

WZÓR - UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

(dalej również: „**Umowa**”)

Umowa podpisana elektronicznie.

Data zawarcia umowy jest dzień złożenia zgodnych oświadczeń woli stron.

pomiędzy:

Narodowym Instytutem Kardiologii Stefana kardynała Wyszyńskiego Państwowym Instytutem Badawczym z siedzibą w Warszawie, przy ul. Alpejskiej 42 (kod pocztowy: 04-628), wpisanym do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem, KRS: 0000041396, NIP: 525-000-85-25, REGON: 000837583, reprezentowanym przez:

.....

(zwanym dalej: „**Powierzającym**”)

a

.....
.....
.....

reprezentowanym przez:

.....

(zwanym dalej: „**Procesorem**”)

(Powierzający i Procesor zwani są dalej łącznie „**Stronami**”, a każdy z osobna „**Stroną**”)

Mając na uwadze fakt, że Strony zawarły umowę (dalej również „**Umowa Główna**”) z dnia numer w przedmiocie na podstawie której Procesor zobowiązał się do przetwarzania danych osobowych
(*należy podać kategorię osób, których dane dotyczą, np. pracowników administratora, pacjentów administratora itp. oraz cel przetwarzania np. uczestników szkoleń, uczestników badania itp.*), Strony zawierają Umowę o następującej treści:

§ 1

Przedmiot powierzenia i oświadczenia Stron

1. Powierzający oświadcza, że jest uprawniony do powierzenia przetwarzania danych osobowych w zakresie wskazanym w Załączniku nr 1 i na zasadach wskazanych w niniejszej Umowie powierza Procesorowi do przetwarzania dane osobowe.
2. Zakres powierzenia, wskazany w Załączniku nr 1, może zostać w każdym momencie rozszerzony albo ograniczony przez Powierzającego. Zmiana Załącznika nr 1 w zakresie ograniczenia albo rozszerzenia zakresu może być dokonana poprzez przesłanie przez Powierzającego do Procesora nowej zmienionej wersji Załącznika nr 1 w formie elektronicznej (na adres e-mail wskazany w Załączniku nr 4). W przypadku braku reakcji Procesora w ciągu 3 dni roboczych (dalej również: „**Dni Robocze**”) od daty wysłania wiadomości przez Powierzającego przyjmuje się, że Procesor zaakceptował zmianę zakresu powierzenia.

3. Dane osobowe przetwarzane są w celu realizacji Umowy. Procesor zobowiązuje się do przetwarzania powierzonych mu danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji obowiązków wynikających z Umowy Głównej.
4. W stosunku do danych osobowych podejmowane mogą być następujące kategorie czynności przetwarzania: *(np. 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 – należy wybrać właściwe)*
5. Z tytułu przetwarzania danych osobowych Procesorowi nie przysługuje prawo do odrębnego wynagrodzenia poza wskazanym w Umowie Głównej (w tym również na wypadek zmiany zakresu przetwarzania).

§ 2

Obowiązki i Odpowiedzialność Stron

1. Procesor oświadcza, że zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. W przypadku, gdy Procesor stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO, jest to wystarczające do wykazania zapewnienia gwarancji, o których mowa w ustępie poprzedzającym w zakresie objętym zatwierdzonym kodeksem postępowania lub zatwierdzonym mechanizmem certyfikacji.
3. Procesor zobowiązany jest:
 - 1) przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Powierzającego, co dotyczy także przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, chyba że obowiązek taki wynika z powszechnie obowiązujących przepisów prawa. Powierzający może przekazywać Procesorowi instrukcje drogą elektroniczną, na adres wskazany w Załączniku nr 4. Procesor powinien wdrożyć instrukcje niezwłocznie, nie później jednak niż w terminie 5 Dni Roboczych. Procesor zobowiązany jest potwierdzić Powierzającemu wdrożenie instrukcji na adres e-mail wskazany w Załączniku nr 4. Jeżeli Procesor nie będzie w stanie wdrożyć instrukcji we wskazanym terminie, powinien poinformować Powierzającego o tym fakcie, za pośrednictwem informacji przesłanej na adres e-mail wskazany w Załączniku nr 4 i wskazać uzasadnienie dlaczego wdrożenie instrukcji Powierzającego nie było możliwe. Procesor może również zaproponować nowy termin wdrożenia instrukcji Powierzającego, który musi zostać zaakceptowany drogą elektroniczną (wysłał e-mail na adres wskazany w Załączniku nr 4) przez Powierzającego;
 - 2) niezwłocznie informować Powierzającego o obowiązku prawnym udostępnienia danych osobowych, o którym mowa w pkt. 1) powyżej, chyba że powszechnie obowiązujące przepisy zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny;
 - 3) dopuszczać do przetwarzania danych osobowych wyłącznie osoby odpowiednie upoważnione do tego;
 - 4) dopuszczać do przetwarzania danych osobowych wyłącznie osoby, które zobowiązały się do zachowania tajemnicy lub które podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
 - 5) jeżeli dane osobowe powierzone Procesorowi do przetwarzania zawierają dane o stanie zdrowia oraz podlegają tajemnicy zawodowej osób wykonujących zawody medyczne, procesowania ich z zachowaniem najwyższej staranności, w tym w zakresie zasad bezpieczeństwa i zabezpieczeń systemów informatycznych oraz innych obowiązków wynikających z przepisów prawa, w szczególności ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz zawartej Umowy;
 - 6) podejmować wszelkie środki wymagane, zgodnie z art. 32 RODO, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz

ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający temu ryzyku, w szczególności:

- a) pseudonimizację i szyfrowanie danych osobowych;
 - b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
 - c) zdolność do szybkiego przywrócenia danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
 - d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
- 7) przestrzegać warunków korzystania z usług podmiotu, któremu powierza przetwarzanie danych osobowych, wskazanych w ust. 13 i 18 poniżej;
 - 8) w razie potrzeby i na żądanie Powierzającego pomagać Powierzającemu 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 RODO. W szczególności dotyczy to wspomagania w zakresie udzielania odpowiedzi na wnioski o korzystanie z praw osoby, której dane dotyczą, w tym w zakresie prawa dostępu przysługującego osobie, której dane dotyczą, prawa do sprostowania danych, prawa do usunięcia danych, prawa do ograniczenia przetwarzania;
 - 9) niezwłocznie, nie później jednak niż w terminie 2 Dni Roboczych na adres wskazany w Załączniku nr 4, informować Powierzającego o tym, iż osoba, której dane dotyczą, skierowała do Procesora korespondencję zawierającą żądanie w zakresie wykonywania praw osoby określonych w rozdziale III RODO, jak również udostępniać treść tej korespondencji;
 - 10) w razie potrzeby i/lub na żądanie Powierzającego pomagać Powierzającemu wywiązywać się z następujących obowiązków:
 - a) wypełniania obowiązków związanych z wdrożeniem odpowiednich środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa przetwarzania przez Powierzającego, zgodnie z art. 32 RODO;
 - b) zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu zgodnie z art. 33 RODO;
 - c) zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 RODO;
 - d) dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO;
 - e) przeprowadzania konsultacji z organem nadzorczym zgodnie z art. 36 RODO;
 - 11) udostępniać Powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków w zakresie powierzenia przetwarzania danych. Procesor jest zobowiązany udostępnić wszelkie informacje i dokumenty w terminie 2 Dni Roboczych od przesłania żądania Powierzającego na adres wskazany w Załączniku nr 4.
4. Procesor zobowiązany jest prowadzić rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu Powierzającego, zawierający następujące informacje:
 - 1) imię i nazwisko lub nazwę oraz dane kontaktowe Procesora oraz Powierzającego, a gdy ma to zastosowanie – przedstawiciela Procesora oraz inspektora ochrony danych,
 - 2) kategorie przetwarzanych dokonywanych w imieniu Powierzającego,
 - 3) gdy ma to zastosowanie – informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO dokumentację odpowiednich zabezpieczeń,
 - 4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
 5. Procesor jest zobowiązany do wdrożenia i stosowania procedur służących wykrywaniu naruszeń ochrony danych osobowych oraz wdrażania właściwych środków naprawczych. Procesor jest zobowiązany do udostępnienia procedur, o których mowa w zdaniu poprzedzającym, na żądanie Powierzającego przekazane

za pośrednictwem e-maila na adres wskazany w Załączniku nr 4. Procesor jest zobowiązany do udzielenia odpowiedzi w terminie 3 Dni Roboczych od przestania przez Powierzającego żądania.

