Zarządzenie nr 22/2018
Rektora Uniwersytetu Medycznego w Białymstoku
z dnia 17.05.2018 r.
w sprawie wprowadzenia Polityki ochrony danych osobowych
w Uniwersytecie Medycznym w Białymstoku

Na podstawie art. 24 ust. 2 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 119 z 04.05.2016) zarządzam, co następuje:

§1

Wprowadzam Politykę Ochrony Danych Osobowych w Uniwersytecie Medycznym w Białymstoku, stanowiącą załącznik do niniejszego zarządzenia.

§2

Z dniem wejście w życie niniejszego zarządzenia:

1) dotychczasowy Pełnomocnik ds. Ochrony Danych Osobowych - Administrator Bezpieczeństwa Informacji staje się Inspektorem Ochrony Danych,
2) wszelkie umowy, projekty, procesy, wewnętrzne akty prawne wiążące się z przetwarzaniem danych osobowych powinny być konsultowane z Inspektorem Ochrony Danych.

§3

1. Upoważnienia do przetwarzania danych osobowych wydane przed dniem 25.05.2018 r. pozostają aktualne.
2. Oświadczenie o poufności podpisane przed dniem 25.05.2018 r. pozostają aktualne.
3. Zgody na przetwarzanie danych osobowych pobrane przed dniem 25.05.2018 r. pozostają aktualne, o ile spełniają wymagania ogólnego rozporządzenia o ochronie danych - RODO.

§4

W sprawach nieuregulowanych w niniejszej polityce zastosowanie mają przepisy 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.

§5

Z dniem wejścia w życie niniejszego zarządzenia traci moc Zarządzenie nr 36/16 Rektora UMB z dnia 29.06.2016 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Uniwersytecie Medycznym w Białymstoku, Zarządzenie nr 49/15 Rektora Uniwersytetu Medycznego w Białymstoku z dnia 10.11.2015 r. w sprawie ochrony danych osobowych przetwarzanych w Uniwersytecie Medycznym w Białymstoku oraz Zarządzenie nr 70/16 Rektora Uniwersytetu Medycznego w Białymstoku z dnia 2.12.2016 r. w sprawie wprowadzenia zmian do Zarządzenia nr 49/15.

§6

Z dniem wejścia w życie niniejszego zarządzenia, w zakresie nieuregulowanym w niniejszej polityce, aktualne pozostaje Zarządzenie nr 52/15 Rektora Uniwersytetu Medycznego w Białymstoku z dnia 25.11.2015 r. w sprawie wprowadzenia Regulaminu Ochrony Danych Osobowych w Uniwersytecie Medycznym w Białymstoku.

§7

Zarządzenie wchodzi w życie z dniem podpisania, z mocą obowiązującą od 25.05.2018 r.

Rektor

prof. dr hab. Adam Krętowski

Załącznik do Zarządzenia nr 22/2018 Rektora UMB z dnia 17.05.2018 r.

Polityka Ochrony Danych Osobowych w Uniwersytecie Medycznym w Białymstoku

Niniejsza Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Uniwersytet Medyczny w Białymstoku w celu spełnienia wymagań 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 – tzw. RODO).
Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

1. DEFINICJE

1) 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 jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej,
2) Przetwarzanie danych osobowych to 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,
3) podmiot danych - każda osoba fizyczna, która jest przedmiotem przetwarzanych danych,

4) Administrator Danych Osobowych (ADO) –Uniwersytet Medyczny w Białymstoku, reprezentowany przez Rektora - samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
5) Organ nadzorczy/UODO – Prezes Urzędu Ochrony Danych Osobowych, niezależny organ publiczny ustanowiony przez państwo członkowskie, zgodnie z art. 51 RODO, monitorujący stosowanie przepisów prawa z zakresu ochrony danych osobowych,
6) ograniczenie przetwarzania – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,
7) pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
8) podmiot przetwarzający (procesor) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych osobowych,
9) odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią,
10) strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe,
11) zgoda – dowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub innego wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,
12) system informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
13) incydent bezpieczeństwa – pojedyncze zdarzenie lub seria zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań Uniwersytetu lub mogą stanowić przyczynę utraty zasobów, reputacji, niezawodności systemów bezpieczeństwa, a także odstępstwa od obowiązujących procedur w zakresie bezpieczeństwa, nawet jeżeli nie prowadzą do wymienionych powyżej skutków,

14) naruszenie ochrony danych osobowych – 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,
15) dane szczególnych kategorii – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne, a także dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej,
16) dane dotyczące zdrowia – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia,
17) organizacja międzynarodowa – organizacja lub organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy, między co najmniej dwoma państwami lub na podstawie takiej umowy,
18) ochrona danych w fazie projektowania - zasada, zgodnie, z którą konieczne jest włączanie ochrony prywatności w samo tworzenie projektu, działanie jego składników oraz w zarządzanie technologiami informacyjnymi i systemami przez cały cykl życia informacji. W przypadku systemów teleinformatycznych oznacza to wbudowanie ochrony prywatności zarówno w architekturę systemu, jak i w procesy biznesowe, które system obsługuje, np. poprzez jak najszybszą pseudonimizację danych czy też umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych,
19) ochrona danych jako opcja domyślna – zasada, którą należy rozumieć jako postulat uwzględnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu. Domyślnie, czyli bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą – i to w kluczowym dla użytkownika momencie przyłączenia się do danego systemu. Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane,
20) anonimizacja- zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych,
21) ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące, 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,

22) 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.

