WARSZAWSKI UNIWERSYTET MEDYCZNY
MEDICAL UNIVERSITY OF WARSAW
Inspektor Ochrony Danych

PODSTAWOWE INFORMACJE DOTYCZĄCE ZASAD OCHRONY DANYCH OSOBOWYCH w Warszawskim Uniwersytecie Medycznym

(Materiał szkoleniowy przeznaczony do szkolenia pracowników/studentów/doktorantów/słuchaczy Uczelni)

Zasady i procedury przetwarzania danych osobowych są zawarte w Rozporządzeniu 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) - RODO;

Zasady i procedury przetwarzania danych osobowych, obowiązujące w Uczelni są zawarte w **zarządzeniu Rektora WUM nr 48 z dnia 23 maja 2018 r.** oraz w załączonych do niego dokumentach, wymienionych poniżej:

1) Polityka bezpieczeństwa danych osobowych;

2) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

3) Regulamin organizacji i przetwarzania danych osobowych.

Ilekroć w dokumentach dotyczących ochrony danych osobowych w WUM mowa jest o:

1) Administratorze - należy przez to rozumieć Administratora Danych Osobowych (ADO), którym jest Warszawski Uniwersytet Medyczny, w którego imieniu właściwe kompetencje sprawuje Rektor;
2) Inspektorze Ochrony Danych (w skrócie IOD) - należy przez to rozumieć osobę wyznaczoną przez Administratora w celu opracowywania, nadzorowania i przestrzegania w jego imieniu zasad ochrony danych oraz zgłoszoną do Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z wymogami przepisów RODO;
3) Lokalnych Dysponentach Danych Osobowych (zwanych dalej LDDO) - należy przez to rozumieć pracowników WUM, którym Administrator powierzył na podstawie upoważnienia obowiązki administrowania danymi osobowymi;
4) Administratorach Systemów Informatycznych (zwanych dalej ASI) - należy przez to rozumieć osoby wyznaczone przez kierownika Działu Informatyki, odpowiedzialne za wdrożenie i stosowanie zasad bezpieczeństwa danych w zakresie technicznych zabezpieczeń systemu informatycznego;
5) Użytkowniku - należy przez to rozumieć każdą osobę posiadającą upoważnienie nadane przez Administratora lub LDDO do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, po złożeniu oświadczenia o zapoznaniu się z obowiązującymi przepisami i zobowiązaniu do ich przestrzegania;
6) danych osobowych - należy przez to rozumieć 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;

7) danych szczególnych kategorii - należy przez to rozumieć dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane genetyczne lub biometryczne, służące do jednoznacznego zidentyfikowania osoby fizycznej oraz dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
8) zbiorze danych - należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, utrwalony zarówno w formie elektronicznej, jak i tradycyjnej (papierowej), dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
9) RODO - należy przez to rozumieć Rozporządzeniu 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);
10) Ustawie – należy przez to rozumieć ustawę z dnia . . . o ochronie danych osobowych (do uzupełnienia po wejściu w życie jej przepisów);
11) Prezesie UODO - należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych, pełniącego zgodnie z RODO funkcję organu nadzorczego;
12) Zarządzeniu - należy przez to rozumieć niniejsze zarządzenie;
13) Polityce - należy przez to rozumieć Politykę Bezpieczeństwa Danych Osobowych WUM (PBDO) stanowiącą załącznik nr 1 do Zarządzenia;
14) Regulaminie - należy przez to rozumieć Regulamin organizacji przetwarzania danych osobowych stanowiący załącznik nr 2 do zarządzania;
15) Instrukcji - należy przez to rozumieć Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiącą załącznik nr 3 do zarządzenia;
16) Formularzu - należy przez to rozumieć jeden z formularzy zawartych w załączniku nr 4 do zarządzenia.

