POLITYKA OCHRONY DANYCH OSOBOWYCH

I. Przepisy ogólne

§ 1.

Polityka ochrony danych osobowych opracowana została na podstawie 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 (Dz. U. UE. L. 2016.119.1), zwanego dalej „RODO".

§ 2.

1. Celem Polityki ochrony danych osobowych w UKS Wilanowskie Wilki zwanej dalej „Polityką ochrony danych", jest zapewnienie właściwej ochrony danych osobowych osób fizycznych przetwarzanych przez UKS Wilanowskie Wilki, poprzez wdrożenie odpowiedniego systemu ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi, w tym określenie czynności i zasad, które należy realizować, aby ograniczyć ryzyko nieautoryzowanego dostępu do danych osobowych oraz wyeliminować negatywne skutki takiego dostępu.
2. Ochrona przetwarzanych danych osobowych polega na podejmowaniu działań mających na celu zapewnienie, aby dane te były pozyskiwane i przetwarzane zgodnie z przepisami prawa, zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem.
3. Ochrona danych osobowych jest realizowana na każdym etapie przetwarzania informacji zawierających dane osobowe i ma zastosowanie do przetwarzania danych osobowych w formie tradycyjnej (papierowej) oraz w systemach informatycznych i na cyfrowych nośnikach elektronicznych danych.

§ 3.

Na użytek niniejszej Polityki ochrony danych:

1) dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2) przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3) administrator – UKS Wilanowskie Wilki, ul. Ledóchowskiej 10, 02-972 Warszawa;

4) naruszenie ochrony danych osobowych - oznacza 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.

II. Zasady dotyczące przetwarzania danych osobowych

§ 4.

Dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");

2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ("ograniczenie celu");

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");

4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");

5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane ("ograniczenie przechowywania");
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

III. Odpowiedzialność i zadania administratora

§ 5.

Administrator jest odpowiedzialny w szczególności za:
1) nadzór nad przestrzeganiem zasad wymienionych w § 4;
2) wykazanie, zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO, przestrzegania zasad wymienionych w § 4 ;
3) wykazanie, zgodnie z art. 7 ust. 1 RODO, że osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych;
4) udzielenie osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO;
5) realizację prawa dostępu do informacji o przetwarzaniu danych przysługującego osobie której dane dotyczą, zgodnie z art. 15 RODO;
6) realizację żądania, z którymi wystąpi osoba, której dane dotyczą, na podstawie art. 16-22 RODO, udzielania wszelkich informacji o działaniach podjętych w związku z żądaniem albo informacji o powodach niepodjęcia działań oraz o możliwości wniesienia skargi;
7) wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia stopnia bezpieczeństwa odpowiadającego stopniu ryzyka naruszenia praw lub wolności osób, której dane dotyczą;
8) prowadzenie rejestru czynności przetwarzania;
9) zgłaszanie naruszenia danych osobowych organowi nadzorczemu;
10) zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;
11) współpracę z organem nadzorczym.

IV. Odpowiedzialność osób uprawnionych do przetwarzania danych osobowych

§ 6.

1. Uprawnionymi do przetwarzania danych osobowych są osoby posiadające upoważnienie nadane przez administratora oraz odpowiednio przeszkolone.
2. Osoby wskazane w ust. 1 są zobowiązane do przetwarzania danych osobowych zgodnie z RODO, do prowadzenia dokumentacji przetwarzania danych osobowych w sposób należycie i wyczerpująco dokumentujący, że podejmowane przez nich czynności są zgodne z zasadami przetwarzania danych.
3. Osoby wskazane w ust.1 są ponadto zobowiązane do dokumentowania otrzymania zgód na przetwarzanie danych osobowych, oraz udzielenia osobom, których dane dotyczą wymaganych prawem informacji.
4. Upoważnienie do przetwarzania danych osobowych, którego wzór określa **załącznik nr 1** do Polityki ochrony danych, powinno zawierać w szczególności:
1) imię i nazwisko osoby upoważnionej;
2) zakres przetwarzanych danych osobowych;
3) czas obowiązywania.
5. Ewidencję osób uprawnionych do przetwarzania danych osobowych, zwanych dalej "użytkownikami", prowadzi pracownik upoważniony przez administratora. Wzór ewidencji określa **załącznik nr 2** do Polityki ochrony danych.
6. Użytkownik traci uprawnienia wynikające z upoważnienia do przetwarzania danych osobowych oraz uprawnienia, o których mowa powyżej, w przypadku:
1) wycofania upoważnienia przez administratora danych osobowych;
2) rozwiązania lub ustania stosunku pracy.
7. Wycofanie upoważnienia następuje w szczególności w przypadku jeżeli użytkownik dopuścił się naruszenia zasad ochrony danych osobowych lub nastąpiła zmiana służbowego zakresu czynności na zakres, z którym nie łączy się przetwarzanie danych osobowych.