2. REJESTR CZYNNOŚCI PRZETWARZANIA

1) Rejestr czynności przetwarzania prowadzony jest przez Inspektora Ochrony Danych Osobowych na podstawie art. 30 ust 1 RODO.
2) W rejestrze są uwzględniane wszystkie czynności przetwarzania danych osobowych Uczelni jako administratora danych.
3) Rejestr czynności przetwarzania jest na bieżąco aktualizowany na podstawie informacji przekazywanych Inspektorowi Ochrony Danych przez kierowników jednostek organizacyjnych Uczelni.
4) Wzór rejestru czynności przetwarzania stanowi załącznik nr 1 do niniejszej polityki.

3. REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA – PODMIOT PRZETWARZAJĄCY

1) Rejestr kategorii czynności przetwarzania prowadzony jest przez Inspektora Ochrony Danych Osobowych na podstawie art. 30 ust 2 RODO.
2) W rejestrze są uwzględniane wszystkie kategorie czynności przetwarzania danych osobowych realizowane przez Uczelnię jako podmiotu przetwarzającego czyli powierzone do przetwarzania Uczelni przez inne podmioty.
3) Rejestr jest na bieżąco aktualizowany na podstawie informacji przekazywanych do Inspektora Ochrony Danych przez kierowników jednostek organizacyjnych Uczelni.
4) Wzór rejestru kategorii czynności przetwarzania stanowi załącznik nr 2 do niniejszej polityki.

4. INFORMACJE PODAWANE W PRZYPADKU ZBIERANIA DANYCH OD OSOBY, KTÓREJ DANE DOTYCZĄ

1) Na podstawie art. 13 RODO wobec wszystkich osób, od których zbierane są dane osobowe w Uczelni, w szczególności pracowników, osób ubiegających się o zatrudnienie, studentów, doktorantów, osób ubiegających się o przyjęcie na studia, zleceniobiorców, kontrahentów będących osobami fizycznymi i innych osób, od których Uczelnia zbiera dane wykonuje się tzw. obowiązek informacyjny.
2) Wzór klauzuli informacyjnej stanowi załącznik nr 3 do niniejszej polityki.

5. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1) Każda osoba w Uczelni przetwarza dane wyłącznie na polecenie (upoważnienie) administratora.
2) Każda osoba upoważniona powinna podpisać oświadczenie o zachowaniu w poufności danych osobowych.
3) Każda osoba mająca dostęp do pomieszczeń przy wykonywaniu czynności zleconych w obszarze przetwarzania danych osobowych (sprzątanie pomieszczeń, konserwacja infrastruktury znajdującej się w obszarze przetwarzania danych osobowych, serwis sprzętu) powinna podpisać oświadczenie o zachowaniu poufności.
4) Procedura nadawania upoważnień do przetwarzania danych wraz z wzorami: upoważnienia, oświadczeń i ewidencji osób upoważnionych stanowi załącznik nr 4 do niniejszej polityki.
5) Każdy pracownik powinien zapoznać się z zasadami ochrony danych osobowych. Materiały szkoleniowe stanowią Załącznik nr 5 do polityki.

6. UMOWY POWIERZENIA DANYCH OSOBOWYCH

1) Uczelnia z podmiotami przetwarzającymi zawiera zgodnie z art. 28 RODO umowy powierzenia.
2) Do umów, porozumień itp. które związane są z powierzeniem danych osobowych podmiotom zewnętrznym kierownik jednostki organizacyjnej przygotowuje do umowy dodatkowo umowę powierzenia danych osobowych.
3) Wzór umowy powierzenia stanowi Załącznik nr 6 do polityki.
4) Wykaz podmiotów przetwarzających prowadzony jest w Załączniku nr 7 Rejestr umów powierzenia.

5) Dopuszcza się niezawieranie odrębnych umów powierzenia lub poufności, jeśli w umowie, porozumieniu itp. z podmiotem zawarte będą wszystkie niezbędne zapisy dotyczące kwestii powierzenia danych osobowych.

7. INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

1) Instrukcja dotyczy podatności oraz 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.
2) Każdy pracownik zobowiązany jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu przełożonemu i Inspektorowi Ochrony Danych.
3) Do typowych podatności bezpieczeństwa danych osobowych należą:
    a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, sprzętu i dokumentów,
    b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
4) Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
    c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5) W przypadku stwierdzenia wystąpienia incydentu Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające podczas którego:
    a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
    b) inicjuje ewentualne działania dyscyplinarne,
    c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
    d) rekomenduje działania zapobiegawcze zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

6) Administrator dokumentuje naruszenia ochrony danych osobowych w rejestrze, stanowiący Załącznik nr 8 do polityki.
7) W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych.

