INSTYTUT MEDYCYNY DOŚWIADCZALNEJ I KLINICZNEJ
im. Mirosława Mossakowskiego
Polskiej Akademii Nauk
02-106 Warszawa, ul. A. Pawińskiego 5
tel. 22 668-52-50, fax 22 668-55-32
NIP 525-000-81-69, REGON 000326463

Zarządzenie Nr 16/2018

Dyrektora Instytutu Medycyny Doświadczalnej i Klinicznej
im. M. Mossakowskiego
Polskiej Akademii Nauk

z dnia 03.09.2018 r.

**w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji"
w Instytucie Medycyny Doświadczalnej i Klinicznej
im. M. Mossakowskiego Polskiej Akademii Nauk**

Niniejszym Zarządzeniem wprowadzam „Politykę Bezpieczeństwa Informacji" w Instytucie Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk. Treść dokumentu stanowi załącznik do niniejszego Zarządzenia.

Jednocześnie unieważniam „Politykę Bezpieczeństwa w zakresie Ochrony Danych Osobowych Instytutu Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego PAN wraz z instrukcją Zarządzania Systemem Informatycznym" wprowadzoną Zarządzeniem nr 10/2013 z dnia 09.09.2013 r.

Niniejsze Zarządzenie wchodzi w życie z dniem 3 września 2018 roku.

DYREKTOR

prof. dr hab. n. med. Maria Barcikowska-Kotowicz

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W INSTYTUCIE MEDYCYNY DOŚWIADCZALNEJ I KLINICZNEJ IM. M. MOSSAKOWSKIEGO POLSKIEJ AKADEMII NAUK

Warszawa, wrzesień 2018 r.

SPIS TREŚCI

Lp.	Rozdział	Str.
I	Wstęp	3
II	Określenie funkcji Administratora Danych Osobowych oraz Inspektora ochrony danych	5
III	Zasady dopuszczania do przetwarzania danych osobowych, obowiązki nałożone na osoby dopuszczone do przetwarzania danych osobowych, zasady powierzania przetwarzania danych osobowych innym podmiotom, zasady udostępniania danych osobowych oraz zasady przetwarzania danych osobowych w systemie informatycznym	5
IV	Realizacja praw przysługujących osobom, których dane osobowe dotyczą	8
V	Podejście do ochrony danych osobowych oparte na ryzyku	11
VI	Procedura postępowania w sytuacji naruszenia ochrony danych osobowych	12
VII	Postanowienia końcowe	13
	Załączniki:	
1	Wzór imiennego upoważnienia do przetwarzania danych osobowych	14
2	Wzór umowy powierzenia przetwarzania danych	15
3	Wzór klauzuli informacyjnej	19
4	Wzór skróconej klauzuli informacyjnej	20
5	Wzór zgody na przetwarzanie danych osobowych	21
6	Wzór Rejestru czynności przetwarzania	22
7	Wzór Rejestru wszystkich kategorii czynności przetwarzania	23
8	Wzór Rejestru naruszeń ochrony danych osobowych	24
9	Wzór Rejestru upoważnień	25

I. Wstęp

1. **Polityka Bezpieczeństwa Informacji w Instytucie Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk (dalej: „Polityka Bezpieczeństwa") dotyczy bezpieczeństwa informacji, a w szczególności danych osobowych przetwarzanych w Instytucie Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk.**

2. **Użyte w Polityce Bezpieczeństwa określenia oznaczają:**

2.1. **Administrator danych osobowych** – osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

2.2. **dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

2.3. **Inspektor ochrony danych** – osobę wyznaczoną przez Administratora danych osobowych, odpowiedzialna za realizację zadań określonych w art. 39 rozporządzenia;

2.4. **Instytut** – Instytucie Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk;

2.5. **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;

2.6. **podmiot przetwarzający** – osobę fizyczną, lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

2.7. **przetwarzanie danych osobowych** – 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;

2.8. **rozporządzenie** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

2.9. **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

3. **Polityka Bezpieczeństwa, opisuje następujące elementy:**

- określenie Administratora danych osobowych oraz Inspektora ochrony danych,
- zasady dopuszczania do przetwarzania danych osobowych oraz obowiązki nałożone na osoby dopuszczone do przetwarzania danych osobowych,
- zasady powierzania danych osobowych innemu podmiotowi,

- zasady udostępniania danych osobowych innemu podmiotowi,
- przetwarzanie danych osobowych w systemie informatycznym,
- realizację praw osób, których dane dotyczą,
- sposób prowadzenia analizy ryzyka naruszenia praw lub wolności osoby fizycznej,
- metodologia oceny skutków dla ochrony danych,
- procedurę postępowania w sytuacji naruszenia ochrony danych osobowych.

Ponadto Polityka Bezpieczeństwa zawiera 9 załączników:

- załącznik nr 1 określający wzór imiennego upoważnienia do przetwarzania danych osobowych,
- załącznik nr 2 określający wzór umowy powierzenia przetwarzania danych osobowych,
- załącznik nr 3 określający wzór klauzuli informacyjnej,
- załącznik nr 4 określający wzór skróconej klauzuli informacyjnej,
- załącznik nr 5 określający wzór zgody na przetwarzanie danych osobowych,
- załącznik nr 6 określający wzór Rejestru czynności przetwarzania,
- załącznik nr 7 określający wzór Rejestru wszystkich kategorii czynności przetwarzania,
- załącznik nr 8 określający wzór Rejestru naruszeń ochrony danych osobowych,
- załącznik nr 9 określający wzór Rejestru upoważnień.

Wzory opisane w Polityce Bezpieczeństwa są wzorami przyjętymi do stosowania w Instytucie i każdy dokument obowiązujący w Instytucie powinien być zgodny z tymi wzorami, co najmniej poprzez kompletność i zgodność logiczną zapisów.

4. W Instytucie dane osobowe przetwarzane są z poszanowaniem podstawowych zasad przetwarzania danych osobowych, opisanych w art. 5 rozporządzenia, w myśl którego dane muszą być:

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

4.2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 rozporządzenia za niezgodne z pierwotnymi celami („ograniczenie celu");

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

4.4. 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");

4.5. 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; 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 na mocy art. 89 ust. 1 rozporządzenia, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

4.6. 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").

4.7. Ww. zasady są uwzględniane w fazie projektowania procesu przetwarzania danych osobowych oraz na każdym etapie przetwarzania danych osobowych, a ich przestrzeganie jest możliwe do wykazania/ udowodnienia przez Administratora danych osobowych („rozliczalność").