V Szkolenia

§ 7.

1. Osoba upoważniona przez administratora przeprowadza szkolenie z zakresu ochrony danych osobowych pracowników, którzy w związku z nawiązanym zatrudnieniem lub zmianą służbowego zakresu czynności będą dopuszczeni do przetwarzania danych osobowych.
2. Ostateczny zakres oraz przebieg szkolenia określa administrator, szkolenie w swoim zakresie powinno obejmować następujące zagadnienia:
1) przepisy o ochronie danych osobowych;
2) zasady przetwarzania danych osobowych;
3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych;
4) zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych;
5) zagrożenia, na jakie może być narażone przetwarzanie danych osobowych, w tym zagrożenia związane z przetwarzaniem danych osobowych w systemach informatycznych;
6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
7) sposób postępowania w przypadku naruszenia ochrony danych;
8) odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

VI. Standardowe zabezpieczenia pomieszczeń i systemów informatycznych

§ 8.

1. Użytkownik zobowiązany jest do odpowiedniego zabezpieczenia danych osobowych przed dostępem osób nieupoważnionych, w szczególności ma obowiązek:
1) przechowywać dane występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu, w szczególności w zamkniętych pomieszczeniach, szafach, biurkach lub kasach pancernych;
2) uniemożliwić dostęp do danych wyświetlanych na ekranach komputerów osobom nieuprawnionym;
3) zachować w tajemnicy loginy i hasła uwierzytelniające go w systemie;
4) bezwzględnie przestrzegać zakresu nadanego upoważnienia;
5) przetwarzania i ochrony danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami;
6) zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia;

7) zgłosić do administratora wszelkie przypadki naruszenia bezpieczeństwa danych oraz stwierdzone nieprawidłowości.

2. Szczegółowe zasady zabezpieczenia danych osobowych przed dostępem osób nieupoważnionych zawiera **załącznik nr 3** do Polityki ochrony danych.

§ 9.

1. W pomieszczeniach, w których przetwarzane są dane osobowe część ogólnodostępna powinna być wyraźnie oddzielona od części służącej do przetwarzania danych, w sposób uniemożliwiający zapoznanie się z danymi osobowymi przez osoby nieuprawnione.

2. Klucze do pomieszczeń, o których mowa w ust. 1, przechowywane są na portierni szkoły w sposób uniemożliwiający dostęp osób niepowołanych, a ich wydawanie i zwrot odnotowywane jest w odpowiedniej ewidencji.

3. Dostęp do budynków, pomieszczeń i części pomieszczeń, w których przetwarzane są dane osobowe podlega całodobowej kontroli.

4. Kontrola, o której mowa w ust. 2, polega na:

1) prowadzeniu ewidencji pobierania i zwrotu kluczy do budynków, pomieszczeń i części pomieszczeń;

2) nadawaniu uprawnień do wejścia do określonych stref służbowych – w formie zapisów elektronicznych na identyfikatorach służbowych i kartach wstępu.

§ 10.

1. Serwisowanie urządzeń i sprzętu związanego z przetwarzaniem danych osobowych powinno następować w możliwie krótkim czasie od wykrycia jego awarii.

2. Systemy informatyczne służące do przetwarzania danych osobowych zabezpiecza się odpowiednim systemem antywirusowym.

3. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny przy wykorzystaniu cyfrowych nośników elektronicznych (np. płyty CD, DVD lub inne nośniki pamięci zewnętrznej) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportuimportu danych za pomocą teletransmisji.