8. AUDYTY

1) Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2) Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO.
3) IOD jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych.
4) IOD opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
5) Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.
6) W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia.
7) Wynik audytu zostaje udokumentowany przez audytora i przekazany Administratorowi.
8) IOD decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

9. ANALIZA RYZYKA

Analiza ryzyka jest przeprowadzana w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. W Uczelni analizę ryzyka w obszarze bezpieczeństwa informacji przeprowadza się raz w roku stosując zasady określone w Zarządzeniu Rektora nr 11/11 z dnia 7.3.2011 r. w sprawie ustalenia zasad kontroli zarządczej w UMB. Wszędzie, gdzie

Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.

10. OCENA SKUTKÓW DLA OCHRONY DANYCH I UPRZEDNIE KONSULTACJE

1) Administrator danych dokonuje, przed rozpoczęciem przetwarzania danych, oceny skutków planowanych operacji przetwarzania dla ochrony danych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, których dane dotyczą. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2) Dokonując oceny skutków dla ochrony danych, administrator danych konsultuje się z Inspektorem Ochrony Danych Osobowych.

11. WYKAZ ZABEZPIECZEŃ

W celu ochrony danych osobowych w Uczelni stosuje się zabezpieczenia fizyczne, organizacyjne i techniczne, które określone są w odrębnych zarządzeniach.

REKTOR
prof. dr hab. Adam Krętowski

Załącznik nr 1 do

Polityki Ochrony Danych Osobowych

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA

ADMINISTRATORA DANYCH na podstawie art. 30 ust. 1 RODO

Nazwa i dane kontaktowe administratora:

Uniwersytet Medyczny w Białymstoku, ul. Kilińskiego 1, 15-089 Białystok, reprezentowany przez Rektora

Dane kontaktowe Inspektora Ochrony Danych Osobowych:

.....

Opis kategorii osób, których dane dotyczą	
Nazwa czynności przetwarzania	
Opis kategorii danych osobowych	
Cele przetwarzania	
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	
Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
Nazwa państwa trzeciego lub organizacji międzynarodowej, gdy mają zastosowanie tam przekazania danych osobowych	
Planowane terminy usunięcia poszczególnych kategorii danych	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	

Załącznik nr 2 do

Polityki Ochrony Danych Osobowych

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA PROWADZONEGO PRZEZ PODMIOT PRZETWARZAJĄCY

na podstawie art. 30 ust. 2 RODO

Dane kontaktowe Inspektora Ochrony Danych Osobowych:

.....

Nazwa oraz dane kontaktowe podmiotu przetwarzającego	
Nazwa oraz dane kontaktowe administratora, w imieniu którego działa podmiot przetwarzający	
Opis kategorii przetwarzań dokonywanych w imieniu administratora	
Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
Nazwa państwa trzeciego lub organizacji międzynarodowej, gdy mają zastosowanie tam przekazania danych osobowych	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	

Załącznik nr 3 do
Polityki Ochrony Danych Osobowych

Wzór klauzuli informacyjnej

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016 r.) informuję, iż:

1) Administratorem Danych Osobowych jest Uniwersytet Medyczny Białymstoku z siedzibą ul. Kilińskiego 1, 15-089 Białystok, reprezentowany przez Rektora,
2) Kontakt do Inspektora Ochrony Danych w Uniwersytecie Medycznym w Białymstoku - adres email: emilia.minasz@umb.edu.pl,
3) Pani/Pana dane osobowe przetwarzane będą w celu */ wpisać cel/* na podstawie Art. 6 ust. 1 lit. *a, b, c, d, e, f /wybrać właściwy/**- ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
   ***w przypadku wybrania f) wymienić prawnie uzasadnione interesy*
4) ***odbiorcami Pani/Pana danych osobowych będą *(podać nazwę odbiorców lub kategorię odbiorców),*
5) Pani/Pana dane osobowe przechowywane będą przez okres .....*dni/lat*,
6) posiada Pani/Pan prawo do: żądania od Administratora Danych dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych
7) *posiada Pani/Pan prawo do cofnięcia zgody w każdym momencie - /dotyczy tylko sytuacji gdy w pkt 3) był wpisany Art. 6 ust. 1 lit. a czyli gdy dane przetwarzamy na podstawie zgody osoby/*
8) *Pani/Pana dane osobowe mamy zamiar przekazywać do państwa trzeciego lub organizacji międzynarodowej – /gdy ma to zastosowanie/,*
9) *****Pani/Pana dane osobowe będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu /gdy ma to zastosowanie/,*
10) ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzasadnione jest, że Pani/Pana dane osobowe przetwarzane są przez Administratora Danych niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
11) podanie danych osobowych jest *****dobrowolne, ale konieczne do realizacji celu przetwarzania / obligatoryjne na mocy przepisu prawa */podać przepis/*.

wyjaśnienia:

**Art. 6 ust. 1 Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:*
a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

***w przypadku wybrania f) wymienić prawnie uzasadnione interesy*

****„odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

„strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

*****„profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które 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;