II. Określenie Administratora danych osobowych oraz Inspektora ochrony danych.

1. Administratorem danych osobowych oraz – w stosownych przypadkach – podmiotem przetwarzającym dane w Instytucie jest Instytut Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk.

2. W Instytucie został wyznaczony Inspektor ochrony danych.

2.1. Instytut stanowi jednostkę organizacyjną Polskiej Akademii Nauk, czyli podmiot wskazany w art. 9 pkt 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

2.2. Inspektor ochrony danych został wyznaczony na podstawie art. 37 ust. 1 lit. a rozporządzenia, w związku z art. 9 pkt 1 ustawy odo.

2.3. Inspektor ochrony danych wykonuje zadania na podstawie umowy o świadczenie usług.

2.4. Inspektor ochrony danych posiada odpowiednie kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania, zadań o których mowa w art. 39 rozporządzenia.

2.5. Inspektor ochrony danych jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych w Instytucie.

2.6. Inspektor ochrony danych jest uprawniony do współpracy z organem nadzorczym oraz pełnienia funkcji punktu kontaktowego dla organu nadzorczego, w tym przekazywania informacji dotyczących ochrony danych osobowych w Instytucie.

2.7. Inspektor ochrony danych jest uprawniony do pełnienia funkcji punktu kontaktowego dla osób, których dane dotyczą, w tym udzielania im informacji na temat spraw związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia.

III. Zasady dopuszczania do przetwarzania danych osobowych, obowiązki nałożone na osoby dopuszczone do przetwarzania danych osobowych, zasady powierzania przetwarzania danych osobowych innym podmiotom oraz udostępniania danych osobowych.

1. Dopuszczenie do przetwarzania danych osobowych.

1.1. Do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające imienne upoważnienie do przetwarzania danych osobowych, którego wzór określa załącznik nr 1.

1.2. Upoważnienia do przetwarzania danych osobowych udziela Administrator danych osobowych lub osoba uprawniona do działania w jego imieniu.

1.3. Dane osobowe mogą być przetwarzane wyłącznie na polecenie Administratora danych osobowych, w związku z wykonywaniem zadań lub obowiązków służbowych/ umownych.

1.4. W przypadku zmiany zakresu przetwarzanych danych osobowych lub zmiany innych danych zawartych w upoważnieniu, rozwiązania stosunku pracy/ umowy cywilnoprawnej – dokonuje się aktualizacji upoważnienia lub jego cofnięcia. Jeżeli upoważnienie zawiera odwołanie do innego dokumentu (np. zakresu obowiązków), również ten dokument musi być na bieżąco aktualizowany, w związku ze zmianami zakresu przetwarzania danych osobowych.

1.5. Upoważnienie, które utraciło moc, należy niezwłocznie zwrócić do Administratora danych osobowych.

1.6. W Instytucie prowadzony jest Rejestr upoważnień, którego wzór określa załącznik nr 8.

1.7. Osoby dopuszczone do przetwarzania danych osobowych powinny odbyć szkolenie z zakresu bezpieczeństwa informacji, w tym szczególnie danych osobowych. Dopuszczalną formą szkolenia jest zapoznanie z materiałami szkoleniowymi.

2. Osoby dopuszczone do przetwarzania danych osobowych są zobowiązane do:

2.1 Znajomości i przestrzegania przepisów dotyczących ochrony danych osobowych, w szczególności rozporządzenia oraz ustawy odo.

2.2 Bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa oraz innych regulacjach wewnątrzorganizacyjnych.

2.3 Przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych lub innych miejscach, zgodnie z otrzymanym poleceniem od Administratora danych osobowych.

2.4 Przetwarzania danych osobowych tylko w zakresie niezbędnym do realizacji danego zadania lub obowiązku służbowego/ umownego.

2.5 Przetwarzania danych osobowych nie dłużej niż jest to niezbędne do realizacji danego zadania lub obowiązku służbowego/ umownego.

2.6 Zabezpieczania danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce Bezpieczeństwa, a jeżeli zachodzi taka potrzeba – również z wykorzystaniem innych metod.

2.7 Niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie.

2.8 Nieudzielania informacji o danych osobowych innym podmiotom lub osobom nieuprawnionym, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w takich przepisach zostały spełnione.

2.9 Informowania Inspektora ochrony danych o wszelkich zmianach w obszarze przetwarzania danych osobowych, w szczególności mających wpływa na zapisy Rejestru czynności przetwarzania lub Rejestru wszystkich kategorii czynności przetwarzania.

3. Powierzenie przetwarzania danych osobowych.

3.1. Przetwarzanie przetwarzania danych osobowych może zostać powierzone innemu podmiotowi, pod warunkiem zawarcia z tym podmiotem pisemnej umowy powierzenia przetwarzania danych osobowych lub na podstawie innego instrumentu prawnego.

3.2. Umowy powierzenia przetwarzania danych osobowych oraz inne instrumenty prawne powinny zawierać wszystkie elementy wskazane w art. 28 rozporządzenia. W tym celu można posługiwać się wzorem określonym w załączniku nr 2. Wzór określa minimalny zakres zapisów jakie muszą zawierać się w umowie powierzenia przetwarzania danych osobowych.

3.3. Stronami umowy powierzenia przetwarzania danych osobowych jest Administrator danych osobowych oraz podmiot przetwarzający (zwany również procesorem).

3.4. Z chwilą zawarcia umowy powierzenia przetwarzania danych osobowych lub wejścia w życie innego instrumentu prawnego, podmiot przetwarzający zobowiązany jest do zabezpieczenia danych osobowych i wykorzystania ich jedynie w ramach umowy/ innego instrumentu prawnego.

3.5. Projekt umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego wymaga zaopiniowania przez Inspektora ochrony danych.

3.6. O podpisaniu umowy powierzenia przetwarzania danych osobowych lub wejściu w życie innego instrumentu prawnego należy poinformować Inspektora ochrony danych.

3.7. Zapisy ust. 3.5. oraz 3.6. mają zastosowanie zarówno do umów lub innych instrumentów prawnych, w których Instytut występuje w roli Administratorów danych osobowych, jak i do umów lub innych instrumentów prawnych, w których Instytut występuje w roli podmiotu przetwarzającego.

4. Udostępnienie danych osobowych innemu podmiotowi.

Wnioski składane do Instytutu przez podmioty zainteresowane udostępnieniem danych osobowych, powinny być konsultowane z Inspektorem ochrony danych lub osobą przez niego wskazaną.