6. Po stwierdzeniu naruszenia ochrony danych osobowych. Procesor bez zbędnej zwłoki, jednak nie później niż 24 godzin od powzięcia wiadomości o naruszeniu, zgłasza ten fakt Powierzającemu, wskazując w zgłoszeniu:
 - 1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorii oraz przybliżoną liczbę osób, których dane dotyczą oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
 - 2) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
 - 3) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
 - 4) opis środków zastosowanych lub proponowanych przez Procesora w celu zapobieżeniu naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.
7. Zgłoszenie naruszenia ochrony danych osobowych następuje na adres mailowy wskazany w Załączniku nr 4.
8. Jeśli wszystkich informacji, o których mowa w ust. 6 powyżej, nie da się udzielić w tym samym czasie, Procesor ma obowiązek ich udzielać Powierzającemu sukcesywnie bez zbędnej zwłoki.
9. Do czasu przekazania Procesorowi instrukcji postępowania w związku z naruszeniem ochrony danych, Procesor podejmuje bez zbędnej zwłoki wszelkie działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
10. Bez wyraźnej instrukcji Powierzającego Procesor nie jest zobowiązany do informowania o naruszeniu ochrony danych osobowych organu nadzorczego ani osób, których dane dotyczą.
11. Procesor dokumentuje wszelkie naruszenia ochrony powierzonych mu przez Powierzającego danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, jak również udostępnia tę dokumentację Powierzającemu na jego żądanie.
12. Procesor ponosi odpowiedzialność za działania swoich pracowników i innych osób, przy pomocy których przetwarza powierzone dane osobowe, jak za własne działanie i zaniechanie.
13. Procesor jest uprawniony do dokonania dalszego powierzenia (podpowierzenia) przetwarzania danych osobowych innemu podmiotowi (dalej również: „**Podprocesor**”) wyłącznie na podstawie uprzedniej pisemnej zgody Powierzającego, która stanowi Załącznik nr 2 do Umowy. Lista podmiotów z których korzysta Procesor stanowi Załącznik nr 3 do Umowy. Powyższe nie wyklucza prawa Procesora do powierzenia przetwarzania danych osobowych powierzonych w ramach Umowy innemu podmiotowi po wcześniejszym zawiadomieniu Powierzającego. W szczególności Procesor informuje Powierzającego o zamiarze wyboru nowego Podprocesora spoza listy wskazanej w Załączniku nr 3 bez zbędnej zwłoki, nie później jednak niż w terminie 10 dni roboczych od planowanego dnia zawarcia umowy dalszego powierzenia przetwarzania z nowym Podprocesorem. W sytuacji w której Powierzający wyrazi sprzeciw wobec korzystania przez Procesora z Podprocesora, Procesor nie jest uprawniony do zawarcia umowy z Podprocesorem, którego dotyczy sprzeciw.
14. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Powierzającego, chyba, że obowiązek taki nakłada na Procesora prawo Unii lub prawo państwa członkowskiego, któremu podlega Procesor. W takim przypadku przed rozpoczęciem przetwarzania Procesor informuje Powierzającego o tym obowiązku prawnym na piśmie, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

15. Powierzenie danych osobowych do dalszego przetwarzania wymaga formy umowy pisemnej lub w przypadku, gdy stroną jest Procesor w państwie trzecim spełnienia wymagań zawartych w § 5 (przy zachowaniu formy pisemnej umowy). Zawarta umowa musi zawierać wszystkie zobowiązania określone w niniejszej umowie oraz precyzować czas, charakter i cel przetwarzania danych, z uwzględnieniem zakresu (lub kategorii) przetwarzanych danych.
16. Jeśli do wykonania, w imieniu Powierzającego, konkretnych czynności przetwarzania Procesor dokona dalszego powierzenia (podpowierzenia) przetwarzania danych osobowych Podprocesorowi, to Procesor zapewnia, iż Podprocesor wypełnia te same obowiązki ochrony danych osobowych, jakie zostały nałożone na Procesora w Umowie, w szczególności obowiązek zapewnienia wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzane przez niego danych osobowych było zgodne z wymogami RODO. Procesor ponosi pełną odpowiedzialność za wypełnienie tych obowiązków ochrony danych osobowych przez Podprocesora.
17. W przypadku, gdy Procesor dokonał dalszego powierzenia danych osobowych, Procesor zapewnia, iż Podprocesor wypełniać będzie, bezpośrednio w stosunku do Powierzającego, obowiązki wymienione w ust. 6, 7 oraz ust. 8-9 i ust. 11 powyżej.
18. Procesor zapewni również w umowie z Podprocesorem możliwość realizacji przez Powierzającego kontroli u Podprocesora (w tym możliwość przeprowadzania audytów, o których mowa w § 3 Umowy). Procesor jest zobowiązany poinformować Podprocesora, że informacje, w tym dane osobowe, na jego temat mogą być udostępnione Powierzającemu w celu wykonania przez niego uprawnień, o których mowa w zdaniu poprzedzającym.
19. Procesor odpowiada za szkody spowodowane przetwarzaniem danych osobowych w sposób naruszający przepisy RODO, jeśli nie dopełnił obowiązków nałożonych na niego przez RODO lub gdy działał poza zgodnymi z prawem instrukcjami Powierzającego lub wbrew tym instrukcjom.
20. Procesor ma obowiązek współdziałać z Powierzającym na jego żądanie w zakresie ustalenia przyczyn szkody wyrządzonej osobie, której dane dotyczą, jak również zapewnia, że obowiązek ten będzie wypełniać bezpośrednio Podprocesor w stosunku do Powierzającego.
21. W przypadku, gdy za szkodę spowodowaną przetwarzaniem odpowiadają zarówno Powierzający, jak i Procesor, ponoszą oni odpowiedzialność solidarną za całą szkodę.
22. W przypadku, gdy Powierzający zapłacił odszkodowanie za całą wyrządzoną szkodę spowodowaną przetwarzaniem, ma prawo żądania od Procesora zwrotu części odszkodowania odpowiadającej części szkody, za którą ponosi on odpowiedzialność.
23. Niezwłocznie, jednak nie później niż w ciągu 2 Dni Roboczych Procesor zobowiązany jest informować (o ile nie doprowadzi to do naruszenia przepisów obowiązującego prawa) Powierzającego o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych przez Procesora, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych, skierowanej do Procesora, o wszelkich kontrolach i inspekcjach dotyczących przetwarzania danych osobowych przez Procesora, w szczególności prowadzonych przez organ nadzoru, a także o wszelkich żądaniach i skargach osób, których dane dotyczą związanych z przetwarzaniem ich danych osobowych.
24. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom trzecim w związku z powierzeniem przetwarzania danych, zgodnie z przepisami Kodeksu cywilnego, z zastrzeżeniem postanowień RODO wskazanych powyżej.