****** *właściwe wybrać, jeśli wybierzesz na podstawie przepisów prawa podać przepis*

Załącznik nr 4 do
Polityki Ochrony Danych Osobowych

Procedura nadawania upoważnień do przetwarzania danych osobowych w Uniwersytecie Medycznym w Białymstoku

§1

1. Proces nadawania upoważnień odbywa się w formie elektronicznej w systemie EZD, z zastrzeżeniem ust. 2.
2. W przypadkach, gdy niezbędna jest wersja papierowa, sprawa może być prowadzona w wersji papierowej.
3. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do procedury, z zastrzeżeniem §2 ust. 5.
4. Upoważnienie do przetwarzania danych osobowych wydawane jest w następujących przypadkach:

1) zatrudnienia nowego pracownika,
2) zmiany stanowiska pracy na inne stanowisko, co jest związane ze zmianą zakresu uprawnień,
3) zmiany miejsca pracy na inną jednostkę organizacyjną, co jest związane ze zmianą zakresu uprawnień,
4) powołania pracownika do zespołu projektu/komisji itp. której praca wiąże się z przetwarzaniem danych osobowych.

§2

1. Upoważnienia pracownikom administracji przygotowują ich przełożeni.
2. Upoważnienia pracownikom jednostek naukowo – dydaktycznych oraz pracownikom zatrudnionym na samodzielnych stanowiskach w Uczelni przygotowuje kierownik Działu Spraw Pracowniczych lub wyznaczony pracownik, na podstawie wniosku przełożonego zatrudnianego pracownika.
3. Zakres upoważnienia musi być zgodny z zakresem czynności, jakie wykonuje pracownik.
4. Upoważnienia do przetwarzania danych osobowych w ramach projektów prowadzonych przez jednostki organizacyjne Uczelni przygotowywane są przez pracowników tych jednostek.
5. W przypadku, gdy projekt określa wzór upoważnienia, upoważnienie jest wydawane według określonego wzoru.
6. Upoważnienia do przetwarzania danych, osobom powoływanym w Uczelni do komisji, zespołów itp. których prace związane są z przetwarzaniem danych osobowych przygotowywane są przez osoby zajmujące się obsługą organizacyjną tych komisji, zespołów.
7. Upoważnienia do przetwarzania danych osobowych akceptuje/podpisuje Rektor lub osoba upoważniona przez Rektora.
8. Pracownicy przygotowujący upoważnienia, nadają upoważnieniu znak sprawy, przekazują do akceptacji/podpisu Rektora lub upoważnionej osoby, przechowują upoważnienia i archiwizują je.
9. Pracownicy, o których mowa w ust. 4 i 6 niniejszego paragrafu, prowadzą rejestry osób upoważnionych.

§3

Rejestr osób upoważnionych do przetwarzania danych osobowych po dniu 25.05.2018 r. prowadzony jest przez Inspektora Ochrony Danych Osobowych, za wyjątkiem rejestrów w ramach realizowanych projektów oraz w ramach powoływanych komisji/zespołów, które znajdują się we właściwych jednostkach.

§4

1. Przed przystąpieniem do przetwarzania danych każdy pracownik zapoznaje się z przepisami o ochronie danych w UMB. Materiały szkoleniowe udostępniane są pracownikowi w Dziale Spraw Pracowniczych.
2. Każda osoba upoważniona do przetwarzania danych osobowych w momencie podpisywania umowy o pracę podpisuje również w Dziale Spraw Pracowniczych oświadczenie o zachowaniu w poufności danych osobowych (Załącznik nr 2 lub Załącznik nr 3 do procedury). Oświadczenie przechowuje się w aktach osobowych pracownika.

§5

1. Upoważnienia wygasają z chwilą ustania zatrudnienia w Uniwersytecie Medycznym w Białymstoku. Informację o dacie ustania zatrudnienia kierownik Działu Spraw Pracowniczych lub upoważniona osoba przekazuje do Inspektora Ochrony Danych Osobowych lub właściwej jednostki, celem odnotowania jej w rejestrze, z zastrzeżeniem ust. 2.
2. Upoważnienia obowiązują do dnia odwołania. Proces odwołania upoważnienia jest taki sam jak nadania upoważnienia.

§6

1. Upoważnienia do przetwarzania danych osobowych nadane przed dniem 25.05.2018 r. oraz oświadczenia podpisane przed dniem 25.05.2018 r. zachowują swoją ważność i znajdują się u Inspektora Ochrony Danych.
2. Rejestr osób upoważnionych do przetwarzania danych osobowych przed dniem 25.05.2018 r. znajduje się u Inspektora Ochrony Danych Osobowych.

Załączniki do procedury:

1. Wzór upoważnienia do przetwarzania danych osobowych
2. Oświadczenie o poufności – osoby przetwarzające dane
3. Oświadczenie o poufności – osoby mające dostęp do pomieszczeń, w których są dane
4. Wzór ewidencji osób upoważnionych

Załącznik nr 1 do
Procedury nadawania upoważnień
do przetwarzania danych osobowych

Białystok, dnia: .....

