dokument wprowadzony Zarządzeniem nr 18/2022
Rektora Akademii z dnia 12 kwietnia 2022 r.

Polityka Ochrony Danych Osobowych w Akademii Wychowania Fizycznego im. Eugeniusza Piaseckiego w Poznaniu

1. Wstęp

Polityka Ochrony Danych Osobowych (dalej zwana też „Polityką") 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 użyte w dokumencie:

1) **Administrator danych osobowych (ADO)** - oznacza Akademię Wychowania Fizycznego im. Eugeniusza Piaseckiego w Poznaniu, który samodzielnie lub wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych.
2) **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).
3) **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.
4) **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.
5) **Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
6) **Anonimizacja** - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.
7) **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.
8) **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.
9) **Podmiot danych** - każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.
10) **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe.
11) **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu ADO.
12) **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 i organu nadzorczego.

13) **Pseudonimizacja -** oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami lub kodem), 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.
14) **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.
15) **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.
16) **Naruszenia ochrony danych** - jest 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 w Uczelni.
17) **Incydent bezpieczeństwa danych** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania Uczelni i zagrażają bezpieczeństwu przetwarzanych danych.

2. Analiza Ryzyka

Za analizę ryzyka odpowiada ADO. 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. Procedura opisana jest w odrębnym dokumencie - „Analiza ryzyka".

3. Rejestr Czynności Przetwarzania

Rejestr czynności przetwarzania prowadzony jest dla obszarów przetwarzania danych osobowych według wzoru stanowiącego **załącznik nr 1.**

4. 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).

5. Upoważnienia

1) Rektor lub osoba upoważniona przez Rektora nadają upoważnienia i polecenia przetwarzania danych osobowych.
2) Upoważnienie i polecenie przetwarzania danych osobowych stanowi **załącznik nr 3.** W przypadku dostępu do szczególnych kategorii danych (np.: w zakresie stanu zdrowia) upoważnienie i polecenie przetwarzania danych osobowych wydawane jest według wzoru określonego w **załączniku nr 3A.**
3) Inspektor Ochrony Danych prowadzi ewidencję osób posiadających upoważnienie i polecenie przetwarzania danych osobowych Ewidencja ma charakter pomocniczy i stanowi **załącznik nr 4**.

6. 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 oraz 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 incydenty ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania z wykorzystaniem dokumentu stanowiącego **załącznik nr 5** (formularz rejestracji incydentu).
6) W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób których dotyczą, ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłaszają ten fakt organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych.

Zgłoszenie dokonuje się w następujących, możliwych formach:

a) elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego na platformie biznes.gov.pl,
b) elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePartyst: /UODO/SkrytkaESP,
c) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl,
d) pocztą tradycyjną listem ZPO, wysyłając wypełniony formularz na adres Urzędu Ochrony Danych Osobowych na adres: ul. Stawki 2, 00-193 Warszawa.

ADO zawiadamia o incydencie także osobę, której dane dotyczą, niezależnie od tego, czy ryzyko naruszenia praw i wolności tej osoby jest wysokie. Wzór zawiadomienia osoby o naruszeniu zasad ochrony Danych Osobowych stanowi **załącznik nr 6** do niniejszej Polityki.

Wzór zgłoszenia naruszenia zasad ochrony Danych Osobowych określa **załącznik nr 7**.

7. Regulamin Ochrony Danych Osobowych

Regulamin ma na celu zapewnienie zasad bezpiecznego przetwarzania danych osobowych w Akademii Wychowania Fizycznego w Poznaniu i stanowi odrębny dokument, ujęty treścią **załącznika nr 8.**

8. Zasady czystego biurka, ekranu i czystej drukarki

Zasady czystego biurka, ekranu i czystej drukarki ujęte są treścią odrębnego dokumentu (**załącznik nr 9**).

9. Szkolenia

Każda osoba przed dopuszczeniem do pracy z danymi osobowymi musi być przeszkolona i zapoznana z zasadami ochrony danych osobowych w Akademii Wychowania Fizycznego w Poznaniu. Szkolenie ma formę e-learningu i dostępne jest pod adresem: *awf.poznan.pl/rodo* (strona dostępna po zalogowaniu). Za przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych.

Po szkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad oraz deklaracji ich stosowania (**załącznik nr 10** - oświadczenie o poufności). Uczestnicy zobowiązani są również do wypełnienia testu. Oświadczenie o poufności oraz test deponowane są u IOD.

10. Plan ciągłości działania

Za opracowanie i aktualizację planu ciągłości działania odpowiada Sekcja IT. Plan ciągłości działania stanowi **załącznik nr 11**. W przypadku zmian konfiguracyjnych lub rozpoczęcia eksploatacji nowego systemu, plan ciągłości działania musi zostać poddany aktualizacji.

11. Instrukcja zarządzania systemami informatycznymi

Instrukcję zarządzania systemami informatycznymi zawarta jest w Regulaminie Ochrony Danych Osobowych.

12. Wykaz zabezpieczeń

Wykaz zabezpieczeń stosowanych przez Administratora Danych Osobowych stanowi **załącznik nr 12**.

13. Pozostałe procedury i regulacje będące elementem polityki ochrony danych osobowych

Częścią składową niniejszego dokumentu są procedury i regulacje określone treścią następujących załączników:

1) **Załącznik nr 13** - Procedura niszczenia wydruków zawierających dane osobowe,
2) **Załącznik nr 14** - Polityka retencji danych,
3) **Załącznik nr 15** - Zasady udostępniania danych osobowych studentów i absolwentów,
4) **Załącznik nr 16** - Nagrywanie zajęć prowadzonych w trybie zdalnym.

14. Obowiązek informacyjny

Administrator Danych Osobowych 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 lub w formie klauzul przy formularzach rejestracyjnych.