Załącznik nr- 2 do Zarządzenia nr 41/2015 Rektora
Warszawskiego Uniwersytetu Medycznego
z dnia 28 maja 2015 r.

REGULAMIN

organizacji przetwarzania danych osobowych.

Załącznik – Ramowy schemat obiegu informacji i dokumentów w procesie przetwarzania danych osobowych w WUM

Regulamin organizacji przetwarzania danych osobowych, określa ogólne zasady, cele przetwarzania danych i wskazuje działania podejmowane przez Administratora Ochrony Danych oraz osoby przez niego upoważnione, w zakresie organizacji przetwarzania i ochrony danych osobowych w jednostkach Warszawskiego Uniwersytetu Medycznego (WUM). Regulamin został opracowany zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity - Dz. U. 2014, poz. 1182 z późn. zm.).

Rozdział 1
Postanowienia ogólne.

§ 1

1. Administrator może upoważnić osoby do wykonywania określonych czynności, znajdujących się w zakresie zadań Administratora.
2. Kontrola prawidłowości wykonywania czynności, o których mowa w ust. 1, należy do Administratora.

Rozdział 2.
Zasady przetwarzania danych osobowych.

§ 2

1. Dane osobowe są przetwarzane w WUM w celu realizacji zadań określonych przepisami prawa.
2. Cel, o którym mowa w ust. 1, należy osiągać przy zachowaniu szczególnej staranności w realizacji przedsięwzięć dotyczących ochrony interesów osób, których dane dotyczą.

§ 3

1. Zasadą obowiązującą w Uczelni jest zachowanie przez użytkowników w tajemnicy wszelkich informacji dotyczących danych osobowych oraz sposobów ich zabezpieczania.
2. Możliwość wystąpienia zagrożeń bezpieczeństwa danych przetwarzanych w systemach lub kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych nakłada na użytkowników i ich przełożonych obowiązek zapewnienia danym skutecznej ochrony.
3. 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.
4. Kopiowanie danych osobowych oraz wykonywanie wydruków jest zabronione chyba, że konieczność ich sporządzania wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.

§ 4

1. Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które posiadają upoważnienie do przetwarzania danych wydane przez Administratora lub osoby przez niego uprawnione jako LADO Formularz 4.7 (w załączniku nr 4 do zarządzenia).
2. Procedury nadawania, cofnięcia, zmiany upoważnień do przetwarzania danych osobowych w Uniwersytecie obejmują:
   1) złożenie przez kierownika wniosku o nadanie, wycofanie, zmianę upoważnienia do przetwarzania danych osobowych, zgodnie z wzorem zawartym formularzu nr 4.4;
   2) podpisanie - przez osobę ubiegającą się o nadanie upoważnienia - po uprzednim przeszkoleniu oświadczenia o zachowaniu w tajemnicy zasad przetwarzania danych oraz sposobów ich zabezpieczania, obejmującej także okres po ustaniu stosunku pracy, zgodnie z wzorem zawartym w formularzu nr 4.5;
   3) nadanie przez Administratora lub osobę przez niego uprawnioną (LADO), upoważnienia do przetwarzania danych osobowych, zgodnie z wzorem zawartym w formularzu nr 4.6.
3. Kopie upoważnień oraz inne dokumenty, w tym oryginał oświadczenia, o których mowa w ust. 2, przechowuje LADO, natomiast okresowa informacja powinna być przekazywana do ABI (PB). (Ramowy schemat obiegu informacji i dokumentów w procesie przetwarzania danych osobowych stanowi załącznik do Regulaminu).

4. Przełożony uprawnionego pracownika ma obowiązek realizacji procedur, o których mowa w ust. 2.
5. Kontrolę realizacji obowiązku, o którym mowa w ust. 1 prowadzi ABI w ramach sprawdzeń.

§ 5

1. Budynki, pomieszczenia lub ich część, w których przetwarzane są dane osobowe tworzą obszary przetwarzania danych osobowych w WUM. Przebywanie osób nieuprawnionych w tych obszarach jest ograniczone i odbywać się może tylko w obecności użytkowników i za zgodą przełożonych.
2. Administrator zapewnia ochronę obszarów przetwarzania danych osobowych w Uczelni, zgodnie z zasadami określonymi w Polityce bezpieczeństwa.
3. Do obszarów podlegających szczególnej ochronie Administrator zalicza serwerownie oraz pomieszczenia, w których przetwarzane są dane wrażliwe.

Rozdział 3
Procedury tworzenia, rejestrowania i dokonywania zmian w przetwarzaniu danych osobowych w zbiorach.

