

Załącznik nr 4 do Umowy

UMOWA powierzenia przetwarzania danych osobowych

zwana dalej „Umową”, zawarta w Warszawie pomiędzy:

Agencją Oceny Technologii Medycznych i Taryfikacji z siedzibą w Warszawie, przy ul. Przeskok 2 (kod poczt. 00-032), działającą na podstawie art. 31 m ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, NIP: 5252347183, REGON: 140278400, zwaną dalej „**Administratorem**”, reprezentowaną przez:

Robert Świś – Dyrektor Biura Prawnego na podstawie udzielonego pełnomocnictwa,

a

..... z siedzibą w przy al. (kod poczt.), wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m.st. Krajowego Rejestru Sądowego, pod numerem KRS, posiadającą numery: NIP:, REGON:, zwaną dalej: „Wykonawcą”, zwaną dalej „**Podmiotem Przetwarzającym**” lub „**Stroną**”, reprezentowaną przez:

.....

łącznie zwanymi dalej „**Stronami**” lub każda z osobna „**Stroną**”.

§ 1.

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi Przetwarzającemu do przetwarzania dane osobowe w trybie określonym w art. 28 ust. 3 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. Urz. L 119 z 04.05.2016, str. 1 ze zm., zwanym dalej RODO), w związku z zawarciem przez Strony umowy dotyczącej dostawy Oprogramowania i wsparcia technicznego, zwanej dalej „**Umową Główną**”.
2. Przedmiotem powierzenia są dane osobowe zwykłe. Dane te będą przetwarzane wyłącznie w celu realizacji Umowy Głównej.

§ 2.

Weryfikacja podmiotu przetwarzającego

1. Podmiot Przetwarzający zobowiązuje się, przy przetwarzaniu danych osobowych powierzonych Umową, do stosowania odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.

2. Podmiot Przetwarzający określa stosowane środki organizacyjne i techniczne, o których mowa w ust. 1 powyżej, w załączniku A do Umowy.

§ 3.

Obowiązki Podmiotu Przetwarzającego

1. Podmiot Przetwarzający przetwarza dane osobowe wyłącznie w celu realizacji Umowy Głównej i na udokumentowane polecenie lub instrukcje Administratora, włączając w to przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na Podmiot Przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega; w takim przypadku przed rozpoczęciem przetwarzania Podmiot Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
2. Jeżeli Podmiot Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydawanych przez Administratora poleceń lub instrukcji, natychmiast poinformuje Administratora o stwierdzonej wątpliwości, pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu. Podmiot Przetwarzający dokumentuje okoliczność poinformowania Administratora o powziętych wątpliwościach.
3. Podmiot Przetwarzający zobowiązuje się do dołożenia należytej staranności przy przetwarzaniu powierzonych Umową danych osobowych.
4. Podmiot Przetwarzający będzie prowadzić rejestr kategorii czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 2 RODO, dokonywanego w imieniu Administratora.
5. Dostęp do danych osobowych przetwarzanych przez Administratora mogą uzyskać wyłącznie osoby upoważnione w formie pisemnej przy założeniu, że dostęp tych osób jest niezbędny do wykonania Umowy i wynikających z niej zadań. Podmiot Przetwarzający udokumentuje na żądanie Administratora udzielenie upoważnień we wskazanej formie.
6. Podmiot Przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 lit. b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie Przetwarzającym, jak i po jego ustaniu.
7. Podmiot Przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie dane osobowe i ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. W terminie nie dłuższym, niż 7 dni od zakończenia Umowy, bez wezwania Administratora, po usunięciu danych osobowych i ich kopii, Podmiot Przetwarzający przekaze Administratorowi protokół potwierdzający wykonanie tego obowiązku.
8. W miarę możliwości Podmiot Przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
9. Podmiot Przetwarzający zobowiązuje się do współpracy w zakresie wykonywania żądań podmiotów danych związanych z przetwarzanymi danymi osobowymi, z zastrzeżeniem, że Podmiot Przetwarzający nie realizuje samodzielnie wniosków osób, których dane dotyczą, np. w zakresie dostępu do danych osobowych. Wszelkie działania w tym zakresie są dopuszczalne po uzgodnieniu z Administratorem.
10. Podmiot Przetwarzający informuje Administratora, w terminie nie dłuższym niż 3 dni robocze od otrzymania żądania osoby fizycznej, której dane osobowe powierzono, o każdym takim żądaniu. Jednocześnie Podmiot Przetwarzający przekazuje wszystkie informacje, którymi dysponuje, dotyczące przedmiotu żądania.