1. Kompetencje Administratora danych osobowych w Warszawskim Uniwersytecie Medycznym, w rozumieniu przepisów RODO, pełni jego Rektor.
2. Rektor wyznacza osobę odpowiedzialną za bezpieczeństwo danych osobowych w Warszawskim Uniwersytecie Medycznym zwaną dalej Inspektorem Ochrony Danych Osobowych (IOD).
3. O fakcie powołania i odwołania IOD Administrator Danych Osobowych zawiadamia Prezesa UODO.
4. Obowiązki Lokalnych Dysponentów Danych Osobowych (LDDO) wynikające z RODO Rektor powierza w formie upoważnienia:
   1) prorektorowi ds. personalnych i organizacyjnych w zakresie pracowników jednostek podległych prorektorom zgodnie z Regulaminem Organizacyjnym, pracowników pełniących funkcje przewodniczących i członków komisji senackich i rektorskich, rzeczników dyscyplinarnych oraz innych zespołów i osób powołanych przez Rektora, wykonawców umów cywilnoprawnych; kanclerzowi w zakresie pracowników administracji i obsługi Uczelni;

2) prorektorowi ds. studenckich i kształcenia w zakresie doktorantów i studentów, w szczególności pełniących funkcje członków komisji senackich i rektorskich;
3) dziekanom w zakresie pracowników, wykonawców umów cywilnoprawnych, doktorantów i studentów właściwych wydziałów;
4) kanclerzowi w zakresie podległych pracowników administracji i obsługi Uczelni
5) zastępcom kanclerza w zakresie pracowników podległych im jednostek oraz wykonawców umów cywilnoprawnych;
6) dyrektorowi Centrum Biblioteczno - Informacyjnego w zakresie pracowników Biblioteki Głównej, osób korzystających z zasobów bibliotecznych i wykonawców umów cywilnoprawnych;
7) okresowo sekretarzowi komisji rekrutacyjnej w zakresie niezbędnym do przeprowadzenia rekrutacji;
8) kierownikom jednostek organizacyjnych prowadzących badania naukowe, prace rozwojowe oraz świadczących usługi badawcze na ich wniosek, w zakresie niezbędnym do przeprowadzenia tych badań i prac.

Zasadą obowiązującą w WUM jest zachowanie przez użytkowników w tajemnicy wszelkich informacji dotyczących danych osobowych oraz sposobów ich zabezpieczania.

Możliwość wystąpienia zagrożeń bezpieczeństwa danych przetwarzanych w systemach lub kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych nakłada na użytkowników obowiązek zapewnienia danym skutecznej ochrony.

Przesyłanie danych osobowych za pomocą urządzeń telekomunikacyjnych lub transmisji danych w sieci publicznej wymaga wykorzystania odpowiednich urządzeń i przedsięwzięć zapewniających poufność i integralność ich przekazu.

Kopiowanie danych osobowych oraz wykonywanie wydruków jest co do zasady zabronione, chyba że konieczność ich sporządzania wynika z nałożonych na użytkownika obowiązków i jest to zarazem dozwolone przepisami prawa.

Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które posiadają pisemne upoważnienie do przetwarzania danych wydane przez Administratora lub LDDO.

Procedury nadawania, wycofywania, zmiany upoważnień do przetwarzania danych osobowych w Warszawskim Uniwersytecie Medycznym (WUM) obejmują:

1) złożenie do Administratora Danych Osobowych (Rektora bądź właściwego Lokalnego Dysponenta Danych Osobowych) wniosku o nadanie, wycofanie, zmianę upoważnienia do przetwarzania danych osobowych, wzór wniosku stanowi formularz nr 4.4;
2) podpisanie przez osobę ubiegającą się o nadanie upoważnienia oświadczenia o zachowaniu w tajemnicy zasad przetwarzania danych oraz sposobów ich zabezpieczania, obejmującej także okres po ustaniu zatrudnienia w (WUM), wzór oświadczenia stanowi formularz nr 4.5 (po uprzednim zapoznaniu z materiałem szkoleniowym);

3) nadanie przez Administratora Danych Osobowych (ADO lub LDDO) upoważnienia do przetwarzania danych osobowych - wzór upoważnienia stanowi formularz nr 4.6.

Pomieszczenia lub ich część, w których przetwarzane są dane osobowe tworzą obszar przetwarzania danych osobowych w Uczelni. Przebywanie osób nieuprawnionych w tym obszarze jest ograniczone i odbywać się może tylko w obecności użytkowników.

Administrator zapewnia ochronę obszaru przetwarzania danych osobowych w WUM, według zasad określonych w polityce bezpieczeństwa.