5. Przetwarzanie danych osobowych w systemie informatycznym.

5.1. Przetwarzanie danych osobowych w systemie informatycznym musi gwarantować zachowanie poufności, integralności oraz dostępności przetwarzanych danych.

5.2. System informatyczny powinien być zabezpieczony specjalistycznym oprogramowaniem ochronnym, za co odpowiada Dział Informatyczny.

5.3. Należy regularnie dokonywać aktualizacji każdego zainstalowanego oprogramowania.

5.4. Należy regularnie sporządzać kopie zapasowe – zapewniające możliwość przywrócenia systemu i dostęp do danych osobowych. Częstotliwość sporządzania kopii zapasowych określi Dział Informatyczny.

5.5. Dostęp do systemu informatycznego w którym są przetwarzane dane osobowe mogą mieć tylko osoby posiadające upoważnienie do przetwarzania danych osobowych.

5.6. Dostęp do systemu informatycznego zabezpieczony jest hasłem indywidualnym dla każdego użytkownika.

5.7. Niedopuszczalne jest ujawniania innym osobom haseł dostępu do systemu informatycznego oraz do oprogramowania i innych funkcjonalności zabezpieczonych hasłem.

5.8. Podczas korzystania z poczty elektronicznej należy zachować szczególną ostrożność, zwłaszcza podczas odbierania wiadomości ze niezweryfikowanych źródeł oraz wiadomości nieoczekiwanych.

5.9. Dane osobowe przesyłane za pośrednictwem poczty elektronicznej poza Instytut powinny być – w miarę możliwości – zaszyfrowane.

5.10. Niedozwolone jest korzystanie z prywatnej poczty elektronicznej w celach służbowych.

5.11. Szczegółowe regulacje dotyczące zasad funkcjonowania systemów informatycznych, w tym szczególnie ich zabezpieczenia oraz przetwarzania w nich danych osobowych mogą określać osobne polityki lub instrukcje wprowadzane do stosowania w Instytucie.

IV. Realizacja praw przysługujących osobom, których dane dotyczą.

1. Zasady realizacji praw osób, których dane dotyczą.

1.1 W zależności od źródła i podstaw przetwarzania danych osobowych, osobie której dane dotyczą mogą przysługiwać prawa określone w rozporządzeniu:

1.1.1 prawo do informacji,

1.1.2 prawo dostępu do danych,

1.1.3 prawo do sprostowania danych,

1.1.4 prawo do usunięcia danych,

1.1.5 prawo do ograniczenia przetwarzania,

1.1.6 prawo do przenoszenia danych,

1.1.7 prawo do sprzeciwu.

1.2 Przed utrwaleniem danych osobowych lub realizacją praw, o których mowa w ust. 1.1.2 – 1.1.7 należy zweryfikować tożsamość danej osoby.

1.3 Tożsamość jest potwierdzana poprzez okazanie dokumentu ze zdjęciem (np. dowód osobisty, paszport, legitymacja studencka) lub w przypadku komunikacji na odległość, poprzez podanie dodatkowych informacji, w celu ich porównania z posiadanymi przez Instytut.

1.4 Jeżeli nie ma możliwości zidentyfikowania osoby, której dane dotyczą z uwagi na brak danych, należy ją o tym poinformować. W takiej sytuacji prawa, o których mowa w ust. 1.1.2 – 1.1.7 nie przysługują, chyba że osoba, której dane dotyczą dostarczy dodatkowych informacji, pozwalających na jej identyfikację.

O takim przypadku należy poinformować Inspektora ochrony danych.

1.5 Za realizację uprawnień, o których mowa w ust. 1.1 nie może być pobierana opłata, z zastrzeżeniem ust. 1.6 oraz 3.3.

1.6 Jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, rozumiany jako zgłoszenie trzeciego żądania w przeciągu 30 dni kalendarzowych, można:

a) pobrać rozsądną opłatę odpowiadającą faktycznie poniesionym kosztom wiązanym m.in. z nakładem pracy,

b) odmówić podjęcia działań.

O takim przypadku należy uprzednio poinformować Inspektora ochrony danych.

1.7 Prawa o których mowa w ust. 1.1.2. – 1.1.7. należy realizować bez zbędnej zwłoki, ale nie później niż w terminie miesiąca od otrzymania żądania. Termin ten może być wydłużany na zasadach określonych w rozporządzeniu.

1.8 Terminy, o których mowa w ust. 1.7. stosuje się odpowiednio do korespondencji dotyczącej realizacji albo odmowy realizacji praw.

1.7 Uprawnienia osób, których dane dotyczą mogą podlegać ograniczeniom lub włączeniom na podstawie innych przepisów Unii lub prawa krajowego, w zakresie opisanych w art. 23 rozporządzenia.

1.8 Prawa, o których mowa w ust. 1.1 są realizowanie w Instytucie przez Dyrektora lub jego zastępców.

2. Prawo do informacji

2.1. Prawo do informacji jest realizowane w Instytucie poprzez stosowanie tzw. klauzul informacyjnych (zgodnie ze wzorem z załącznika nr 3 i 4).

2.2. Treść klauzuli informacyjnych powinna odpowiadać wymogom określonym w art. 13 albo 14 rozporządzenia oraz być napisana zwięźle, przejrzyście, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

2.3. Klauzulę informacyjną przekazuje się podczas pozyskiwania danych osobowych albo przy pierwszym kontakcie z osobą, której dane dotyczą, z zastrzeżeniem, że:

2.3.1. klauzule informacyjne w pełnej treści powinny być umieszczane w sekretariacie, na stronie internetowej lub w treści zawieranych umów/ obowiązujących regulaminów – jeżeli takie funkcjonują.

2.3.2. skrócone klauzule informacyjne mogą być stosowane wyłącznie, w przypadku jednoczesnej publikacji pełnej treści danej klauzuli informacyjnej w Internecie oraz w wersji papierowej (np. w sekretariacie lub umowie).

2.3.3. nie prowadzi się korespondencji wyłącznie w celu realizacji obowiązku informacyjnego.

2.4. Obowiązku informacyjnego nie trzeba realizować, jeżeli osoba, której dane dotyczą dysponuje już tymi informacjami, zwłaszcza, jeśli już wcześniej udostępniono tej osobie klauzulę informacyjną.