11. Podmiot Przetwarzający informuje Administratora o incydentach, które mogłyby doprowadzić do naruszenia ochrony danych. Przekazanie informacji o takich zdarzeniach powinno nastąpić bez zbędnej zwłoki, nie później niż w ciągu **24 godzin** od stwierdzenia takiego zdarzenia lub podejrzenia, na adres: iod@aotm.gov.pl.
12. Podmiot Przetwarzający, realizując obowiązek określony w ust. 11 powyżej, przekazuje Administratorowi wszelkie niezbędne informacje, w szczególności o: charakterze naruszenia (podając kategorie i przybliżoną liczbę osób, których może dotyczyć naruszenie, kategorie i przybliżoną liczbę wpisów danych, których dotyczy naruszenie), możliwych konsekwencjach naruszenia, działaniach podjętych w celu usunięcia naruszenia i zabezpieczenia danych osobowych, wdrożonych procedurach i działaniach eliminujących takie zdarzenia w przeszłości.
13. Podmiot Przetwarzający zobowiązuje się niezwłocznie zawiadomić Administratora o każdym żądaniu udostępnienia danych osobowych, w tym żądaniach właściwych organów państwowych, chyba, że z przepisów prawa wynika zakaz informowania o takim żądaniu.

§ 4.

Prawo kontroli

1. Administrator będzie realizował prawo kontroli w celu oceny, czy środki organizacyjne i techniczne zastosowane przez Podmiot Przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych odpowiadają postanowieniom Umowy. Kontrola może obejmować w szczególności zakres upoważnienia do przetwarzania danych osobowych, liczbę osób upoważnionych i zasady odwoływania upoważnienia.
2. Administrator uprzedzi Podmiot Przetwarzający o zamiarze przeprowadzenia kontroli na 7 dni kalendarzowych wcześniej.
3. Podmiot Przetwarzający udzieli odpowiedzi na każde pytanie Administratora dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych oraz przedstawi niezbędne informacje lub dokumenty, zależnie od żądania Administratora.
4. Podmiot Przetwarzający usunie uchybienia stwierdzone przez Administratora podczas kontroli. Usunięcie uchybień nastąpi w terminie wskazanym przez Administratora nie dłuższym, niż 7 dni.

§ 5.

Dalsze powierzenie danych do przetwarzania

1. W przypadku korzystania z usług innego podmiotu przetwarzającego, Podmiot Przetwarzający przedstawi Administratorowi wykaz dalszych podmiotów przetwarzających.
2. Jednocześnie Podmiot Przetwarzający przeprowadzi odpowiednią weryfikację dalszych podmiotów przetwarzających. Weryfikacja ma na celu ocenę, czy inny Podmiot Przetwarzający gwarantuje odpowiedni poziom ochrony danych osobowych.
3. Podmiot Przetwarzający zapewnia, że w przypadku, gdy korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w Umowie, w tym obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.
4. Podmiot Przetwarzający odpowiada wobec Administratora za niewywiązanie się z obowiązków ochrony danych przez inny podmiot przetwarzający, z którego usług korzysta.

5. Podstawą przekazania powierzonych danych do państwa trzeciego lub organizacji międzynarodowej może być jedynie udokumentowane, pisemne polecenie Administratora, 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 o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

§ 6.