4. Cyfrowe nośniki elektroniczne zawierające dane osobowe, przekazywane poza obszar

przetwarzania danych, powinny być zabezpieczone w sposób zapewniający poufność i integralność tych danych.

VII. Szczegółowe regulacje dotyczące ochrony danych osobowych

§ 11.

1. W […] wprowadza się następujące szczegółowe regulacje dotyczące ochrony danych osobowych:

1) „Procedury postępowania związane z ochroną danych osobowych w UKS Wilanowskie Wilki, stanowiące **załącznik nr 4** do Polityki ochrony danych;

2) Zgłaszanie naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, stanowiące **załącznik nr 5** do Polityki ochrony danych;

X. Przepisy końcowe

§ 14.

1. Dane osobowe będące w posiadaniu […] poddawane są archiwizacji.

2. Archiwizowanie przetwarzanych danych osobowych odbywa się zgodnie z odrębnymi przepisami.

§ 15.

Tryb niszczenia dokumentów zawierających dane osobowe, zapisanych w szczególności na nośnikach papierowych lub cyfrowych nośnikach elektronicznych, określa **załącznik nr 6** do Polityki ochrony danych.

Załącznik nr 1 do Polityki ochrony danych

Warszawa, dnia ……201…. r.

Wzór

U P O W A Ż N I E N I E nr …

Na podstawie art. 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 (Dz. Urz. UE.L.2016.119.1)

u p o w a ż n i a my

Pana/Panią……

……

(imię, nazwisko, funkcja)

do przetwarzania danych osobowych członków (w tym również członków uczestników UKS Wilanowskie Wilki), tj. danych podanych w karcie zgłoszenia oraz dowodach wpłat zawartych w dokumentacji oraz zbiorach dotyczących działalności UKS Wilanowskie Wilki (tj. bazy danych członków zawierającej również informacje o dokonywanych płatnościach).

Upoważnienie wygasa z chwilą wykreślenia jako członka klubu lub rezygnacji z pełnionej funkcji.

Jest Pan/Pani zobowiązany(a) do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał(a) Pan/Pani dostęp w związku z wykonywaniem obowiązków wynikających z pełnionej funkcji, jak również sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu współpracy z UKS Wilanowskie Wilki.

……
(podpis administratora danych - członków Zarządu UKS Wilanowskie Wilki)

Oświadczam, że jestem przeszkolony/a w zakresie ochrony danych osobowych i zapoznałem/am się z przepisami Rozporządzenia 2016/679

……..
(data i podpis członka UKS Wilanowskie Wilki)

Załącznik Nr 2 do Polityki ochrony danych

Wzór

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Funkcje/ jednostka organizacyjna	Numer upoważnienia	Data nadania	Zakres upoważnienia	Uwagi	Data ustania

Załącznik nr 3 do Polityki ochrony danych

Zasady zabezpieczenia danych osobowych przed dostępem osób nieupoważnionych

1. Loginy i hasła dostępowe do systemu informatycznego należy zachować w tajemnicy, nie powierzać swoich identyfikatorów innym. Niedopuszczalne jest zapisywanie loginów i haseł na kartkach i umieszczanie ich w ogólnie dostępnych miejscach (pod klawiaturą, na monitorze, w szufladach, biurkach itp.).
2. Dane występujące w formie tradycyjnej (dokumenty, wydruki, skany, tradycyjna korespondencja pocztowa) należy przechowywać w odpowiednio zabezpieczonym miejscu, w szczególności w zamkniętych pomieszczeniach, szafach, biurkach lub kasach pancernych. Dotyczy to także zawierających dane nośników elektronicznych *(płyty CD, DVD, a także pamięci typu PenDrive i dyski USB).*
3. Po skończonej pracy dokumenty tradycyjne należy zabezpieczyć poprzez schowanie ich do zamykanych szaf biurowych. Nie należy pozostawiać dokumentów na wierzchu w ogólnie dostępnych miejscach (dotyczy to także wydruków z drukarek, kopii i skanów itp). Po skończonej pracy komputer należy wyłączyć (Windows, menu *Star*t > *Zamknij system*), sprawdzić drukarkę czy na jej podajnikach nie pozostały jakieś wydruki (które również należy schować). Pokój biurowy należy zamknąć na klucz, a klucz zabrać i zdać w miejscu pobrania.
4. W razie konieczności opuszczenia pokoju na tzw. krótki czas, należy zabezpieczyć dostęp do przetwarzanych danych poprzez zamknięcie drzwi opuszczanego pomieszczenia na klucz i zabranie go ze sobą. W przypadku pracy w pokoju wieloosobowym, przed wyjściem należy zabezpieczyć stanowisko pracy poprzez zablokowanie komputera (nacisnąć jednocześnie „Win + L" lub „Ctrl+Alt+Del" i wybrać opcję „*Zablokuj komputer*"). Uniemożliwi to osobom nieuprawnionym dostęp do danych wyświetlonych na ekranie monitora.
5. Wszelkie przeznaczone do wyrzucenia, niepotrzebne, wykorzystane już pojedyncze wydruki, kartki, notatki zawierające jakiekolwiek informacje wrażliwe, w tym w szczególności dane osobowe, (typu wydruki robocze, zestawienia, wykazy pomocnicze)