2.5. Obowiązku informacyjnego nie trzeba realizować, jeżeli dane zostały pozyskane w inny sposób niż od osoby, której dane dotyczą, a:

2.5.1. udzielenie takich informacji byłoby niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku lub

2.5.2. pozyskiwanie lub ujawnianie takich danych osobowych jest wyraźnie uregulowane prawem Unii lub państwa członkowskiego lub

2.5.3. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego.

3. Prawo dostępu i sprostowania

3.1. W przypadku kiedy osoba, której dane dotyczą powołuje się na prawo dostępu do danych osobowych jest ona uprawniony do:

3.2.1 uzyskania potwierdzenia, czy Administrator danych osobowych przetwarza jej dane osobowe (czy dane osobowe są przetwarzane w Instytucie),

a jeżeli ma to miejsce, wtedy jest uprawniony również do:

3.1.2. uzyskania dostępu do tych danych oraz informacji wskazanych w art. 15 ust. 1 lit a-h rozporządzenia,

3.1.3. uzyskania kopii danych osobowych podlegających przetwarzaniu.

3.2. Prawo dostępu do danych osobowych nie jest równoznaczne z prawem żądania dostępu do dokumentów zawierających te dane.

3.3. Przekazanie kopii, o której mowa w ust. 3.1.3 jest wolne od opłat, jednak za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, pobiera się opłatę w rozsądnej wysokości – wynikającej z faktycznych kosztów jej wytworzenia.

3.4. Przed realizacją praw, o których mowa w ust. 3.1. należy bezwzględnie dokonać weryfikacji tożsamości osoby wnoszącej żądanie – na zasadach określonych w ust. 1.3.

3.5. Osobie, której dane dotyczą, w każdym czasie przysługuje prawo niezwłocznego sprostowania danych osobowych, które są nieprawidłowe. Zapis ust. 3.4 stosuje się odpowiednio.

4. Prawo do usunięcia danych

4.1. Prawo usunięcia danych osobowych nie znajduje zastosowania w Instytucie wobec danych, których przetwarzania jest niezbędne:

4.1.1. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator Danych Osobowych,

4.1.2. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 rozporządzenia,

4.1.3. do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych Osobowych,

4.1.4. do celów archiwalnych w interesie publicznym lub do celów badań naukowych,

4.1.5. do ustalenia, dochodzenia lub obrony roszczeń.

4.2. W przypadkach, o których mowa w ust. 4.1.1. oraz 4.1.3. odmowy zrealizowania prawa do usunięcia danych dokonuje się w oparciu o właściwy przepis prawa materialnego w związku z art. 17 ust. 3 lit. b rozporządzenia.

4.3. O odmowie informuje się osobę zainteresowaną oraz Inspektora ochrony danych.

4.4. O wpłynięciu żądania usunięcia danych, należy poinformować Inspektora ochrony danych.

5. Prawo do ograniczenia przetwarzania

5.1. Ilekroć osoba, której dane dotyczą żąda ograniczenia przetwarzania należy dokonać analizy, czy realizacja tego uprawnienia nie stoi w sprzeczności z ważnym interesem publicznym Unii lub państwa członkowskiego.

5.2. Jeżeli zachodzą przesłanki uzasadniające przetwarzanie niezależnie od żądania ograniczenia, należy o tym poinformować osobę wnoszącą żądanie oraz Inspektora ochrony danych.

5.3. Realizacja żądania ograniczenia przetwarzania pozostaje bez wpływu na możliwość przechowywania danych.

5.4. O wpłynięciu żądania ograniczenia przetwarzania danych należy poinformować Inspektora ochrony danych.

6. Prawo do przenoszenia danych

6.1. W ramach realizacji prawa do przenoszenia danych, osoba której dane dotyczą może:

6.1.1 otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (np. .txt, .pdf, .odt, .doc, .rtf, .jpeg) dane osobowe jej dotyczące, które dostarczyła administratorowi,

6.2.2. żądać, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

6.3. Prawo do przenoszenia danych przysługuje wyłącznie jeżeli przetwarzania odbywa się na podstawie zgody lub umowy oraz odbywa się w sposób zautomatyzowany oraz nie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

6.4. Prawo do przenoszenia danych dotyczy wyłącznie danych osobowych uzyskanych od osoby, której te dane dotyczą. Wszelkie informacje będące wynikiem przetwarzania danych w Instytucie nie podlegają temu uprawnieniu (np. wyniki badań, analiz, opracowań).

6.5. O wpłynięciu żądania przeniesienia danych, należy poinformować Inspektora ochrony danych.

7. Prawo do sprzeciwu

7.1. Prawo do sprzeciwu wobec przetwarzania danych osobowych znajduje zastosowanie tylko i wyłącznie wobec danych osobowych przetwarzanych w Instytucie:

7.1.1. w celu wykonywania zadań realizowanych w interesie publicznym lub w ramach sprawowania powierzonej władzy publicznej;

7.1.2. w oparciu o przesłankę tzw. prawnie uzasadnionych interesów Instytutu.

7.2. Sprzeciw wobec przetwarzania danych osobowych musi być uzasadniony szczególną sytuacją osoby, której dane dotyczą.

7.3. O wpłynięciu sprzeciwu wobec przetwarzania danych należy poinformować Inspektora ochrony danych.

7.4. W przypadku stwierdzenia zasadności sprzeciwu nie wolno dalej przetwarzać danych osobowych.

V. Podejście do ochrony danych osobowych oparte na ryzyku.

1. W Instytucie dla wszystkich czynności przetwarzania prowadzona jest analiza ryzyka naruszenia praw lub wolności osób fizycznych.

1.1. Analiza ryzyka jest mechanizmem wkomponowanym w Rejestr czynności przetwarzania oraz Rejestr wszystkich kategorii czynności przetwarzania, oceniającym prawdopodobieństwo wystąpienia ryzyka oraz wagę w sposób ciągły, z wykorzystaniem algorytmu obliczeniowego.

1.2. Rejestry, o których mowa w ust. 1.1. prowadzone są przez Inspektora ochrony danych zgodnie ze wzorami określonymi w załącznikach nr 6 i 7.

1.3. Stosowane w Instytucie środki techniczne i organizacyjne zapewniające ochronę danych osobowych są adekwatne i proporcjonalne do wyników analizy ryzyka, o której mowa w ust. 1.1.

