„Polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych”

Akademia Wychowania Fizycznego we Wrocławiu

al. Ignacego Jana Paderewskiego 35

51-612 Wrocław

listopad 2018

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Niniejszy dokument został opracowany w celu zapewnienia prawidłowości wdrożenia i zabezpieczenia procesu przetwarzania danych osobowych w Akademii Wychowania Fizycznego we Wrocławiu oraz kompleksowości rozwiązań w przedmiotowym obszarze.
2. Głównym celem wprowadzenia „Polityki bezpieczeństwa" jest zapewnienie zgodności działania Akademii z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Polityka bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych oraz ich zabezpieczenia przed nieuprawnionym dostępem.
2. Na politykę bezpieczeństwa składają się następujące informacje:
   - wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
   - wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
   - opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
   - sposób przepływu danych pomiędzy poszczególnymi systemami,
   - określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
2. **zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3. **przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4. **poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
5. **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6. **zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
7. **usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
8. **dokumentacja przetwarzania danych** - dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
9. **sprawdzenie** – czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
10. **sprawozdanie** – dokument opracowany przez IOD po dokonaniu sprawdzenia,
11. **„Polityka Bezpieczeństwa"** – „Polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych",
12. **ADO** - Administrator Danych Osobowych,
13. **IOD** - Inspektor Ochrony Danych,
14. **ASI** - Administrator Systemów Informatycznych,
15. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. PODMIOTY ZAANGAŻOWANE W PROCES OCHRONY DANYCH OSOBOWYCH W AWF WROCŁAW

2.1. INFORMACJE OGÓLNE

- ✓ Administrator Danych Osobowych,
- ✓ Inspektor Ochrony Danych,
- ✓ Administrator Systemów Informatycznych,
- ✓ Osoby upoważnione do przetwarzania danych osobowych.

2.2. ADMINISTRATOR DANYCH OSOBOWYCH

Do obowiązków Administratora Danych Osobowych należy m. in.:

- ➢ wdrożenie odpowiednich i skutecznych środków oraz wykazanie, że czynności przetwarzania są zgodne rozporządzeniem oraz, że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.
- ➢ współpraca z organem nadzorczym,
- ➢ udostępnianie organowi nadzorczemu rejestrów w celu monitorowania operacji przetwarzania.
- ➢ wdrożenie środków minimalizujące ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufności oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie.

2.3. INSPEKTOR OCHRONY DANYCH

Do uprawnień i obowiązków Inspektora Ochrony Danych należą m. in.:

- ➢ stały nadzór nad treścią „Polityki Bezpieczeństwa",
- ➢ nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych,
- ➢ nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
- ➢ prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,

- nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,
- informowanie Administratora Danych – Rektora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych,
- szacowanie ryzyka właściwe dla przetwarzania,
- prowadzenie rejestru czynności lub rejestru kategorii czynności.

2.4. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

Administratorem Systemów Informatycznych jest osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).

Do uprawnień i obowiązków ASI należy m. in.:

- nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
- nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
- podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

- identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.

2.5. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

Wzór upoważnienia dla pracownika zajmującego się przetwarzaniem danych osobowych zawiera załącznik nr 2.

3. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Akademia, jako Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze umowy.
2. Do umów zawieranych z podmiotami zewnętrznymi, przy realizacji których istnieje prawdopodobieństwo dostępu do pomieszczeń lub informacji i danych podlegających ochronie powinny zostać włączone klauzule:
    - dotyczące obowiązku ochrony tych informacji przez strony umowy zarówno w trakcie trwania umowy, jak i po jej ustaniu,
    - ograniczenia dostępu do informacji wyłącznie do osób związanych z realizacją umowy,
    - zakazu ujawniania danych,
    - odpowiedzialności w przypadku naruszenia bezpieczeństwa danych zarówno przez podmiot jak i zatrudnionych pracowników.
3. Projekty umów powierzenia przetwarzania danych osobowych innemu podmiotowi należy opiniować u IOD.
4. Jednostki organizacyjne, w których zawierane są umowy powierzenia przetwarzania danych osobowych zobowiązane są do prowadzenia rejestru umów powierzenia.
5. Podmiot, któremu powierzono przetwarzanie danych osobowych może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie, ponosi również odpowiedzialność za zachowanie wszelkich wymogów wynikających z przepisów prawa w zakresie ochrony danych osobowych, w szczególności zastosowanie wymogów technicznych i organizacyjnych do zabezpieczenia przedmiotowych danych.

4. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi każdy pracownik mający dostęp do danych.
2. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
3. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
4. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
5. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
7. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

5. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić IOD w przypadku stwierdzenia naruszenia:
    - zabezpieczenia systemu informatycznego,
    - technicznego stanu urządzeń,
    - zawartości zbioru danych osobowych,
    - ujawnienia metody pracy lub sposobu działania programu,
    - jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
    - innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.).
2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
3. W razie niemożliwości zawiadomienia IOD lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
4. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych IOD lub upoważnionej przez niego osoby, należy:
    - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
    - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
    - zaniechać, o ile to możliwe dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
    - podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych
    - stosownie do objawów i komunikatów towarzyszących naruszeniu,

- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub osoby upoważnionej.

5. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, IOD lub osoba go zastępująca:
   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy AWF,
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   - rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu ADO,
   - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza AWF.
6. IOD dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   - wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   - określenie czasu i miejsca naruszenia i powiadomienia,
   - określenie okoliczności towarzyszących i rodzaju naruszenia,
   - wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   - wstępną ocenę przyczyn wystąpienia naruszenia,
   - cenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
7. Raport, o którym mowa w pkt 6, IOD niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.
8. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu IOD zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
9. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo AWF, IOD, Pełnomocnika ds. Ochrony Informacji Niejawnych.

10. Analiza, o której mowa w ust. 9, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Wzór raportu z naruszenia bezpieczeństwa systemu informatycznego stanowi załącznik nr 8 do niniejszego opracowania.

6. TRYB I SPOSÓB SPRAWDZANIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH ORAZ OPRACOWANIA SPRAWOZDANIA

1. Sprawdzenie jest przeprowadzane w trybie:
   - sprawdzenia planowego – według planu sprawdzeń,
   - sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez IOD wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;
2. Plan sprawdzeń określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.
3. IOD w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych.
4. Plan sprawdzeń jest przygotowywany przez IOD na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje, co najmniej jedno sprawdzenie.
5. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem, co najmniej raz na pięć lat.
6. Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez IOD o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.
7. IOD zawiadamia administratora danych o rozpoczęciu sprawdzenia doraźnego.
8. IOD dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
9.. Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:
   - sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

- odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
- sporządzeniu kopii otrzymanego dokumentu;
- sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
- sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

10. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności IOD mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych osobowych, w szczególności osoby zarządzającej tym systemem.
11. Materiały są sporządzane w postaci papierowej lub w postaci elektronicznej.
12. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia IOD przeprowadzenie czynności w toku sprawdzenia.
13. IOD zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.
14. Po zakończeniu sprawdzenia IOD przygotowuje sprawozdanie.
15. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.
16. IOD przekazuje administratorowi danych sprawozdanie:

Wzór sprawozdania ze sprawdzenia stanowi załącznik nr 7 do niniejszego opracowania.

7. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

ADO jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych AWF, a w szczególności:

1. zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
2. zapobiegać przetwarzaniu danych z naruszeniem RODO oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych,
3. zapobiegać przed zabraniem danych przez osobę nieuprawnioną.

7.1.ZABEZPIECZENIA ORGANIZACYJNE

- Zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych. IOD zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
- Kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

Wykaz pomieszczeń, w których przetwarzane są dane osobowe zawiera załącznik nr 1.

7.2. ZABEZPIECZENIA TECHNICZNE

1. W pomieszczeniach, w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego.
2. W pomieszczeniach, w których znajdują się serwery zamontowane powinny być czujniki dymu.
3. W pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.
4. Wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

7.3. ZABEZPIECZENIA CHRONIĄCE PRZED UTRATĄ DANYCH

1. Odrębne zasilanie sprzętu komputerowego.
2. Ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS.
3. Ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny. Za proces tworzenia kopii zapasowych odpowiada ASI lub osoba specjalnie do tego celu wyznaczona.
4. Ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.