§ 6

1. Tworzy się zbiory danych osobowych przez nadanie danym osobowym odpowiedniej struktury, dostępnej według określonych kryteriów, niezależnie od tego, czy zestaw danych jest rozproszony lub podzielony funkcjonalnie.
2. Przetwarzanie danych osobowych może odbywać się metodą:
   1) papierową, w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych;
   2) informatyczną, w systemach informatycznych;
   3) poza zbiorem danych.
3. Zgodnie z potrzebami realizacji zadań służbowych, przełożeni użytkowników tworzą zbiory lub wnioskują o ich wycofanie (zmianę), według następujących reguł:
   1) nazwa zbioru powinna odzwierciedlać cel przetwarzania danych i być zgodna z nazewnictwem stosowanym w przepisach prawa;
   2) należy wskazać podstawy prawne do przetwarzania danych;
   3) należy określić sposób i miejsca przetwarzania danych oraz użytkowników;
   4) należy przekazać informację ABI w celu określenia poziomu bezpieczeństwa systemu, w którym przetwarzane są dane;
   5) należy zapewnić ochronę danym osobowym.

§ 7

1. Administrator ma obowiązek zgłosić do rejestracji w GIODO wyłącznie zbiory zawierające dane wrażliwe zgodnie z wzorem wniosku określonym w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.
2. LADO mają obowiązek zgłoszenia zbioru do rejestracji i przesłania go do ABI.
3. Zbiór zawierający dane wrażliwe można przetwarzać po potwierdzeniu przez GIODO jego zarejestrowania.
4. Wewnętrzny rejestr zbiorów danych osobowych przetwarzanych w WUM prowadzi ABI w formie papierowej.

Rozdział 4
Szkolenie oraz prowadzenie dokumentacji z zakresu przetwarzania danych osobowych.

§ 8

1. Każda osoba przed rozpoczęciem przetwarzania danych ma obowiązek zapoznania się z przepisami dotyczącymi bezpieczeństwa przetwarzania i ochrony danych osobowych. Przełożony zobowiązany jest umożliwiać podwładnym zapoznanie się z tymi przepisami.
2. W przypadku wdrażania w Uniwersytecie nowych procedur przetwarzania i ochrony danych osobowych, ABI na wniosek osób, o których mowa w § 9 ust 3, może polecić zorganizowanie dodatkowych szkoleń dla wskazanych przez przełożonych grup użytkowników.
3. Szkolenia, o których mowa w ust. 2, organizuje ABI we współpracy z Działem Personalnym i Kanclerzem WUM.

Rozdział 5.
Obowiązki osób upoważnionych przez Administratora.

§ 9

1. Administrator wykonuje zadania z zakresu przetwarzania i ochrony danych osobowych zgodnie z przepisami Ustawy.
2. Administrator stosuje środki techniczne i przedsięwzięcia organizacyjne zapewniające skuteczną realizację zadań w zakresie bezpieczeństwa i ochrony danych przetwarzanych w Warszawskim Uniwersytecie Medycznym.
3. Zadania, o których mowa w ust. 1, z upoważnienia Administratora wykonują:
   1) LADO;
   2) kierownicy jednostek organizacyjnych WUM w odniesieniu do danych osobowych przetwarzanych w swoich jednostkach;
   3) osoba upoważniona do wykonywania określonych zadań w imieniu Administratora.
4. Wzór upoważnienia, dla osób o których mowa w ust. 3 pkt 1, stanowi formularz nr 4.7 w załączniku nr 4 do Zarządzenia.

§ 10

1. Za organizację, koordynację, kontrolę i nadzór nad przestrzeganiem przepisów o ochronie danych osobowych w Uczelni odpowiada ABI na podstawie powołania przez Administratora.
2. Zadania ABI wynikające z przepisów prawa zostały określone w § 8 Polityki bezpieczeństwa.

§ 11

1. Pion eksploatacji podległy zastępcy kanclerza ds. eksploatacji oraz Dział Informatyki realizują czynności techniczne związane z zapewnieniem skutecznej fizycznej ochrony danym osobowym przetwarzanym w Uczelni.
2. Do zadań kierowników działów pionu eksploatacji należy zapewnienie technicznego zabezpieczenia i wyposażenia pomieszczeń i obiektów, które tworzą obszary przetwarzania danych ze szczególnym uwzględnieniem środków ochrony fizycznej, określonych w § 20 ust. 2 pkt. 3 i 5 Polityki Bezpieczeństwa, stanowiącej załącznik nr 1 do Zarządzenia.
3. Czynności, o których mowa w ust. 2, wykonuje się na wniosek ABI lub właściwego kierownika jednostki organizacyjnej WUM.