2. Ocena skutków dla ochrony danych

2.1. Ocena skutków dla ochrony danych wykonywana jest w Instytucie w oparciu o:

2.1.1. zapisy z Rejestru czynności przetwarzania/ Rejestru wszystkich kategorii czynności przetwarzania,

2.1.2. weryfikację zgodności przetwarzania z zasadami przetwarzania, o których mowa w art. 5 rozporządzenia,

2.1.3. analizę ryzyka naruszenia praw i wolności osób fizycznych,

2.1.4. środki planowane w celu zaradzenia ryzyku,

2.1.5. konsultacje z Inspektorem ochrony danych.

2.2. Ocena skutków dla ochrony danych ma formę opisową (pisemną, w tym elektroniczną) dla danej czynności przetwarzania.

2.3. W Instytucie ocenie skutków podlegają rodzaje operacji przetwarzania dotyczące:

2.3.1. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 rozporządzenia,

2.3.2. rodzaje operacji przetwarzania wymienione w wykazie, o którym mowa w art. 35 ust. 4 rozporządzenia.

2.4. Ocenę wykonuje się przed rozpoczęciem procesu przetwarzania oraz w czasie jego trwania, jeżeli zmienia się ryzyko wynikające z operacji przetwarzania lub w razie zaistnienia takiej potrzeby.

VI. Procedura postępowania w przypadku naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia.

1. Procedura określa sposób postępowania w przypadku:

1.1 zaistnienia prawdopodobieństwa naruszenia ochrony danych osobowych w systemie informatycznym,

1.2 zaistnienie prawdopodobieństwa naruszenia ochrony danych osobowych przetwarzanych poza systemem informatycznym,

1.3 stwierdzenia naruszenia ochrony danych osobowych.

2. W przypadku stwierdzenia, przez osobę przetwarzającą dane osobowe, zaistnienia choćby jednej z okoliczności, o których mowa w ust. 1, osoby te są zobowiązane natychmiast zawiadomić Dyrektora Instytutu oraz Inspektora ochrony danych.

3. Inspektor ochrony danych albo osoba imiennie przez niego wskazana, w obecności osoby, która stwierdziła zaistnienie okoliczności z ust. 1 przeprowadza oględziny miejsca lub sprzętu, przyjmuje wyjaśnienia w tym zakresie i sporządza protokół.

4. Protokół, o którym mowa w ust. 3, powinien zostać sporządzony bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 48 godzin po stwierdzeniu okoliczności z ust. 1 oraz zawierać w szczególności:

4.1 precyzyjny opis zdarzenia będącego podstawą wszczęcia procedury,

4.2 określenie terminu zdarzenia wskazującego na stwierdzenia naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz termin ujawnienia tego zdarzenia,

4.3 określenia których danych naruszenie dotyczy (np. poprzez odwołanie do Rejestru czynności przetwarzania),

4.4 określenie szkód i zagrożenia dla danych przetwarzanych w zbiorze, zakresu naruszenia i kategorii osób, których danych naruszenie dotyczy,

4.5 określenie prawdopodobieństwa i wagi naruszenia praw lub wolności osób, których dane dotyczą,

4.6 wskazanie osób odpowiedzialnych za powstanie zdarzenia, o którym mowa w ust. 4.1.

5. Po sporządzeniu protokołu, o którym mowa w ust. 4, Inspektor ochrony danych dokonuje analizy i oceny całokształtu zdarzenia, następnie przekazuje protokół Dyrektorowi Instytutu oraz rekomenduje sposób dalszego postępowania:

5.1. niepodejmowanie dalszych działań – wobec braku znamion naruszenia ochrony danych osobowych albo

5.2. wprowadzenie środków eliminujących w przyszłości podobne zdarzenia lub

5.3. zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu lub

5.4. zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

6. Dyrektor Instytutu decyduje o sposobie dalszego postepowania. W tym zakresie korzysta z doradztwa Inspektora ochrony danych. Sposób postępowania jest indywidualny dla każdego przypadku i nie podlega schematyzacji.

7. W przypadku stwierdzenia naruszenia ochrony danych osobowych, Inspektor ochrony danych odnotowuje ten fakt w Rejestrze naruszeń, prowadzonym zgodnie ze wzorem z załącznik nr 9.

VII. Postanowienia końcowe

1. Wszelkie zmiany w Polityce Bezpieczeństwa wymagają formy pisemnej.
2. Wszystkie osoby przetwarzające dane osobowe w Instytucie zobowiązane są do zapoznania się z zapisami Polityki Bezpieczeństwa i jej stosowania.
3. Nieprzestrzeganie zapisów Polityki Bezpieczeństwa może wiązać się z odpowiedzialnością wynikającą z prawa pracy (ciężkie naruszenie podstawowych obowiązków pracowniczych) lub odszkodowawczą.

Załącznik nr 1.

Wzór upoważnienia do przetwarzania danych osobowych

Instytut Medycyny Doświadczalnej i Klinicznej
im. M. Mossakowskiego Polskiej Akademii Nauk
ul. Pawińskiego 5
02-106 Warszawa

Warszawa,.....r.

Upoważnienie do przetwarzania danych osobowych nr ..../(*rok*)

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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z późn. zm.; dalej zwane RODO) oraz rozdziału II ust. 1.3. Polityki Bezpieczeństwa Informacji w Instytucie Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk

upoważniam (*„Panią"/"Pana"*)(*imię i nazwisko*)

do przetwarzania danych osobowych przetwarzanych w Instytucie Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk, w zakresie niezbędnym do realizacji zadań określonych w (*wskazać zakres przetwarzania, np. zakres obowiązków lub czynności przetwarzania*), w szczególności do gromadzenia, utrwalania, opracowywania, modyfikowania, przechowywania, niszczenia.

Upoważnienie jest ważne (*należy wskazać od kiedy oraz do kiedy, np. poprzez datę albo wskazanie dnia odwołania/ rozwiązania/ wygaśnięcia stosunku pracy*).

Osoba upoważniona nie może udzielać dalszych upoważnień.

Osoba upoważniona jest jednocześnie zobowiązana do zachowania poufności, nieujawniania osobom nieupoważnionym oraz zachowania w tajemnicy wszelkich danych osobowych, przetwarzanych w ramach niniejszego upoważnienia, a które nie są przeznaczone do publicznego rozpowszechniania.

Zgodnie z art. 29 oraz 32 ust. 4 RODO przetwarzania danych osobowych jest dozwolone wyłącznie na polecenia Administratora Danych Osobowych – upoważnienie nie stanowi samoistnej podstawy legalizującej przetwarzanie danych osobowych.