Upoważnienie/Odwołanie upoważnienia nr: do przetwarzania danych osobowych

Na podstawie art. 29 i art. 32 ust. 4 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. upoważniam Panią/Pana **/imię i nazwisko/** pracownika do przetwarzania następujących danych osobowych, w systemie informatycznym i w zbiorze papierowym, w zakresie wykonywanych obowiązków służbowych na zajmowanym stanowisku:

** [ ] Pracownicy UMB
[ ] Pracownicy podległej jednostki organizacyjnej UMB
[ ] Byli pracownicy
[ ] Emeryci i renciści
[ ] Umowy cywilnoprawne
[ ] Rekrutacja pracowników
[ ] Studenci
[ ] Doktoranci
[ ] Uczestnicy studiów podyplomowych
[ ] Kandydaci na studia
[ ] Absolwenci
[ ] Korespondencja wychodząca i przychodząca (adresaci i nadawcy)
[ ] Monitoring wizyjny
[ ] Skargi
[ ] Dobrowolni donatorzy zwłok ludzkich
[ ] Osoby korzystające z Biblioteki i czytelni
[ ] Goście hotelowi
[ ] Mieszkańcy domów studenta
[ ] Kontrahenci
[ ] Osoby ubiegające się o nostryfikacje
[ ] Osoby ubiegające się o przeniesienie na studia
[ ] Osoby ubiegające się o nadanie stopni i tytułów naukowych
[ ] Uczestnicy konferencji
[ ] Uczestnicy kursów specjalizacyjnych
[ ] Zamówienia publiczne
[ ] Archiwum
[ ] Wymiana międzynarodowa
[ ] Uczestnicy badań naukowych
[ ] innych (wpisać jakich) .....

Upoważnienie obowiązuje do dnia odwołania lub wygasa z chwilą ustania zatrudnienia w Uniwersytecie Medycznym w Białymstoku.

** wpisać numer upoważnienia*
***właściwe zaznaczyć*

Załącznik nr 2 do
Procedury nadawania upoważnień
do przetwarzania danych osobowych

Imię Nazwisko

Białystok, dnia .....

OŚWIADCZENIE

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz wewnętrznymi aktami prawnymi obowiązującymi w Uczelni w tym zakresie.

W szczególności zobowiązuję się do:

1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych zadaniach,
2) zachowania w tajemnicy danych osobowych, do których mam lub będę mieć dostęp w związku z wykonywaniem zadań, zarówno w trakcie jak i po ustaniu realizacji zadań,
3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań,
4) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
5) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem przetwarzaniem, w tym zniszczeniem, utratą, modyfikacją, nieuprawnionym dostępem do danych lub ujawnieniem.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

Imię Nazwisko

.....
czytelny podpis

Załącznik nr 3 do
Procedury nadawania upoważnień
do przetwarzania danych osobowych

Imię Nazwisko

Białystok, dnia .....

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz Polityką ochrony danych osobowych obowiązującą w Uniwersytecie Medycznym w Białymstoku.

W szczególności zobowiązuję się do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas wykonywania czynności służbowych (sprzątanie pomieszczeń, konserwacja infrastruktury, ochrona obiektów i pomieszczeń),
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu i Inspektorowi Ochrony Danych Osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

Imię Nazwisko

.....
czytelny podpis oświadczającego

Załącznik nr 4 do
Procedury nadawania upoważnień
do przetwarzania danych osobowych

Ewidencja Osób upoważnionych

Numer	Jednostka organizacyjna	Nazwisko i imię	Data wydania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia
1					
2					

Załącznik nr 5
do Polityki Ochrony
Danych Osobowych

Nowe unijne rozporządzenie dotyczące danych osobowych tzw. RODO

Szkolenie wewnętrzne
dla pracowników Uniwersytetu Medycznego
w Białymstoku

Opracowała:
Emilia Minasz

1

REFORMA PRZEPISÓW O OCHRONIE DANYCH

- 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 osobowych) tzw. RODO
- Zapisy RODO mają być wdrożone w Uczelni do 25 maja 2018 r. Tego dnia już należy stosować RODO bez okresu przejściowego

2

ROZPORZĄDZENIE UNIJNE

- ujednolicenie zasad ochrony danych osobowych w krajach Unii Europejskiej
- zwiększenie praw osób, których dane są przetwarzane
- nowe zasady
- nowe obowiązki

3

NOWE PODEJŚCIE DO OCHRONY DANYCH

- nie zmieniają się w sposób istotny podstawy prawne i zasady przetwarzania danych
- rewolucyjny charakter ma wprowadzenie nowych zasad, które zwiększają samodzielność ale i odpowiedzialność Uczelni.
- za przestrzeganie rozporządzenia i wykazanie jego przestrzegania odpowiedzialny jest administrator danych.
- **rozliczalność** - administrator samodzielnie decyduje jakie środki bezpieczeństwa wdrożyć by zapewnić zgodność przetwarzania danych z wymogami rozporządzenia (uwzględniając aktualny stan wiedzy technicznej, koszt wdrażania, oraz charakter, zakres i cel przetwarzania) ale musi być w stanie wykazać że przetwarza jest bezpiecznie i zgodnie z RODO

4

INSPEKTOR OCHRONY DANYCH

- Od 25 maja 2018 nie będzie ABI
- Będzie Inspektor ochrony danych danych osobowych
- Włączanie inspektora we wszystkie procesy, w których przetwarzane są dane osobowe
- Zadania Inspektora:
  - informowanie o obowiązkach wynikających z RODO i doradzanie w tej sprawie,
  - monitorowanie przestrzegania RODO oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia oraz audyty,
  - udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
  - współpraca i konsultacje z organem nadzorczym,
  - punkt kontaktowego dla organu nadzorczego i osób, których dane przetwarzamy.