należy przed wyrzuceniem do kosza zniszczyć w niszczarce. Tego typu dokumentów nie wolno wyrzucać bezpośrednio do kosza na śmieci, bez ich wcześniejszego zniszczenia *(dotyczy to także elektronicznych nośników z danymi typu płyty CD, DVD).*

6. Treść przetwarzanych danych osobowych oraz sposób ich ochrony i metody ich zabezpieczeń należy zachować w tajemnicy.

7. Wszelkie zauważone nieprawidłowości w funkcjonowaniu systemów informatycznych oraz aplikacji komputerowych należy zgłaszać niezwłocznie do Zarządu UKS Wilanowskie Wilki.

8. Wszelkie zauważone naruszenia bezpieczeństwa danych osobowych (przetwarzanych zarówno w systemie komputerowym, jak i tradycyjnie, w formie papierowej) należy zgłosić niezwłocznie do administratora danych osobowych.

Załącznik nr 4 do Polityki ochrony danych

PROCEDURY POSTĘPOWANIA ZWIĄZANE Z OCHRONĄ DANYCH OSOBOWYCH - odrębny dokument

Załącznik nr 5 do Polityki ochrony danych

Zgłaszanie naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych

Warszawa, dnia .....roku

Prezes Urzędu Ochrony Danych Osobowych

ZGŁOSZENIE
W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 RODO 2016/679, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu …..... w …..... .

1.	**Charakter naruszenia ochrony danych:**	Np. *przesłanie przez pracownika wiadomości e-mail do błędnego adresata (nieznana osoba) zamiast do współpracownika wraz z załącznikiem w formacie pliku Excel (niezabezpieczonego) zawierającego dane klientów (takie jak: imię i nazwisko, adres zamieszkania, PESEL, nr. dowodu tożsamości,, numer telefonu, adresy e-mail, numery kart kredytowych)*
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	Np. *Klienci. Liczba osób, których dane dotyczą 5681*.
3.	**Liczba rekordów, których dotyczy naruszenie:**	Np. *821*
4.	**Możliwe konsekwencje naruszenia ochrony danych:**	Np. *powstanie szkód majątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub kradzież lub sfałszowanie tożsamości, strata finansowa*
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	Np. *wdrożenie stosownych środków kryptograficznych, w tym w tym pseudonimizacja, zakaz przesyłania załączników zawierających dane osobowe w sposób niezabezpieczony.*
6.	**Dane inspektora ochrony**	Nie dotyczy

	danych	

……
…….....
.....……
…….*

……
(Administrator)

*W przypadku zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin, administrator danych zobowiązany jest do złożenia wyjaśnień w przedmiocie przyczyn opóźnienia.

Załącznik nr 6 do Polityki ochrony danych

Tryb niszczenia dokumentów zawierających dane osobowe

Niszczenie dokumentów zawierających dane osobowe, zapisanych w szczególności na nośnikach papierowych lub cyfrowych nośnikach elektronicznych, odbywa się bezpośrednio, pod warunkiem zachowania standardów niszczenia tych dokumentów i nośników określonych w obowiązujących przepisach.