Przetwarzanie danych osobowych niezgodnie z RODO może wiązać się z odpowiedzialnością dyscyplinarną, cywilną lub karną – przewidzianą w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

Upoważnienie, które utraciło ważność, należy zwrócić osobie udzielającej upoważnienia.

.....
(data i podpis osoby upoważnianej)

.....
(Administrator Danych Osobowych)

Egz. nr 1: osoba upoważniana
Egz. nr 2: ad acta

Załącznik nr 2.

Wzór umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych

zawarta (*dd-mm-rrrr*) w (*miejscowość*) pomiędzy:

(*nazwa*) z siedzibą w (*miejscowość, kod, ulica, nr*),

reprezentowanym/ną przez: (*imię, nazwisko oraz stanowisko*) – Administrator danych osobowych,

zwanym dalej: **Administratorem**,

a

(*nazwa*) z siedzibą w (*miejscowość, kod, ulica, nr*),

reprezentowanym/ną przez: (*imię, nazwisko oraz stanowisko*) – Podmiot przetwarzający,

zwaną dalej: **Procesorem,**

łącznie zwanymi **Stronami**.

W niniejszej umowie zastosowano następujący skrót:

1) rozporządzenie - 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 rozporządzenia o ochronie danych),
2) 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.

(*oraz inne, jeśli znajdą zastosowanie*)

§ 1.

1. Procesor będzie przetwarzał w imieniu Administratora dane osobowe powierzone w trybie art. 28 rozporządzenia, na warunkach i w celu określonym w niniejszej umowie.
2. Procesor może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na Procesora prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Procesor. W takim przypadku przed rozpoczęciem przetwarzania Procesor informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

§ 2.

1. Na mocy niniejszej umowy Procesor będzie przetwarzał (*„dane zwykłe" lub „szczególne kategorie danych osobowych" lub „dane osobowe dotyczące wyroków skazujących i naruszeń prawa"*) (*wskazanie kategorii osób, których dane dotyczą, np. pracownicy*) w zakresie (*wszystkie rodzaje danych, np. imię, nazwisko, nr PESEL*).
2. Dane osobowe powierzone przez Administratora będą przetwarzane przez Procesora wyłącznie w celu (*opis celu lub podstawa realizacji zadania lub odniesienie do innej umowy*), (*określenie czasu przetwarzania*).

§ 3.

Procesor, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zobowiązuje się do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

§ 4.

1. Procesor zapewnia, że powierzone dane osobowe będą przetwarzane wyłącznie przez osoby do tego upoważnione.
2. Procesor może upoważniać swoich pracowników – którzy zobowiążą się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy – do przetwarzania danych osobowych powierzonych niniejszą umową.
3. Czynności określone w ust. 2 wymagają zachowania formy pisemnej.
4. Procesor prowadzi ewidencję osób upoważnionych.

§ 5.

1. Procesor nie korzysta z usług innego podmiotu przetwarzającego (zwanego dalej Podwykonawcą) bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. W przypadku ogólnej pisemnej zgody Procesor informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia Podwykonawców, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
2. Procesor zapewnia, że na Podwykonawcę nałożone zostaną – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii Europejskiej lub prawu krajowemu – te same obowiązki ochrony danych, jakie na Procesora nakłada niniejsza umowa, a w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom rozporządzenia.
3. Jeżeli Podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków Podwykonawcy spoczywa na Procesorze.

§ 6.

1. Procesor, biorąc pod uwagę charakter przetwarzania danych, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III rozporządzenia.
2. Procesor, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 rozporządzenia.
3. (*„Procesor zobowiązuje się realizować w imieniu Administratora obowiązek informacyjny określony w art. 13 lub 14 rozporządzenia." – jeżeli w danych okolicznościach znajduje to zastosowanie)*

§ 7.

1. Procesor udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia oraz umożliwia Administrator lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

2. Administrator informuje Procesora o terminie i zakresie audytu/inspekcji z co najmniej 5-dniowym wyprzedzeniem.
3. Jeżeli audyt albo inspekcja są realizowane w związku naruszeniem ochrony danych osobowych lub uzasadnionym podejrzeniem takiego naruszenia, Administrator może odstąpić od obowiązku określonego w ust. 2.
4. Po audycie/inspekcji Administrator może przekazać Procesorowi pisemne zalecenia wraz z terminem ich realizacji.
5. Procesor niezwłocznie informuje Administratora, jeżeli jego zdaniem zalecenie, o którym mowa w ust. 4, stanowi naruszenie rozporządzenia lub innych przepisów Unii Europejskiej lub krajowych.

§ 8.

1. W przypadku naruszenia ochrony danych osobowych lub uzasadnionego podejrzenia takiego naruszenia, Procesor bez zbędnej zwłoki, jednak nie później niż w terminie 24 godzin po stwierdzeniu naruszenia – zgłasza je Administratorowi.
2. Zgłoszenia o którym mowa w ust. 1 dokonuje się za pośrednictwem poczty elektronicznej, na adres: (*wskazać adres na który należy przesłać zgłoszenie*) oraz potwierdza jego odbiór telefonicznie.
3. Zgłoszenie o którym mowa w ust. 1 powinno zawierać co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Procesor niezwłocznie informuje Administratora o każdym postępowaniu administracyjnym lub sądowym dotyczącym powierzonych do przetwarzania danych osobowych, a także o każdej kontroli lub audycie dotyczącym tychże danych osobowych.
5. Procesor ponosi pełną odpowiedzialność za wszelkie szkody powstałe w związku z przetwarzaniem przez niego danych osobowych, w sposób niezgodny z rozporządzeniem, niniejszą umową lub zaleceniami, o których mowa w § 7 ust. 4 – poniesione przez Administratora, osoby, których dane zostały powierzone lub osoby trzecie.

§ 9.

1. Niniejsza umowa obowiązuje od (*data, np. 25 maja 2018 r. lub „dnia jej zawarcia"*) do (*data albo zdarzenie albo odniesienie do czasu obowiązywanie innej umowy*).
2. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Procesor:
   a) nie wykona zaleceń, o których mowa w § 7 ust. 4;
   b) przetwarza powierzone dane osobowe w sposób niezgodny z przepisami o ochronie danych osobowych lub niniejszą umową.

§ 10.

1. Po zakończeniu świadczenia usług, o których mowa w § 2, Procesor – zależnie od decyzji Administratora – usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie istniejące ich kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

2. W przypadku korzystania z usług Podwykonawcy, Procesor zapewnia realizację obowiązku, o którym mowa w ust. 1 przez Podwykonawcę.