5

UPRAWNIENIA OSÓB, KTÓRYCH DANE DOTYCZĄ

- prawo do bycia poinformowanym o operacjach przetwarzania
- prawo dostępu
- prawo do przenoszenia danych
- prawo do sprostowania/uzupełnienia danych
- prawo do usunięcia danych (prawo do bycia zapomnianym)
- prawo do ograniczenia przetwarzania
- prawo do sprzeciwu
- prawo do tego, by nie podlegać profilowaniu

6

NOWE OBOWIĄZKI INFORMACYJNE

Większy nacisk na realizację obowiązku informacyjnego - zwiększenie zakresu informacji, jakie należy przekazać osobom, których dane są pozyskiwane. Rozbudować klauzule informacyjne o:

- dane kontaktowe inspektowa ochrony danych osobowych,
- podstawa prawna przetwarzania i okres, przez który dane osobowe będą przetwarzane
- informacje o prawie do żądania usunięcia danych, ograniczenia przetwarzania, do przenoszenia danych, cofnięcia zgody,
- informacje o profilowaniu,
- informacje o prawie wniesienia skargi do UODO

7

DANE WRAŻLIWE w RODO

Poszerzenie definicji danych wrażliwych:

Dane wrażliwe to szczególna kategoria danych:

- dane dotyczące zdrowia fizycznego i psychicznego (*ZFŚS, dane medyczne, stopień niepełnosprawności*, o korzystaniu z usług opieki zdrowotnej, ryzyko choroby)
- dane genetyczne (*DNA, próbki biologiczne*)
- dane biometryczne (*wizerunek lub dane daktyloskopijne*)
- wyroki skazujące i naruszenia prawa,
- przynależność związkowa, polityczna, religijna, rasowa

8

JAK WYKONAĆ OBOWIĄZEK INFORMACYJNY

Klauzulę można wpisać:

- w umowie
- w formularzu, na kwestionariuszu
- na stronie internetowej, w BIP
- na internetowym formularzu rejestracyjnym

9

ZAPEWNIENIE LEGALNOŚCI

- przetwarzanie jest legalne gdy osoba wyrazi na to zgodę
- legalność w celu realizacji umowy
- przetwarzanie jest legalne, gdy jest niezbędne do wypełnienia obowiązku prawnego (np. Kodeks Pracy)
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby (np. klęski żywiołowe, humanitarne)
- przetwarzanie w interesie publicznym lub w ramach sprawowania władzy publicznej (np. działalność fundacji, opieki zdrowotnej)
- przetwarzane na podstawie prawnie uzasadnionych interesów administratora i strony trzeciej (np. marketing bezpośredni własnych produktów, monitoring, rejestr korespondencji, współpracownicy)

10

PRZYKŁADY ZGÓD
SPOSOBY DOKUMENTOWANIA ZGODY

PRZYKŁADY ZGÓD

- na przetwarzanie danych w cv w celach rekrutacyjnych
- na uczestnictwo w konkursie
- na udostępnienie danych innym podmiotom
- na publikację wizerunku w mediach i w internecie

SPOSOBY DOKUMENTOWANIA ZGODY

- podpis osoby
- mail
- zaznaczenie checkboxa na formularzu internetowym

11

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Zgoda jest jedną z kilku równoważnych podstaw prawnych do przetwarzania danych osobowych

Zgoda – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osobie w formie oświadczenia lub wyraźnego działania potwierdzającego.

- zgoda nie może być domniemana lub dorozumiana
- musi być dobrowolna, świadoma, konkretny cel (jeden cel – jedna zgoda)
- przedstawiona w sposób wyraźnie odróżniający ją od pozostałych kwestii
- zrozumiała, łatwo dostępna forma, jasny, prosty język
- każda osoba musi mieć pewność komu i na co wyraża zgodę
- okienka domyślnie zaznaczone lub niepodjęcie działania nie oznaczają zgody
- możliwość odwołania zgody

12

OGÓLNE WYTYCZNE (ZASADY) DOTYCZĄCE PRZETWARZANIA DANYCH W RODO

- **zgodność z prawem, rzetelność i przejrzystość** -przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
- **ograniczenie celu** - zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (*dalsze przetwarzanie w calach archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami)*
- **minimalizacja danych** - adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
- **prawidłowość** - 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,

13

OGÓLNE WYTYCZNE (ZASADY) DOTYCZĄCE PRZETWARZANIA DANYCH W RODO

- **ograniczenie przechowywania** -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; *(dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą,*
- **integralność i poufność** - 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