§ 3 **Prawo kontroli**

1. Powierzający posiada prawo kontroli właściwego przetwarzania przez Procesora powierzonych mu danych osobowych. Procesor na każdy pisemny wniosek Powierzającego zobowiązany jest do udzielenia pisemnej informacji dotyczącej przetwarzania powierzonych mu danych osobowych, w terminie 5 Dni Roboczych od dnia otrzymania wniosku Powierzającego.
2. Procesor umożliwia Powierzającemu lub upoważnionemu przez Powierzającego audytorowi przeprowadzenie audytów, w tym inspekcji, i zobowiązuje się współpracować z Powierzającym w zakresie dotyczącym wyłącznie realizacji Umowy. Powierzający zobowiązuje się, że jako upoważniony audytor nie zostanie wyznaczony podmiot prowadzący pośrednio lub bezpośrednio działalność konkurencyjną w stosunku do działalności prowadzonej przez Procesora. Ewentualne czynności kontrolne będą prowadzone na koszt i ryzyko Powierzającego.
3. Termin przeprowadzenia kontroli zostanie ustalony z Procesorem, jednak kontrola nie może odbyć się wcześniej niż w terminie 5 Dni Roboczych od przekazania Procesorowi żądania, na adres mailowy wskazany w Załączniku nr 4.
4. Procesor niezwłocznie informuje Powierzającego, jeśli wydane Procesorowi polecenie, w oparciu o § 2 ust. 3 pkt 10 Umowy lub w oparciu o ust. 1 powyżej, stanowi naruszenie RODO lub innych powszechnie obowiązujących przepisów.
5. Po przeprowadzonym audycie przedstawiciel Powierzającego lub upoważniony przez Powierzającego przedstawiciel audytora sporządza protokół pokontrolny, który podpisują przedstawiciele obu Stron. Procesor zobowiązuje się w terminie uzgodnionym z Powierzającym, dostosować do zaleceń pokontrolnych zawartych w protokole, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
6. Powierzający ma także prawo żądać od Procesora składania pisemnych wyjaśnień dotyczących realizacji Umowy. Procesor zobowiązuje się odpowiedzieć niezwłocznie, jednak nie później niż w terminie 3 Dni Roboczych.
7. Procesor jest zobowiązany zapewnić w umowie z dalszym podmiotem przetwarzającym możliwość przeprowadzania przez Powierzającego (lub podmiot zewnętrzny, któremu Powierzający zleci wykonanie audytu) audytu zgodności przetwarzania danych osobowych przez dalszy podmiot przetwarzający z Umową na zasadach określonych w § 3 ust. 1 – 3.
8. Koszty związane z przeprowadzeniem audytu ponosi podmiot, który zlecił przeprowadzenie audytu, bez prawa do żądania zwrotu takich kosztów ani zapłaty dodatkowego wynagrodzenia.
9. W przypadku, gdy Procesor audytowany jest za zgodność z przepisami RODO przez niezależny podmiot trzeci z własnej inicjatywy, Procesor zobowiązuje się udostępnić Powierzającemu na jego żądanie wyniki tego audytu bez zbędnej zwłoki, nie później niż w terminie 3 dni roboczych.