§ 11.

1. Wszelkie zmiany niniejszej umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowania przepisy kodeksu cywilnego oraz rozporządzenia.
3. Umowę sporządzono w (*liczba egzemplarzy ze wskazaniem poszczególnych ich dysponentów*).

Administrator **Procesor**

Dodatkowe instrukcje przygotowywania umowy:

1. **Fragmenty podkreślone są elementami instrukcji i nie stanowią treści wzoru.**
2. **Każdorazowo należy upewnić się, że zaproponowane powyżej zapisy są adekwatne do stanu faktycznego.**
3. **Powyższy wzór należy uzupełnić zgodnie z zapisami RODO i w oparciu o właściwe przepisy prawa materialnego.**
4. **Wzór zawiera podstawowe zapisy wymagane w umowie powierzenia przetwarzania danych i może być rozszerzany o inne, niesprzeczne zapisy.**
5. **Zapisy dotyczące powierzenia przetwarzania danych osobowych mogą stanowić część umowy głównej lub niezależną umowę (tak jak to zaproponowano we wzorze).**
6. **W przypadku jakichkolwiek wątpliwości dotyczących wzoru, informacje można uzyskać u Inspektora ochrony danych.**
7. **Wzór służy wyłącznie do wykorzystania służbowego.**

Załącznik nr 3.

Wzór klauzuli informacyjnej

Administratorem danych osobowych jest Instytut Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk, którego siedziba mieści się w Warszawie (02-106) przy ul. Pawińskiego 5, a dane kontaktowe to: tel. (22) 668-52-50, e-mail: sekretariat@imdik.pan.pl.

Z inspektorem ochrony danych można skontaktować się pod nr tel. 605-976-900 lub za pośrednictwem poczty elektronicznej: daneosobowe@imdik.pan.pl.

Pani/ Pana dane osobowe:

1) będą przetwarzane zgodnie z (*„art. 6 ust. 1 lit. X" – należy wskazać właściwą literę lub „art. 9 ust. 2 lit. X" – należy wskazać właściwą literę*) 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 rozporządzenia o ochronie danych osobowych), dalej zwanego RODO,

   w celu (*opis celu*),

   na podstawie (*podstawa prawna przetwarzania, jeżeli dane są przetwarzane zgodnie z art. 6 ust. 1 lit. c albo e lub art. 9 ust. 2 lit. g*);

2) (*„nie będą udostępniane innym odbiorcom" albo „mogą zostać udostępnione" należy podać odbiorcę lub kategorię odbiorców*);

3) będą przechowywane nie dłużej, niż to wynika z przepisów o archiwizacji (*chyba, że inne ramy czasowe*);

4) (*„będą"/ „nie będą"*) przetwarzane w sposób zautomatyzowany, w celu podjęcia decyzji w sprawie indywidualnej. (*jeżeli będą, trzeba podać informacje o zasadach podejmowania tych decyzji oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania)*

Na zasadach określonych w RODO przysługuje Pani/Pan prawo żądania:

5) dostępu do swoich danych osobowych, ich sprostowania, usunięcia (w przypadkach i na zasadach określonych w RODO), ograniczenia przetwarzania (*jeśli przetwarzanie odbywa się w związku z art. 6 ust. 1 lit. a albo b albo art. 9 ust. 2 lit. a, wtedy również „przenoszenia danych"*);

6) wniesienia sprzeciwu (*tylko jeżeli podstawą przetwarzania jest art. 6 ust. 1 lit. e albo f*);

7) wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych

Ma Pani/ Pan prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. *(tylko jeżeli przetwarzanie odbywa się w związku z art. 6 ust. 1 lit. a albo art. 9 ust. 2 lit. a)*;

Podanie danych osobowych (*„jest dobrowolne" albo „jest wymogiem ustawowym" albo „jest warunkiem zawarcia umowy"*) i (*„jest"/„nie jest"*) Pani/Pan zobowiązana/ny do ich podania. (*należy również wskazać konsekwencje ich niepodania*).

Dodatkowe instrukcje przygotowywania klauzuli informacyjnej:

1. **Fragmenty podkreślone są elementami instrukcji i nie stanowią treści wzoru.**
2. **Każdorazowo należy upewnić się, że zaproponowane powyżej zapisy są adekwatne do stanu faktycznego.**
3. **Powyższy wzór należy uzupełnić zgodnie z zapisami RODO i w oparciu o właściwe przepisy prawa materialnego.**
4. **W przypadku jakichkolwiek wątpliwości dotyczących wzoru, informacje można uzyskać u Inspektora ochrony danych.**

5. **Wzór służy wyłącznie do wykorzystania służbowego.**

Załącznik nr 4.

Wzór skróconej klauzuli informacyjnej

Administratorem danych osobowych jest Instytut Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk, którego siedziba mieści się w Warszawie (02-106) przy ul. Pawińskiego 5, a dane kontaktowe to: tel. (22) 668-52-50, e-mail: sekretariat@imdik.pan.pl.

Z inspektorem ochrony danych można skontaktować się pod nr tel. 605-976-900 lub za pośrednictwem poczty elektronicznej: daneosobowe@imdik.pan.pl.

Więcej informacji dotyczących przetwarzania danych osobowych znajduje się (*należy wskazać co najmniej 2 miejsca publikacji pełnej treści klauzuli informacyjnej: w Internecie oraz w formie papierowej (np. w sekretariacie, regulaminie, umowie).*

Dodatkowe instrukcje przygotowywania skróconej klauzuli informacyjnej:

1. **Fragmenty podkreślone są elementami instrukcji i nie stanowią treści wzoru.**
2. **Każdorazowo należy upewnić się, że zaproponowane powyżej zapisy są adekwatne do stanu faktycznego.**
3. **Powyższy wzór należy uzupełnić zgodnie z zapisami RODO i w oparciu o właściwe przepisy prawa materialnego.**
4. **Stosowanie skróconej klauzuli informacyjnej jest możliwe wyłącznie w przypadku wcześniejszej publikacji pełnej treści klauzuli informacyjnej, co najmniej w Internecie oraz w formie papierowej (np. w sekretariacie, regulaminie, umowie).**
5. **W przypadku jakichkolwiek wątpliwości dotyczących wzoru, informacje można uzyskać u Inspektora ochrony danych.**
6. **Wzór służy wyłącznie do wykorzystania służbowego.**

Załącznik nr 5.