7.4. ZABEZPIECZENIA PRZED NIEAUTORYZOWANYM DOSTĘPEM

1. Wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (skrosowanie) danego użytkownika do sieci komputerowej dokonuje ASI w uzgodnieniu i po powiadomieniu IOD.
2. Aby uzyskać dostęp do systemu, należy zwrócić się do IOD z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.
3. W systemie informatycznym stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora i hasła:
   - każdy użytkownik systemu przetwarzania posiada swój unikalny identyfikator,
   - użytkownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami,
   - każdy użytkownik zarządza swoimi hasłami dla wszystkich identyfikatorów, których używa,
   - hasło użytkownika jest jego własnością i zna je wyłącznie dany użytkownik – zabronione jest przekazywania hasła innym osobom.

7.5. ZABEZPIECZENIA PRZED NIEAUTORYZOWANYM DOSTĘPEM PRZEZ INTERNET

W zakresie dostępu z sieci wewnętrznej do sieci rozległej Internet stosuje się firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. „Ściana ogniowa" składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.

7.6. ZABEZPIECZENIA ANTYWIRUSOWE

Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w sposób następujący:

1. Zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego.
2. Możliwość centralnego uaktualnienia wzorców wirusów.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania. Niezależnie od niniejszych zasad opisanych „Polityce bezpieczeństwa" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

8. ARCHIWIZACJA DANYCH

Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii awaryjnych i kopii bezpieczeństwa. Za proces tworzenia kopii odpowiada ASI lub osoba specjalnie do tego celu wyznaczona.

8.1.WYKONYWANIE KOPII

1. Kopie wykonywane są na taśmę, płytę CD, DVD, zewnętrzne nośniki pamięci lub serwer kopii.
2. Dane systemu wraz z bazą danych kopiowane są co najmniej raz w tygodniu – tzw. pełny backup bazy danych.
3. Kopie awaryjne danych zapisywanych w programie wykonywane są codziennie – tzw. dump schematu systemu.
4. Kopie przechowywane są w miejscach zapewniających ich odpowiednią ochronę przed osobami niepowołanymi oraz czynnikami zewnętrznymi mogącymi je uszkodzić (np. kasa pancerna, serwerownia z kontrolą dostępu).
5. ASI odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
6. ASI podejmuje odpowiednie czynności w celu okresowej weryfikacji kopii zapasowych pod kątem ich przydatności.

8.2. NISZCZENIE KOPII

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny, tak by nie można było użyć ich ponownie.
3. Poprawność zniszczenia nośnika magnetycznego powinna być sprawdzona przez IOD.
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

ZAŁĄCZNIKI

Załącznik nr 1

- Wykaz pomieszczeń , w których przetwarzane są dane osobowe w AWF.

Załącznik nr 2

- Wzór upoważnienia do przetwarzania danych.

Załącznik nr 3

- Wzór oświadczenia o zobowiązaniu się do zachowania poufności.

Załącznik nr 4

- Wykaz zbiorów danych osobowych w AWF.

Załącznik nr 5

- Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 6

- Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Załącznik nr 7

- Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających.

Załącznik nr 8

- Raport z naruszenia bezpieczeństwa systemu informatycznego.

Załącznik nr 1 – Wykaz pomieszczeń, w których przetwarzane są dane osobowe w AWF

Dział/Stanowiska	Budynek i pokój	System komputerowy służący do przetwarzania danych osobowych
Archiwum AWF	Budynek WOSS pok.109	Azak firmy Archicom S.C
Dziekanat Wydziału WF	Budynek DS. Spartakus pok.110, 107	eOrdo (system dziekanatowy firmy Unold Comp.),
Dziekanat Wydziału Fizjoterapii	Budynek P4 pok. 2/23-31	eOrdo (system dziekanatowy firmy Unold Comp.),
Dziekanat Nauk o Sporcie	Hala Wielofunkcyjna pok.72	eOrdo (system dziekanatowy firmy Unold Comp.),
Dom Studencki „Spartakus"	Budynek DS. „Spartakus" Pok.13,14,15	eOrdo (system dziekanatowy firmy Unold Comp.),
Dom Studencki „Olimpia"	Budynek DS. „Olimpia"	eOrdo (system dziekanatowy firmy Unold Comp.),
Biblioteka	Budynek Biblioteki	Aleph (system biblioteczny firmy Aleph),
Inspektorat BHP i P.-POŻ.	Budynek WOSS pok.107	Teta (system kadrowo-płacowy firmy Teta)
Księgowość	Hala Wielofunkcyjna pok.32	eOrdo (system dziekanatowy firmy Unold Comp.), F-K (system finansowo-księgowy firmy Yuma)
Dział Spraw Pracowniczych i Płac	Hala Wielofunkcyjna pok.15,16,17	Teta i Teta HRM (systemy kadrowo-płacowe firmy Teta)
Rektorat	Budynek przy Banacha 11	eOrdo (system dziekanatowy firmy Unold Comp.)
Centrum Doskonalenia Kadr	Budynek przy Witelona 25 pok.013	eOrdo (system dziekanatowy firmy Unold Comp.)
Pracownicy dydaktyczni i administracyjni	INTRANET	Omnis (system dziekanatowy firmy Unold Comp.), Teta HRM (system kadrowo-płacowy firmy Teta)
Komisje Rekrutacyjne	Budynkek P4	eOrdo (system dziekanatowy firmy Unold Comp.)

Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Inspektor Ochrony Danych w Akademii Wychowania Fizycznego we Wrocławiu, na podstawie art.28 i 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), upoważniam Panią:

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Akademii Wychowania Fizycznego we Wrocławiu. Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

Data i podpis osoby upoważnionej

Załącznik nr 3 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

......................, dnia ....

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y . . . . zamieszkała/y w . . . . zatrudniona/y na stanowisku . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z .... Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

....

(Podpis)

Załącznik nr 4 – Wykaz zbiorów danych osobowych w AWF

- ✓ **Dane kadrowe i płacowe,**
- ✓ **Dane w systemie księgowym,**
- ✓ **Dane studenckie – dziekanaty,**
- ✓ **Dane studenckie - pozostałe jednostki,**
- ✓ **Rekrutacja na studia,**
- ✓ **Rekrutacja do pracy,**
- ✓ **Dane gromadzone w systemie bibliotecznym,**
- ✓ **Dane osób zamieszkałych w domach studenckich,**
- ✓ **Dane gromadzone przez Centrum Doskonalenia Kadr,**
- ✓ **Dane gromadzone w archiwum AWF,**
- ✓ **Dane podręczne przechowywane w działach,**
- ✓ **Dane Biura Karier,**
- ✓ **Dane w projektach (badawcze, unijne, zagraniczne itp..).**

Załącznik nr 5 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Nr upoważnienia	Nazwa zbioru objętego zakresem upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Załącznik nr 6 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

ŚRODKI TECHNICZNE

Środek ochrony technicznej i fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).**		
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą krat, rolet lub folii antywłamaniowej.**		
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**		
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**		
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**		
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**		
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**		
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**		

9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**		
10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**		
11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie.**		
17. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**		
18. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**		

ŚRODKI ORGANIZACYJNE

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych		
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych		
Wyznaczono Inspektora Ochrony Danych		
Opracowano i wdrożono Politykę Bezpieczeństwa		
Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych		
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych		
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego		

Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy		
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym		
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco		

Załącznik nr 7 - Sprawozdanie z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/ czynności sprawdzających

.....

miejscowość, data

SPRAWOZDANIE

Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*

w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej:.....
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli: .....
3. Data wykonania czynności kontrolnych:.....
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: .....
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:.....

   .....
6. Ustalenia dokonane w trakcie czynności kontrolnych:.....

   .....

   .....

   .....

   .....

   .....
7. Wnioski i zalecenia pokontrolne:

   .....

   .....

   .....

   .....

   .....

.....

(data i podpis osoby wykonującej czynności kontrolne)

.....

(data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:
Kierownik kontrolowanej jednostki organizacyjnej
Inspektor Ochrony Danych

* niepotrzebne skreślić

Załącznik nr 8 - Raport z naruszenia bezpieczeństwa systemu informatycznego

Akademia Wychowania Fizycznego
we Wrocławiu

Wrocław, dnia .....

Raport z naruszenia bezpieczeństwa systemu informatycznego

1. Data: .... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:
.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:
.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:
.....
.....
.....

6. Podjęte działania:
.....
.....
.....

7. Postępowanie wyjaśniające:
.....
.....
.....

.....

(Data i podpis Inspektora Ochrony Danych)