§ 4

Wsparcie Powierzającego w wykonywaniu praw określonych w rozdziale III RODO

1. Zgodnie z art. 28 ust. 3 pkt. e RODO biorąc pod uwagę charakter przetwarzania, Procesor w miarę możliwości pomaga Powierzającemu 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 RODO.
2. Procesor jest zobowiązany do wsparcia Powierzającego w zakresie realizacji następujących praw podmiotów danych osobowych:
 - 1) obowiązku informacyjnego przewidzianego w art. 13 i art. 14 RODO;
 - 2) prawa dostępu do danych;
 - 3) prawa do sprostowania danych;

- 4) prawa do usunięcia danych;
 - 5) prawa do ograniczenia przetwarzania;
 - 6) obowiązku poinformowania o sprostowaniu lub usunięciu danych lub o ograniczeniu przetwarzania;
 - 7) prawa do przenoszenia danych;
 - 8) prawa do sprzeciwu;
 - 9) kwestii związanych z prawem do niepodlegania zautomatyzowanemu przetwarzaniu danych, w tym profilowaniu.
3. Żądanie Powierzającego w zakresie uzyskania wsparcia w związku z realizacją praw wymienionych w ust. 2 zostanie niezwłocznie przekazane Procesorowi na adres mailowy wskazany w Załączniku nr 4.
 4. Procesor w ciągu 2 Dni Roboczych od otrzymania żądania potwierdzi jego otrzymanie Powierzającemu.
 5. Procesor w terminie 5 Dni Roboczych od terminu wskazanego w ust. 4 poinformuje Powierzającego o wykonaniu przekazanego żądania.
 6. Jeżeli Procesor nie jest w stanie zrealizować żądania przekazanego mu przez Powierzającego jest ono zobowiązany do przygotowania i przekazania Powierzającemu wyjaśnienia opisującego przyczyny dla których zrealizowanie żądania Powierzającego było niemożliwe.

§ 5

Ocena Procesora z wymaganiami RODO

Powierzający dokona oceny Procesora na podstawie uzupełnionej i podpisanej ankiety (oryginał), potwierdzającej stosowanie środków organizacyjnych i technicznych w zakresie ochrony danych osobowych, której wzór stanowi Załącznik nr 5 do Umowy.

§ 6

Transfer danych osobowych do państw trzecich

1. Procesor nie może przekazywać (transferować) danych osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym (dalej również: „EOG”), chyba że Powierzający udzieli mu uprzedniej, pisemnej pod rygorem nieważności, zgody zezwalającej na taki transfer zgodnie z §2 ust. 13
2. Jeśli Powierzający udzieli Procesorowi uprzedniej zgody na przekazanie danych osobowych do państwa trzeciego, Procesor może dokonać transferu tych danych osobowych tylko wtedy, gdy:
 - 1) państwo docelowe zapewnia adekwatny poziom ochrony danych osobowych do tego, który obowiązuje w Unii Europejskiej lub
 - 2) Powierzający i Procesor lub Podprocesor zawarli umowę w oparciu o standardowe klauzule umowne lub wdrożyli inny mechanizm, który zgodnie z przepisami prawa legalizuje transfer danych do państwa trzeciego.

§ 7

Adresy stron i dane osób

1. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana na adresy Stron wskazane w Załączniku nr 4.
2. Procesora w kontaktach z Powierzającym oraz Powierzający w kontaktach z Procesorem w zakresie ustaleń Umowy reprezentować będą osoby wskazane w Załączniku nr 4.
3. Zmiana adresów i danych tych osób nie stanowi zmiany Umowy. O każdej zmianie danych zawartych w Załączniku nr 4, Strony powiadomią się na piśmie, za potwierdzeniem odbioru lub drogą elektroniczną.