§ 12

1. Dział Informatyki realizuje czynności techniczne związane z zapewnieniem bezpieczeństwa przetwarzania danych osobowych w podległych systemach informatycznych.
2. Do zadań kierownika Działu Informatyki w szczególności należy:

1) wyznaczanie ASI (osoba lub zespół osób) do poszczególnych systemów informatycznych Uczelni - uwzględniając wielkość zbiorów i typologię systemów oraz nadzorowanie ich działalności;
2) dostosowywanie systemów do wymogów prawa;
3) planowanie i wdrażanie rozwiązań systemowych i technicznych elementów bezpieczeństwa danych przetwarzanych w systemach;
4) zapewnienie sprzętu i oprogramowania systemów, odpowiadających normom przewidzianym dla poziomów bezpieczeństwa przetwarzania danych w systemach;
5) nadzorowanie technicznego zabezpieczania i odpowiedniego wyposażenia pomieszczeń, w których znajdują się serwery.

§ 13

1. Kierownicy jednostek organizacyjnych WUM są odpowiedzialni za przestrzeganie przepisów dotyczących przetwarzania i ochrony danych osobowych w podległych im jednostkach w zakresie upoważnień nadanych przez Administratora.
2. Do zadań osób, o których mowa w ust. 1, należy:
   1) wnioskowanie do Administratora o udostępnianie danych osobowych w celach innych niż włączenie do zbioru;
   2) wnioskowanie o rejestrację (aktualizację) zbiorów wrażliwych danych osobowych przez GIODO - wypełnianie wniosków zgłoszenia;
   3) przedkładanie do Administratora lub LADO wniosków o nadanie (wycofanie) lub zmianę upoważnień do przetwarzania danych osobowych dla pracowników i innych osób;
   4) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;
   5) zabezpieczanie danych osobowych zgodnie z przepisami zawartymi w dokumentacji przetwarzania i ochrony danych osobowych;
   6) udzielanie informacji osobom, których dane są zbierane;
   7) wnioskowanie do Administratora o zawarcie umów dotyczących udostępniania lub powierzenia przetwarzania danych osobom i podmiotom zewnętrznym;
   8) wskazywanie osoby wykonującej w jednostce organizacyjnej czynności administracyjne związane z przetwarzaniem i ochroną danych osobowych;
   9) okresowe przekazywanie do ABI wykazu zbiorów danych i programów zastosowanych do ich przetwarzania oraz lokalizacji obszarów ich przetwarzania;
   10) w porozumieniu z ABI rozpatrywanie skarg i wniosków dotyczących przetwarzania i ochrony danych osobowych;
   11) na żądanie Administratora lub osoby przez niego upoważnionej przeprowadzenie okresowych analiz ryzyka dla poszczególnych systemów i na tej podstawie przedstawianie Administratorowi propozycji w zakresie stosowania środków technicznych i przedsięwzięć organizacyjnych w celu zapewnienia skutecznej ochrony przetwarzania danych;
   12) Osoby, o których mowa w ust. 1, realizując zadania w imieniu Administratora współpracują z ABI, kierownikami Działów Eksploatacji, kierownikiem Działu Informatyki oraz innymi osobami upoważnionymi przez Administratora.

§ 14

1. Osoby upoważnione do podpisywania umów z osobami lub podmiotami zewnętrznymi, o których mowa, w § 1 ust. 2 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, , zobowiązane są do umieszczania postanowień umownych, gwarantujących bezpieczeństwo i ochronę danych osobowych przetwarzanych w Uniwersytecie.
2. Postanowienia, o których mowa w ust. 1, dotyczą udostępniania lub powierzenia danych

do przetwarzania i zawierają:

1) określenie przedmiotu i celu umowy;
2) zobowiązanie zleceniobiorcy do zapewnienia bezpieczeństwa i właściwej ochrony przetwarzanych danych osobowych;
3) zobowiązanie zleceniobiorcy do przestrzegania procedur, o których mowa w § 6;
4) oświadczenie zleceniobiorcy dotyczące dostosowania systemów informatycznych wykorzystywanych w procesie przetwarzania danych osobowych do wymogów rozporządzenia, o którym mowa w § 15 ust. 2;
5) zapewnienie zleceniodawcy nadzoru i kontroli nad przetwarzaniem i ochroną danych osobowych;
6) określenie kar umownych za nieprzestrzeganie zapisów umownych;
7) możliwość rozwiązania umowy w trybie natychmiastowym w przypadku stwierdzenia omijania przez stronę umowy przepisów dotyczących bezpieczeństwa i ochrony przetwarzanych danych osobowych.

Rozdział 6
Postanowienia końcowe.

§ 15

W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie znajdują:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. 2014 r., poz. 1182 z póź. zm.);
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536).