REGULAMIN OCHRONY DANYCH OSOBOWYCH W AKADEMII WYCHOWANIA FIZYCZNEGO IM. EUGENIUSZA PIASECKIEGO W POZNANIU

Akademia Wychowania Fizycznego
im. Eugeniusza Piaseckiego w Poznaniu

I. Zasady bezpiecznego użytkowania sprzętu komputerowego

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu komputerowego, zobowiązany jest on do jego zabezpieczenia przed: zniszczeniem, uszkodzeniem lub kradzieżą. Stwierdzone zniszczenie, uszkodzenie lub kradzież użytkownik ma obowiązek niezwłocznie zgłaszać bezpośredniemu przełożonemu.
2. Użytkownik jest zobowiązany uniemożliwić osobom niepowołanym (np. studentom, pracownikom innych jednostek organizacyjnych, osobom postronnym) dostęp do danych osobowych przechowywanych w pamięci komputera lub wyświetlanych na monitorze.
3. W przypadku chwilowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest do zablokowania komputera za pomocą kombinacji klawiszy Win+L.
4. Po zakończeniu pracy należy:
   1) wylogować się z systemu a następnie wyłączyć komputer,
   2) zabezpieczyć stanowisko pracy, w szczególności poprzez schowanie do zamykanych na klucz szaf wydruków oraz nośników, na których znajdują się dane osobowe.
5. Użytkownicy komputerów, którzy mają zdalny dostęp spoza Uczelni do systemów przetwarzających dane osobowe lub inne dane podlegające ochronie zobowiązani są do stosowania personalnych, szyfrowanych połączeń VPN.

II. Identyfikator (login)

1. Każdy użytkownik przetwarzający dane osobowe w systemie informatycznym musi posiadać swój własny, indywidualny identyfikator (login). Zabronione jest udostępnianie identyfikatora innym pracownikom lub osobom trzecim.
2. Tworzenie identyfikatorów odbywa się na podstawie karty obiegowej. Tworzony jest przez pracownika Sekcji IT, a uprawnienia do danego modułu ustalane są z bezpośrednim przełożonym użytkownika.
3. Identyfikator jest blokowany w momencie zakończenia stosunku pracy, na podstawie karty obiegowej.

III. Hasła

1. Hasła powinny:
   1) składać się z minimum ośmiu znaków,
   2) zawierać duże litery, małe litery, cyfry i znaki specjalne.
2. Hasła nie powinny być:
   1) ujawniane innym pracownikom lub osobom trzecim,
   2) zapisywane na kartkach.
3. W przypadku ujawnienia hasła, fakt ten należy niezwłocznie zgłosić do Sekcji IT w celu wygenerowania nowego.
4. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów informatycznych przetwarzających dane osobowe lub inne dane podlegające ochronie.

IV. Zabezpieczenie nośników z danymi osobowymi

1. Pracownicy zobowiązani są do:
   1) stosowania zasady czystego biurka, ekranu i czystej drukarki, stanowiącej załącznik do Polityki Ochrony Danych Osobowych.
   2) niszczenia nośników w niszczarkach lub do ich utylizacji. Opis znajduje się w dokumencie ”*Procedura niszczenia wydruków zawierających dane osobowe*”, stanowiącym załącznik do Polityki Ochrony Danych Osobowych.

2. Wycofane z użytku lub uszkodzone nośniki elektroniczne (dyski HDD lub SSD, pendrive, dyski przenośne, karty pamięci itp.) należy przekazywać do Sekcji IT. Zostaną one zniszczone w bezpieczny sposób, uniemożliwiający ich odczyt.
3. Zabrania się:
   1) wynoszenia na zewnątrz nośników bez zgody bezpośredniego przełożonego,
   2) pozostawiania nośników poza zabezpieczonymi pomieszczeniami, np.: na korytarzach, na drukarkach, w pomieszczeniach ogólnodostępnych,
   3) wyrzucania nośników na śmietnik.
4. Podczas wysyłania poza Uczelnię nośników należy stosować następujące zasady bezpieczeństwa:
   1) adresat powinien zostać powiadomiony o przesyłce,
   2) należy stosować bezpieczne koperty,
   3) przesyłkę należy nadawać za potwierdzeniem odbioru,
   4) w sytuacji przewozu przez pracownika Uczelni zobowiązany jest on do zabezpieczenia przesyłki przed zagubieniem lub kradzieżą,
   5) pliki znajdujące się na nośniku elektronicznym muszą być zabezpieczone hasłem.

V. Wysyłanie danych osobowych z wykorzystaniem poczty elektronicznej

1. Wysyłanie danych osobowych z użyciem poczty elektronicznej może odbywać się wyłącznie za zgodą i wiedzą bezpośredniego przełożonego.
2. Pliki powinny być zabezpieczone hasłem. Hasło powinno być przekazane odbiorcy telefonicznie lub za pomocą SMS.
3. Przy zabezpieczeniu plików hasłem obowiązuje minimum 8 znaków: duże i małe litery, cyfry lub znaki specjalne.
4. Należy zwracać szczególną uwagę na poprawność adresu odbiorcy. W przypadku kilku odbiorców tej samej wiadomości należy stosować funkcję UDW.
5. Zaleca się zaznaczyć w wiadomości żądanie potwierdzenia przeczytania wiadomości.

VI. Ochrona antywirusowa

1. Komputery, na których przetwarza się dane osobowe, wyposażone są w wielostanowiskowy, licencjonowany program antywirusowy.
2. Zabronione jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku podejrzenia zainfekowania systemu operacyjnego lub pojawienia się nietypowych komunikatów np.: „Twój system jest zainfekowany, zainstaluj program antywirusowy”, użytkownik zobowiązany jest do niezwłocznego poinformowania o tym fakcie Sekcję IT.
4. W przypadku stwierdzenia braku programu antywirusowego lub podejrzenia jego nieprawidłowego działania należy niezwłocznie powiadomić Sekcję IT.