§ 8
Czas trwania Umowy

1. Po zakończeniu świadczenia usług związanych z przetwarzaniem Procesor ma obowiązek usunąć lub zwrócić Powierzającemu – zależnie od decyzji Powierzającego – wszelkie dane osobowe, które zostały mu powierzone, jak również usunąć wszelkie ich istniejące kopie, chyba że powszechnie obowiązujące przepisy nakazują przechowywanie tych danych osobowych.
2. W terminie 5 Dni Roboczych od wygaśnięcia lub rozwiązania niniejszej umowy Procesor przesyła Powierzającemu pisemne potwierdzenie zniszczenia bądź zwrotu danych osobowych o następującej treści: „..... (nazwa Procesora) oświadcza, że dokonał *zniszczenia* bądź *zwrotu* (*należy wybrać właściwe*) wszelkich danych osobowych powierzonych do przetwarzania w związku z realizacją umowy zawartej z Narodowym Instytutem Kardiologii Stefana Kardynała Wyszyńskiego – Państwowym Instytutem Badawczym w Warszawie w dniu nr, jak również ich kopii, oraz przekazał nośniki danych, z których usunięcie danych osobowych nie było możliwe zgodnie z protokołem z dn.”.. Potwierdzenie należy przelać na adres e-mail Powierzającego wskazany w Załączniku nr 4.
3. Powierzający jest uprawniony do rozwiązania Umowy bez wypowiedzenia, jeżeli Procesor nie wypełnia obowiązków wskazanych w § 2 Umowy, lub uniemożliwia Powierzającemu skorzystania z prawa kontroli wskazanego w § 3 Umowy.
4. W przypadku podpowierzenia przetwarzania danych osobowych Procesor zobowiązuje się do zawarcia w umowach z Podprocesorami postanowień, zgodnie z którymi umowy podpowierzenia danych będą ulegały automatycznemu rozwiązaniu w razie zakończenia obowiązywania niniejszej Umowy.

§ 9
Postanowienia końcowe

1. Niniejsza Umowa podlega prawu polskiemu. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej Strony.
2. W sprawach, które nie zostały uregulowane Umową, znajdują zastosowanie odpowiednie przepisy Kodeksu cywilnego, RODO oraz innych obowiązujących przepisów z zakresu ochrony danych osobowych, a także przepisy regulujące prawa pacjenta, zasady wykonywania zawodów medycznych oraz prowadzenia działalności leczniczej.
3. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem nieważności, z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.
4. Procesor nie może przenieść praw lub obowiązków wynikających z niniejszej Umowy bez pisemnej zgody Powierzającego.
5. O ile Umowa główna nie stanowi inaczej, wszelkie spory w związku z niniejszą Umową zostaną poddane pod rozstrzygnięcie sądu powszechnego miejscowo właściwego ze względu na siedzibę Powierzającego.
6. Umowa została zawarta w postaci elektronicznej.
7. Umowa została zawarta z chwilą złożenia ostatniego z podpisów elektronicznych stosownie do wskazania znacznika czasu ujawnionego w szczegółach dokumentu zawartego w postaci elektronicznej.

W imieniu Powierzającego

W imieniu Procesora

ZAŁĄCZNIK NR 1
ZAKRES PRZETWARZANIA

Kategoria osób, których dane dotyczą	Rodzaj danych osobowych

ZAŁĄCZNIK NR 2
PISEMNA ZGODA POWIERZAJĄCEGO NA KORZYSTANIE PRZEZ PROCESORA Z USŁUG PODPROCESORÓW

Działając w imieniu Powierzającego, zgodnie z § 2 ust. 13 Umowy, niniejszym wyrażam zgodę na korzystanie przez Procesora z Podprocesorów w ramach świadczenia usług na podstawie niniejszej Umowy.

Oświadczam, iż Procesor przedstawił mi listę Podprocesorów z których usług korzysta. Lista stanowi załącznik nr 3 do Umowy.

W imieniu Powierzającego

..... / data

ZAŁĄCZNIK NR 3
LISTA PODPROCESORÓW Z USŁUG KTÓRYCH KORZYSTA PROCESOR

1.
2.
3.

ZAŁĄCZNIK NR 4
DANE KONTAKTOWE STRON

1. Dane kontaktowe Stron:

- a. wszelka korespondencja w sprawach związanych z Umową będzie kierowana do **Powierzającego** na następujące dane kontaktowe – adres: Narodowy Instytut Kardiologii Stefana kardynała Wyszyńskiego Państwowy Instytut Badawczy ul. Alpejska 42, 04-628 Warszawa tel.; email: , iod@ikard.pl
- b. wszelka korespondencja w sprawach związanych z Umową będzie kierowana do **Procesora** na następujące dane kontaktowe – adres: ,
tel.email:

