autouzupełniania formularzy zapamiętywania haseł.
5. 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 niezwłocznie zgłaszać pracownikom Działu IT.
6. Dział IT nigdy nie wysyła informacji z prośbą o podanie loginów/haseł do jakichkolwiek systemów teleinformatycznych.

§ 8.

Ochrona antywirusowa

1. Komputery, na których przetwarza się dane osobowe mają zainstalowany wielostanowiskowy, licencjonowany program antywirusowy.
1. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
2. W przypadku stwierdzenia np. spowolnionej pracy komputera lub pojawienia się nietypowych komunikatów systemowych, użytkownik zobowiązany jest do bezzwłocznego wylogowania się z systemu oraz zaprzestania pracy. Jednocześnie 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 oraz 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, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do incydentów wymagających powiadomienia, należą:

    d. zdarzenia losowe (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

    e. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, dysków, oprogramowania, użytkowników, utrata / zagubienie danych),

    f. 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:
    g. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    h. dokumentacja jest niszczona bez użycia niszczarki,
    i. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
    j. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
    k. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
    l. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez zgody bezpośredniego przełożonego,
    m. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
    n. telefoniczne próby wyłudzenia danych osobowych,
    o. kradzież, zagubienie komputerów lub nośników zawierających dane osobowe,
    p. maile zachęcające do ujawnienia identyfikatora lub hasła,
    q. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
    r. hasła do systemów przyklejone są w pobliżu komputera.

§ 10.

Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda osoba dopuszczona do przetwarzania danych osobowych zobowiązana jest 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. Zabronione jest przekazywanie bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
3. Zabronione jest przekazywanie lub ujawnianie 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

1. 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.

1. 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.

2. 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.

3. Po ustaniu celu przetwarzania danych osobowych, do którego zostały zebrane, danych tych nie należy używać do innych celów niż wskazane w klauzuli zgody.

4. 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.

5. 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.)
6. 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.
7. Wszelkie wątpliwości należy konsultować z Inspektorem Ochrony Danych

   dostępnym pod adresem iod@uap.edu.pl

2. 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.

3. 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.

REKTOR
UNIWERSYTETU ARTYSTYCZNEGO
im. Magdaleny Abakanowicz
w Poznaniu
prof. dr hab. Wojciech Hora