Do miejsc podlegających szczególnej ochronie Administrator zalicza pomieszczenia Działu Personalnego, Działu Płac oraz Dziekanaty i sekretariaty.

Środki ochrony, zastosowane przez Administratora dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, obejmują:

- środki fizyczne;
- środki osobowe;
- środki techniczne.

<u>Środki ochrony fizycznej obejmują</u>:

- lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
- ustalenie zasad gospodarki kluczami do pomieszczeń i szaf;
- wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, w drzwi zamykane na klucz, odpowiednio zabezpieczone okna, meble, zamknięcia i niezbędne zabezpieczenia alarmowe;
- składowanie nośników wymiennych i nośników kopii zapasowych, w odpowiednio zabezpieczonych szafach.

<u>Środki ochrony osobowej obejmują</u>:

- dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie nadane przez Administratora lub LDDO;
- zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemów (urządzeń) służących do ich przetwarzania;
- odebranie stosownych zobowiązań i oświadczeń; tj. zobowiązania do zachowania w tajemnicy danych i sposobów ich zabezpieczenia oraz oświadczenia o zapoznaniu się z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także z dokumentacją przetwarzania i ochrony danych osobowych.

<u>Środki ochrony technicznej obejmują</u>:

- mechanizmy kontroli dostępu do systemów i zasobów;
- zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (programy antywirusowe, ściany ogniowe, itp.);
- regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;
- zastosowanie ochrony zasilania.

Za naruszenie zasad ochrony danych osobowych, w tym zabezpieczenia systemu informatycznego bądź urządzenia w którym są przetwarzane dane osobowe, przyjmuje się każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną lub uszkodzenia jakiegokolwiek elementu, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym lub nieuprawnionym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

W przypadku stwierdzenia lub podejrzenia naruszenia zasad zabezpieczenia danych osobowych lub zaistnienia zdarzeń, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik przetwarzający dane osobowe w WUM jest zobowiązany przerwać przetwarzanie tych danych i niezwłocznie powiadomić o zaistniałym zdarzeniu bezpośredniego przełożonego oraz IOD, a następnie powinien postępować stosownie do ich decyzji.

Zgłoszenie naruszenia procedur ochrony danych osobowych powinno zawierać:

- opis symptomów naruszenia procedur ochrony danych osobowych;
- określenie sytuacji, miejsca i czasu zajścia zdarzenia;
- identyfikację rodzaju zaistniałego zdarzenia, w tym określenie skali zniszczeń, metody dostępu do danych osoby nieupoważnionej, itp.;
- przedstawienie wszelkich istotnych informacji i dokumentów (wydruków, raportów, innych), mogących wskazywać na przyczynę naruszenia;
- określenie znanych danej osobie możliwości zabezpieczenia zbiorów oraz wszelkich działań podjętych po ujawnieniu zdarzenia w celu uniemożliwienia lub ograniczenia dostępu osób nieuprawnionych, minimalizacji szkód i zabezpieczenia.

W WUM zabrania się przetwarzania danych szczególnych kategorii oraz danych o wyrokach skazujących i naruszeniach prawa, chyba, że pozwalają na to przepisy prawa bądź osoba, której tego typu dane dotyczą wyraziła pisemną zgodę.

Pracownik WUM, który:

a) przetwarza w zbiorze danych:
- dane osobowe, do których przetwarzania nie jest upoważniony;
- dane osobowe, których przetwarzanie jest zabronione;
- dane osobowe niezgodne z celem stworzenia danego zbioru;

b) udostępnia lub umożliwia dostęp do zbioru danych osobowych osobom nieupoważnionym;

c) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;

d) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw

- podlega odpowiedzialności porządkowej określonej w przepisach Kodeksu Pracy.

Pełny opis zasad i rozwiązań obowiązujących w Warszawskim Uniwersytecie Medycznym w obszarze ochrony danych osobowych opisany jest w:

1) Zarządzeniu Rektora nr 48 z dnia 23 maja 2018 roku;
2) Polityce bezpieczeństwa danych osobowych;
3) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4) Regulaminie organizacji i przetwarzania danych osobowych.

Wymienione wyżej dokumenty są dostępne dla każdego pracownika Uczelni.