2. Dane przedstawicieli Stron:

- a. **Powierzającego** w kontaktach z Procesorem w zakresie ustaleń Umową reprezentować będą następujące osoby:
.....
Narodowy Instytut Kardiologii Stefana kardynała Wyszyńskiego Państwowy Instytut Badawczy, ul. Alpejska 42, 04-628 Warszawa tel. email:
Inspektor Ochrony Danych Narodowy Instytut Kardiologii Stefana kardynała Wyszyńskiego Państwowy Instytut Badawczy, ul. Alpejska 42, 04-628 Warszawa, e-mail: iod@ikard.pl
- b. **Procesora** w kontaktach z Powierzającym w zakresie ustaleń Umową reprezentować będą następujące osoby:
.....
adres
tel. email:



**ANKIETA WERYFIKACJI PROCESORA
Z WYMAGANAMI OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH 2016/679¹**

Nazwa Procesora	
Adres Procesora	
Dane kontaktowe	

PYTANIA DOTYCZĄCE KWESTII ORGANIZACYJNYCH		TAK	NIE	NIE DOTY- CZY	UWAGI
1.	Czy zgodnie z art. 29 RODO osoby przetwarzające dane osobowe w imieniu i na polecenie Procesora otrzymały upoważnienia do przetwarzania tych danych, z wyszczególnieniem zakresu przetwarzania?				
2.	Czy osoby przetwarzające dane w imieniu i na polecenie Procesora zobowiązały się do zachowania w poufności tych danych oraz sposobów ich przetwarzania?				
3.	Czy Procesor wyznaczył Inspektora Ochrony Danych (dalej: IOD)?				
	Jeżeli TAK, proszę podać imię i nazwisko oraz dane kontaktowe IOD.				
4.	W przypadku braku konieczności powołania IOD – czy Procesor wyznaczył osobę odpowiedzialną za ochronę danych osobowych?				

¹ Zgodnie z art. 28 ust. 1 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, dalej zwane „RODO”), (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)

	Jeżeli TAK, proszę podać imię i nazwisko oraz dane kontaktowe osoby, która jest odpowiedzialna za ochronę danych osobowych.				
5.	Czy Procesor realizuje wymagania art. 30 ust. 2 RODO (czy prowadzi rejestr kategorii czynności przetwarzania)?				
6.	Czy Procesor opracował politykę ochrony danych osobowych lub inną dokumentację opisującą zasady ochrony danych osobowych?				
7.	Czy Procesor zapewnia, że nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie oraz zapoznany z obowiązującymi przepisami prawa?				
8.	Czy Procesor dba o doskonalenie wiedzy swoich pracowników w zakresie ochrony danych osobowych poprzez cykliczne szkolenia?				
9.	Czy Procesor stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO?				
10.	Czy Procesor korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy gwarantują odpowiednie bezpieczeństwo danych osobowych (zgodność z RODO) oraz czy te podmioty zostały przez niego zweryfikowane? (jeżeli dotyczy)				
11.	Czy Procesor podpisał stosowne umowy powierzenia z podwykonawcami? (jeżeli dotyczy)				
12.	Czy w ciągu ostatnich dwóch lat Procesor przeprowadził kompleksowy audyt zgodności z przepisami o ochronie danych osobowych?				
13.	Czy wynik audytu, o którym mowa powyżej został udokumentowany?				
14.	Czy Procesor wdraża nowe rozwiązania w oparciu o zasadę „privacy by design”?				

15.	Czy Procesor działa zgodnie z zasadą „privacy by default”?				
16.	Czy Procesor wypracował zasady realizacji praw Podmiotów Danych w zakresie ochrony danych osobowych, o którym mowa w art. 15-22 RODO?				
17.	Czy Procesor dokonuje szacowania ryzyka przetwarzania danych osobowych?				
18.	Czy wyniki przeprowadzonego szacowania ryzyka zostały udokumentowane?				
19.	Czy Procesor dokonała oceny skutków dla ochrony danych osobowych dla czynności przetwarzania (o których mowa w art. 35 RODO i w wykazie rodzajów operacji przetwarzania danych wymagających oceny skutków dla ochrony ich danych, opublikowanym w komunikacie Prezesa Urzędu Ochrony Danych Osobowych), a które wchodzi w zakres planowanej?				
20.	Czy wyniki przeprowadzonej oceny skutków dla ochrony danych osobowych zostały udokumentowane?				
PYTANIA DOTYCZĄCE BEZPIECZEŃSTWA FIZYCZNEGO					
21.	Czy Procesor opracował procedury dotyczące nadawania fizycznego dostępu do pomieszczeń, w których przechowywana jest dokumentacja zawierająca dane osobowe, zapewniające weryfikację tożsamości i zakres nadawanego dostępu?				
22.	Czy istnieją mechanizmy kontroli dostępu do tych pomieszczeń?				
23.	Czy dostęp do pomieszczeń pozostających w dyspozycji Procesor po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany?				