14

PRIVACY BY DESIGN , PRIVACY BY DEFAULT

- **ochrona danych w fazie projektowania** - uwzględnienie ochrony danych w fazie projektowania, wbudowanie ochrony prywatności w każdy nowy projekt, w jego konstrukcję, w architekturę systemu informatycznego, w procesy biznesowe poprzez np. jak najszybszą pseudonimizację danych, wbudowanie ochrony prywatności w przepisy wewnętrzne, w przetargi publiczne

- **ochrona danych jako opcja domyślna**, jak najdalej posunięte zabezpieczenia prywatności w ustawieniach początkowych każdego systemu, domyślnie czyli bez jakiejkolwiek aktywności osób w momencie przyłączania się do systemu, minimalizacja danych – tylko przetwarzane są te dane które są niezbędne do osiągnięcia celu, dla którego zostały zebrane

15

PROPONOWANE ZABEZPIECZENIA

Nie ma szczegółowych wskazówek jakie środki techniczne wdrożyć

Stosujemy zabezpieczenia wynikające z oceny ryzyka – rozliczani będziemy z ich stosowania , więc musimy je uzasadnić

Proponowane zabezpieczenia:

- zabezpieczenia chroniące dane przez utratą, zniszczeniem, modyfikacją, nieuprawnionym dostępem lub ujawnieniem
- działania przywracające dostępność danych po incydencie (np. procedura postępowania po krytycznej awarii serwera, krytycznym ataku sieciowym, ataku wirusów szyfrujących dane)
- regularne testy, mierzenie i oceny skuteczności zabezpieczeń (audyty IT, ewidencja włamań, testy hackerskie)
- pseudonimizacja i szyfrowanie danych

16

DOKUMENTACJA CZYNNOŚCI PRZETWARZANIA DANYCH

Rejestr czynności przetwarzania danych osobowych

- obowiązek prowadzenia wewnętrznego rejestru czynności przetwarzania danych
- rejestr tworzy Inspektor ochrony na podstawie informacji od jednostek organizacyjnych Uczelni
- rejestr – pomocne narzędzie przy w stosowaniu zasady rozliczalności
- przez rejestr rozumieć można klasyfikowanie przetwarzanych danych ze względu na m.in. zakres przetwarzanych danych, cele przetwarzania, kategorie osób, których dane dotyczą czy środki bezpieczeństwa

17

ANALIZA RYZYKA

Ryzyko może prowadzić m.in. do kradzieży tożsamości, straty majątkowej, naruszenia dóbr osobistych

- istotne jest ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
- koncepcja uwzględniania w każdym procesie przetwarzania ryzyka dla praw i wolności, jakie może nieść przetwarzanie i każdorazowo dostosowywanie wykorzystywanych narzędzi zabezpieczających dane do tego ryzyka; stopień zabezpieczeń ma odpowiadać stwierdzonemu ryzyku

18

OCENA SKUTKÓW DLA OCHRONY DANYCH

- wymagana jest jeśli operacje przetwarzania danych mogą powodować wysokie ryzyko naruszenia prywatności osób, których dane dotyczą: np. przy użyciu nowych technologii, użyciu zautomatyzowanych procesów przetwarzania danych, w tym profilowania, przetwarzania na dużą skalę szczególnych kategorii danych np. danych na temat zdrowia
- na etapie projektowania; powinna obejmować planowane operacje i cele przetwarzania, oceny jego niezbędności i proporcjonalności zabezpieczenia i mechanizmy mające minimalizować ryzyko, realna ocena ryzyk, umożliwiająca administratorom podejmowanie działań mających na celu ich rozwiązanie
- konsultacja z organem nadzorczym - gdy administrator danych nie może w wystarczającym stopniu zniwelować zidentyfikowanego ryzyka (znaleźć wystarczających środków) lub mimo zastosowania środków, ryzyko jest nadal wysokie

19

POWIERZENIE DANYCH

- większa odpowiedzialność za wybór podmiotu, któremu powierzamy dane
- na podmiocie, któremu powierzamy dane spoczywają bardzo podobne obowiązki jak na administratorze
- umowa powierzenia
- konieczność uwzględnienia w umowach relacji z dalszymi przetwarzającymi
- pisemna zgoda administratora danych na podpowierzanie

20

AUTOMATYCZNE PRZETWARZANIE DANYCH OPARTE NA PROFILOWANIU

- ocena czynników osobowych osoby fizycznej
- analiza i wyciąganie wniosków z zebranych danych
- profilowanie jest możliwe:

- kiedy jest to niezbędne do zawarcia lub wykonania umowy
- przepis prawa na to zezwala
- osoba, której dane dotyczą, udzieliła wyraźnej zgody
- poinformować osobę o fakcie profilowania i konsekwencjach tego

21

NARUSZENIA OCHRONY DANYCH

- wszelkie naruszenia zgłaszać do ABI
- naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

Nowy obowiązek zgłaszania naruszeń:

- administrator zgłasza do organu nadzorczego, że doszło do naruszenia ochrony danych osobowych (nie później niż 72 h od stwierdzenia naruszenia)

- administrator zawiadamia osoby, których dane dotyczą o naruszeniu
- zgłoszenie dotyczy tych incydentów, które mogą skutkować ryzykiem naruszenia praw i wolności osób (np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych)

22

Administracyjne kary pieniężne za naruszenia RODO

W podmiotach publicznych kary będą wynosiły do 100 000 zł

Kary:
- za naruszenia – wysokość uzależniona od tego jakie to naruszenie
- za niezgłoszenie naruszenia do organu nadrzędnego

23

ABI kontakt:

Pytania i wątpliwości dotyczące ochrony danych osobowych proszę kierować do Administratora Bezpieczeństwa Informacji (ABI)/przyszłego Inspektora Ochrony Danych Osobowych

ABI – Emilia Minasz

Tel. 7485414

email: emilia.minasz@umb.edu.pl

24

Załącznik nr 6 do

Polityki Ochrony Danych Osobowych

Umowa powierzenia przetwarzania danych osobowych,
zwana dalej „Umową"
zawarta w Białymstoku w dniu .....

pomiędzy:
Uniwersytetem Medycznym w Białymstoku, ul. Kilińskiego 1, 15 – 089 Białystok, zwanym w dalszej części umowy „Administratorem danych" reprezentowanym przez .....
a
.....zwanym dalej „Podmiotem przetwarzającym"

§1

Przedmiot, zakres i cel przetwarzania danych

1. Przedmiotem umowy jest powierzenie przez Uniwersytet Medyczny w Białymstoku danych osobowych do przetwarzania Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") na zasadach i w celu określonym w niniejszej umowie.
2. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy dane wyłącznie w celu ..... *(*należy podać cel przetwarzania danych) np. realizacji umowy z dnia ..... nr ....*, powierzone na podstawie umowy dane
   **pracowników, studentów lub inne wymienić*
   **dane zwykłe lub/i dane szczególnych kategorii*
   **w zakresie niezbędnym do realizacji umowy lub wymienić np. w zakresie imienia, nazwiska, PESEL itd.)*
   zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. *Na powierzonych danych osobowych mogą być wykonywane następujące czynności przetwarzania:*
   ** jeśli można określić to wymienić konkretne czynności*

§2

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.

4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy przetwarzanych danych oraz sposobów ich zabezpieczenia przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa.
6. Podmiot przetwarzający zobowiązuje się stosować ochronę powierzonych danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) za pomocą odpowiednich środków technicznych lub organizacyjnych.
7. Podmiot przetwarzający zobowiązuje się do pomocy Administratorowi danych w niezbędnym zakresie w wywiązywaniu się z obowiązków odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

§3

Zgłaszanie naruszeń

1. Podmiot przetwarzający zobowiązuje się po stwierdzeniu naruszenia ochrony danych osobowych do zgłoszenia tego Administratorowi danych bez zbędnej zwłoki, nie później niż w ciągu 24 godzin.
2. Informacja przekazana Administratorowi danych powinna zawierać co najmniej:
   a) opis charakteru naruszenia oraz - o ile to możliwe - wskazanie kategorii i przybliżonej liczby osób, których dane zostały naruszone i ilości/rodzaju danych, których naruszenie dotyczy,
   b) opis możliwych konsekwencji naruszenia,
   c) opis zastosowanych lub proponowanych do zastosowania przez Podmiot przetwarzający środków w celu zaradzenia naruszeniu, w tym minimalizacji jego negatywnych skutków.

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7-dniowym jego uprzedzeniem.
3. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów.

4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w§5 ust.1 umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych powierzonych przez Administratora danych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych.

§7

Czas obowiązywania umowy

Rozwiązanie umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od ..... do ..... .*
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem miesięcznego okresu wypowiedzenia.
3. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z umową;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

4. Podmiot przetwarzający uprawniony jest do przetwarzania powierzonych danych do dnia wygaśnięcia lub rozwiązania umowy.
5. W terminie 14 dni od ustania umowy, Podmiot przetwarzający zobowiązany jest do *_usunięcia/zwrócenia_ powierzonych danych, ze wszystkich nośników, programów, aplikacji w tym również kopii, chyba że obowiązek ich dalszego przetwarzania wynika z odrębnych przepisów prawa.

§8

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy prawa powszechnie obowiązującego, w tym Rozporządzenia.
3. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.

Administrator danych	Podmiot przetwarzający

* wybrać właściwe

Załącznik nr 7 do
Polityki Ochrony Danych Osobowych

Wzór rejestru umów powierzenia

L.p.	Nazwa administratora	Numer umowy powierzenia	Kategoria osób których dane dotyczą	Zakres czynności przetwarzania

Załącznik nr 8 do
Polityki Ochrony Danych Osobowych

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW BEZPIECZEŃSTWA DANYCH

L.p.	Opis	Źródło i data zgłoszenia	Działania naprawcze	Data rozpoczęcia i zakończenia działań	Osoba odpowiedzialna za realizację	Działania zapobiegające na przyszłość