Dokument wprowadzony zarządzeniem 24/2018
Rektora AWF w Poznaniu
z dnia 05 czerwca 2018 r.

Polityka Ochrony Danych Osobowych

w

Akademii Wychowania Fizycznego

im. Eugeniusza Piaseckiego 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 jak np. kod genetyczny.

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 Administratora, 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 legalnie przetwarzane,
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 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).

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.

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.

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

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

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 do zarządzenia – 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 wdrożenia 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 do zarządzenia - 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, stanowiący załącznik nr 6 do zarządzenia.
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 Akademii Wychowania Fizycznego w Poznaniu i stanowi załącznik nr 7 do zarządzenia - Regulamin Ochrony Danych Osobowych.

6 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być przeszkolona, zapoznana zasadami ochrony danych osobowych w Akademii Wychowania Fizycznego 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 - plan ciągłości działania.

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 instruktarzowe 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.