Wzór zgody na przetwarzania danych osobowych

Wyrażam zgodę na przetwarzanie moich danych osobowych (*wskazać, których danych, np. „zawartych w formularzu"*), w celu (*należy określić cel przetwarzania, np. „udziału w badaniu dotyczącym..."*).

Przysługuje mi prawo do cofnięcia w dowolnym momencie niniejszej zgody, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Administratorem danych osobowych jest Instytut Medycyny Doświadczalnej i Klinicznej im. M. Mossakowskiego Polskiej Akademii Nauk, którego siedziba mieści się w Warszawie (02-106) przy ul. Pawińskiego 5, a dane kontaktowe to: tel. (22) 668-52-50, e-mail: sekretariat@imdik.pan.pl.

.....
(data i podpis)

Dodatkowe instrukcje przygotowywania zgody:

1. **Fragmentu podkreślone są elementami instrukcji i nie stanowią treści wzoru.**
2. **Każdorazowo należy upewnić się, że zaproponowane powyżej zapisy są adekwatne do stanu faktycznego.**
3. **Powyższy wzór należy uzupełnić zgodnie z zapisami RODO i w oparciu o właściwe przepisy prawa materialnego.**
4. **Wyrażenie zgody na przetwarzania danych osobowych nie wyłącza obowiązku informacyjnego (klauzule informacyjne).**
5. **Przetwarzanie danych wskazanych na podstawie zgody nie może jednocześnie wynikać z przepisów prawa materialnego.**
6. **W przypadku jakichkolwiek wątpliwości dotyczących wzoru, informacje można uzyskać u Inspektora ochrony danych.**
7. **Wzór służy wyłącznie do wykorzystania służbowego.**

Wzór Rejestru czynności przetwarzania

Arkusz 1 (tytułowy)

Oznaczenie Administratora Danych Osobowych (nazwa, adres, dane kontaktowe)

Oznaczenie Inspektora ochrony danych (imię i nazwisko, dane kontaktowe)

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Arkusz 2 (wykaz czynności)

Czynność przetwarzania	Cel przetwarzania	Podstawa prawna (z RODO oraz prawa materialnego)	Kategoria osób, których dane dotyczą	Źródło danych osobowych	Kategorie danych osobowych	Zautomatyzowane podejmowanie decyzji	Komórki organizacyjne, w których przetwarzana są dane	Podmioty, którym powierzono przetwarzanie lub współadministratorzy; odbiorcy danych	Przekazanie danych do państwa trzeciego	Planowany termin zakończenia przetwarzania

Arkusz 3 (analiza ryzyka)

Czynność przetwarzania	Liczba danych zwykłych	Liczba danych wrażliwych	Podatność na czynniki zewnętrzne	Zautomatyzowane podejmowanie decyzji	Liczba komórek org., w których dane są przetwarzane	Liczba współadministratorów oraz podmiotów, którym powierzono przetwarzanie danych osobowych	Ryzyko (suma)	Ocena skutków/ środki zaradcze	
	1 do 5 = 1 6 i więcej = 2	0 = 0 1 do 2 = 1 3 i więcej = 2	Przetwarzanie tylko w Instytucie = 0 poza Instytutem = 1	Nie = 0 Tak = 1	1 do 2 = 1 3 i więcej = 2	0 = 0 1 = 1 2 i więcej = 2	2 do 3 = *niskie* 4 do 6 = *średnie* 7 do 8 = *wysokie* 9 do 10 = *krytyczne*	Ryzyko niskie/ średnie = *Ryzyko akceptowalne* Ryzyko wysokie = *Wymagane środki minimalizujące* Ryzyko krytyczne = *Wymagana ocena skutków*	Środki minimalizujące

Wzór Rejestru wszystkich kategorii czynności

Arkusz 1 (tytułowy)

Oznaczenie Podmiotu przetwarzającego (nazwa, adres, dane kontaktowe)

Oznaczenie Inspektora ochrony danych podmiotu przetwarzającego (imię i nazwisko, dane kontaktowe)

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa w podmiocie przetwarzającym

Arkusz 2 (wykaz czynności)

Kategoria czynności przetwarzania	Oznaczenie i dane kontaktowe Administratora danych osobowych	Oznaczenie i dane kontaktowe Inspektora ochrony danych wyznaczonego przez Administratora danych osobowych	Podmioty, którym podpowierzono przetwarzania danych	Rodzaj danych osobowych (zwykłe/ wrażliwe)	Czas trwania przetwarzania	Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej

Arkusz 3 (analiza ryzyka)

Czynność przetwarzania	Liczba danych zwykłych	Liczba danych wrażliwych	Podatność na czynniki zewnętrzne	Zautomatyzowane podejmowanie decyzji	Liczba komórek org., w których dane są przetwarzane	Liczba współadministratorów oraz podmiotów, którym podpowierzono przetwarzanie danych osobowych	Ryzyko (suma)	Ocena skutków/ środki zaradcze	
	1 do 5 = 1 6 i więcej = 2	0 = 0 1 do 2 = 1 3 i więcej = 2	Przetwarzanie tylko w Instytucie = 0 poza Instytutem = 1	Nie = 0 Tak = 1	1 do 2 = 1 3 i więcej = 2	0 = 0 1 = 1 2 i więcej = 2	2 do 3 = *niskie* 4 do 6 = *średnie* 7 do 8 = *wysokie* 9 do 10 = *krytyczne*	Ryzyko niskie/ średnie = *Ryzyko akceptowalne* Ryzyko wysokie = *Wymagane środki minimalizujące* Ryzyko krytyczne = *Wymagana ocena skutków*	Środki minimalizujące

Wzór Rejestru upoważnień

Nr upoważnienia	Imię	Nazwisko	Stanowisko	Zakres (ewentualnie odwołanie do dokumentu określającego zakres)	Obowiązuje OD	Obowiązuje DO	Data utraty ważności	Uwagi

Załącznik nr 9

Wzór Rejestru naruszeń

Lp.	Data (godzina) stwierdzenia	Osoba zgłaszająca	Lokalizacja (system informatyczny/ lokalizacja fizyczna)	Opis zdarzenia na podstawie protokołu	Szkody stwierdzone dla organizacji	Dane, których naruszenie dotyczy	Kategoria osób, których dane dotyczą	Prawdopodobieństwo i waga naruszenia praw lub wolności osób, których dane dotyczą	Wskazanie osób odpowiedzialnych za naruszenie	Rekomendowane działania	Podjęte działania