VII. Postępowanie w przypadku naruszenia ochrony danych osobowych. Zgłaszanie incydentów.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia bezpośredniego przełożonego oraz Inspektora Ochrony Danych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub wystąpienia incydentu.

Sytuacje wymagające zgłoszenia:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
2) niewłaściwe zabezpieczenie sprzętu komputerowego przed kradzieżą i utratą danych osobowych,
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka lub ekranu, ochrony haseł, niezamykanie pomieszczeń/szaf/biurek),

4) umożliwianie dostępu osobom nieuprawnionym do danych osobowych przetwarzanych w systemach informatycznych lub w wersjach tradycyjnych,
5) zdarzenia losowe (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
6) zdarzenia wewnętrzne (np. awaria komputera, utrata/zagubienie danych),
7) incydenty (włamanie do systemu informatycznego lub pomieszczenia, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

Przykłady incydentów:

1) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
2) niszczenie dokumentacji bez użycia niszczarki lub wyrzucanie do śmietnika ,
3) fizyczna obecność osób zachowujących się podejrzanie w pomieszczeniach, w których przetwarzane są dane osobowe,
4) otwarte drzwi do pomieszczeń lub szaf, gdzie przetwarzane lub przechowywane są dane osobowe,
5) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
6) wynoszenie nośników w wersjach tradycyjnych lub elektronicznych na zewnątrz bez zgody bezpośredniego przełożonego,
7) udostępnienie w formie papierowej, elektronicznej lub ustnej danych osobowych osobom nieupoważnionym
8) telefoniczne próby wyłudzenia danych osobowych,
9) kradzież, zagubienie komputera lub nośnika zawierających dane osobowe,
10) wiadomości e-mail zachęcające do ujawnienia identyfikatora lub hasła,
11) pojawienie się wirusa komputerowego lub niestandardowa praca komputera,
12) hasła do systemów znajdujące się w widocznym miejscu.

VIII. Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

    1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych zadaniach, określonych przez kierownika danej jednostki organizacyjnej,
    2) zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań służbowych,
    3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem zadań powierzonych przez Pracodawcę,
    4) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
    5) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem oraz przetwarzaniem.

2. Zabronione jest:
    1) przekazywanie bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym, osobom, których tożsamości nie można zweryfikować lub takim, co do których istnieje podejrzenie, że podszywają się pod kogoś innego,
    2) przekazywanie lub ujawnianie danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

IX. Postępowanie dyscyplinarne

1. Przypadki zaniechania obowiązków, wynikających z niniejszego Regulaminu, potraktowane będą jako naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

X. Pozostałe zasady

1. Zbieranie i przetwarzanie danych osobowych

Dane osobowe przetwarzane w Uczelni powinny być przedmiotem szczególnego traktowania i dbałości. Dotyczy to zarówno danych pracowników, 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 zgodę osoby, której dotyczą. Zawsze należy pamiętać, aby przy pozyskiwaniu danych posiadać podstawę prawną lub posiadać zgodę podmiotu danych.
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; każda osoba, od której pozyskuje się dane osobowe, zarówno drogą elektroniczną jak i papierową, ma prawo do pełnej informacji co do celu oraz 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).
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 oraz plików 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 itp.

2. Komunikacja marketingowa

1) Wysyłanie wiadomości marketingowych powinno odbywać się wyłącznie na adresy e-mail, których użytkownicy wyrazili na to zgodę oraz zapoznali się z klauzulą informacyjną.
2) Komunikacja marketingowa na zlecenie innych jednostek organizacyjnych Uczelni na wskazane adresy e-mail jest możliwa po wcześniejszym uzyskaniu zgód osób, do których skierowana jest oferta.

3. Imprezy niecykliczne, konkursy, wydarzenia

W przypadku organizowania imprez niecyklicznych, kursów, wydarzeń itp. z użyciem formularzy rejestracyjnych zamieszczonych na stronie WWW Uczelni należy umieszczać „checkbox" zawierający obligatoryjną zgodę na przetwarzanie danych osobowych oraz treść obowiązku informacyjnego. Dane pozyskane w ten sposób muszą być adekwatne do celu. Należy unikać nadmiarowości gromadzonych informacji.

4. Strona WWW podczas przerw w funkcjonowaniu Uczelni oraz w przypadku ogłoszenia stanów CRP lub innych stanów nadzwyczajnych

W powyższych przypadkach, w celu zminimalizowania skutków ewentualnego ataku hackerskiego na stronę WWW Uczelni, zaleca się przełączenie strony w tryb „tylko do odczytu". Zminimalizuje to skutki ewentualnych nieautoryzowanych zmian treści oraz pojawienia się strat wizerunkowych.

5. Dane osobowe w badaniach statystycznych

W celu uniknięcia ewentualnego wycieku danych osobowych, w tym danych wrażliwych, zaleca się, aby materiał do badań statystycznych poddany został pseudonimizacji. Polega to na zmianie identyfikatorów, które są danymi osobowymi na takie, które nimi nie są. Na przykład imiona i nazwiska osób można zastąpić liczbami.

6. Niszczenie dokumentów i wydruków z danymi osobowymi

Postępowanie z dokumentami i wydrukami opisuje „Procedura niszczenia wydruków zawierających dane osobowe", stanowiąca załącznik do Polityki Ochrony Danych Osobowych.

7. 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 do zrealizowania celu.
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 lub zaliczeń należy przyporządkowywać oceny do numeru albumu. Nie należy podawać wyników telefonicznie ze względu na brak możliwości zweryfikowania komu udzielana jest informacja.