24.	Czy Procesor posiada działający system alarmowy oraz system monitoringu przemysłowego obejmujący miejsca, gdzie przechowywana jest dokumentacja medyczna oraz inne dane osób fizycznych?				
PYTANIE DOTYCZĄCE STOSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA W ŚRODOWISKU INFORMATYCZNYM					
25.	Czy Procesor zapewnia jednoznaczną identyfikację działań w systemach informatycznych za pomocą unikalnego ID Użytkownika?				
26.	Czy system, w którym są przetwarzane dane osobowe posiada funkcjonalności pozwalające na jednoznaczne wskazanie i odtworzenie działań użytkownika o konkretnym ID, w określonym czasie?				
27	Czy Procesor posiada formalne zasady zarządzania hasłami (minimalna długość, złożoność, częstotliwość zmiany, możliwość powtórzenia hasła, szyfrowanie przechowywanych haseł), które są wdrożone?				
28.	Czy urządzenia (np. tablety, smartfony), i komputery osobiste, na których przetwarzane są dane osobowe, mają włączoną automatyczne blokowanie ekranu po okresie bezczynności użytkownika?				
29.	Czy u Procesora stosuje politykę tzw. „czystego biurka”?				
30.	Czy dane osobowe gromadzone w formie papierowej przechowywane są w zamkniętych szafach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?				
31.	Czy dokumenty w formie papierowej są niszczone przy pomocy niszczarek dokumentów o odpowiedniej klasie bezpieczeństwa?				
32.	Czy Procesor zabezpieczył urządzenia przenośne oraz nośniki pamięci, wynoszone poza obszar przetwarzania kryptograficznie?				

33.	Czy zapewniono mechanizmy umożliwiające szybkie przywrócenie dostępu do danych osobowych oraz przywrócenie systemu w przypadku wystąpienia incydentu fizycznego lub technicznego?				
34.	Czy Procesor prowadzi monitorowanie nieudanych prób zalogowania się do systemu oraz blokowanie konta po określonej nieudanej liczbie prób zalogowania?				
35.	Czy zostały wprowadzone mechanizmy kopii zapasowych, czy kopie zapasowe są regularnie tworzone?				
36.	Czy kopie zapasowe są testowane okresowo pod kątem ich odtworzenia?				
37.	Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach?				
38.	Czy Procesor jest właścicielem infrastruktury fizycznej (serwerownia, serwery) na której funkcjonują systemy IT, w których są przetwarzane dane osobowe?				
39.	Czy Procesor wyznaczył osobę odpowiedzialną za bezpieczeństwo IT?				
	Jeśli tak, proszę podać służbowe dane kontaktowe tej osoby (imię, nazwisko, nr telefonu, adres e-mail).				
41.	Czy Procesor korzysta z chmury publicznej (cloud computing)?				
	Jeżeli tak, to z jakiego rozwiązania?				
42.	Czy rozwiązanie chmurowe pozwala na przetwarzanie danych zgodnie z obowiązującymi regulacjami?				
43.	W przypadku stosowania rozwiązań w chmurze, czy stosowane są metody ograniczające dostęp do danych dla osób nieuprawnionych np. szyfrowanie danych?				
44.	Czy systemy IT, w których są przetwarzane dane osobowe zarządzane są przez podmiot zewnętrzny?				

45.	Jeśli administratorem systemu IT lub dostawcą utrzymującym system jest podmiot zewnętrzny, proszę wskazać czy posiada on zdalny dostęp do środowiska IT?				
46.	Jeżeli do systemów IT ma dostęp podmiot zewnętrzny, to czy z podmiotem tym podpisana została umowa powierzenia przetwarzania danych osobowych lub w przypadku dalszego powierzenia – umowa dalszego powierzenia danych osobowych?				
47.	Czy użytkownicy mają dostęp zdalny do zasobów? Jeśli tak, to w jaki sposób zabezpieczony jest kanał komunikacji?				
48.	Czy Procesor gwarantuje ciągłość funkcjonowania swojej platformy?				
49.	Czy bezpieczeństwo przetwarzania jest potwierdzane certyfikatami bezpieczeństwa, normami?				

.....
Data i podpis Procesora

Ocena Inspektora Ochrony Danych w Narodowym Instytucie Kardiologii

Rekomenduję zawarcie umowy powierzenia przetwarzania danych osobowych

.....
Data i podpis IOD

Nie rekomenduję zawarcia umowy powierzenia przetwarzania danych osobowych

.....
Data i podpis IOD