Odpowiedzialność

1. Jeżeli do Administratora zostaną skierowane przez osoby trzecie roszczenia cywilnoprawne lub zostaną wszczęte wobec niego przez organy publiczne (w tym właściwe organy nadzorcze) postępowania z powodu naruszenia przez Podmiot Przetwarzający obowiązków wynikających z Umowy, RODO lub innych przepisów prawa powszechnie obowiązującego dotyczące ochrony danych osobowych, Podmiot Przetwarzający zwolni Administratora z ponoszenia jakiejkolwiek odpowiedzialności cywilnoprawnej lub naprawi szkodę poniesioną z powyższego tytułu przez Administratora.
2. Podmiot Przetwarzający odpowiada także za szkody wynikłe z udostępnienia lub wykorzystania danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie osobom nieuprawnionym powierzonych do przetwarzania danych osobowych.
3. Podmiot przetwarzający poinformuje Administratora danych o każdym postępowaniu dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych powierzonych Umową. Dotyczy to w szczególności postępowań administracyjnych, sądowych, wydanych decyzji, rozstrzygnięć czy orzeczeń, dotyczących przetwarzania tych danych osobowych, kierowanych do Podmiotu przetwarzającego, a także wszelkich kontroli w zakresie przetwarzania u Podmiotu Przetwarzającego tych danych osobowych, włączając w to kontrole prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych.

§ 7.

Czas trwania umowy

Umowa obowiązuje przez okres obowiązywania Umowy Głównej.

§ 8.

Rozwiązanie umowy

Administrator może rozwiązać Umowę ze skutkiem natychmiastowym w przypadku istotnego naruszenia jej postanowień przez Podmiot przetwarzający.

§ 9.

Postanowienia końcowe

1. Umowa ma zastosowanie do wszystkich danych osobowych powierzonych Podmiotowi Przetwarzającemu do przetwarzania mocą Umowy.
2. Umowa zastępuje, w zakresie powierzenia przetwarzania danych osobowych do których ma zastosowanie, wszelkie wcześniejsze umowy i porozumienia zawarte pomiędzy Stronami.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności albo równoważnej formy elektronicznej.
4. We wszelkich sprawach nieobjętych Umową stosuje się przepisy prawa polskiego.

Załącznik A

do Umowy powierzenia przetwarzania danych osobowych - oświadczenie Podmiotu Przetwarzającego

Oświadczenie Podmiotu Przetwarzającego

Osoby wykonujące operacje na danych osobowych otrzymały upoważnienia do przetwarzania danych, w których został określony zakres przetwarzanych przez te osoby danych.

Osoby upoważnione zostały zobligowane do zachowania poufności.

Dostęp do danych powierzonych danych osobowych mają tylko uprawnieni pracownicy oraz współpracownicy, zgodnie z zasadą „wiedzy koniecznej”.

Została opracowana i wdrożona dokumentacja ochrony danych osobowych. Zostały wdrożone procedury przesyłania danych drogą elektroniczną.

Zostały wdrożone procedury zabezpieczania nośników danych osobowych. Zostały zapewnione niezbędne środki techniczne do ochrony nośników danych. Zostały wdrożone procedury postępowania przy naruszeniach ochrony danych. Dokumentacja ochrony danych podlega okresowym przeglądom.

Podmiot Przetwarzający przeprowadza okresowe audyty zgodności z RODO.

Podmiot Przetwarzający jest w stanie wykazać zgodność przetwarzania z postanowieniami niniejszej umowy powierzenia.

Osoby upoważnione przechodzą szkolenia z ochrony danych osobowych.

Zostały wdrożone środki ochrony elektronicznych nośników informacji oraz sprzętu komputerowego i mobilnego jak szyfrowanie, zapory systemowe, antywirusy.

Załącznik B

do Umowy powierzenia przetwarzania danych osobowych – protokół usunięcia danych

**Oświadczenie
w sprawie zniszczenia danych osobowych przez Podmiot Przetwarzający**

Oświadczam, że zostały zniszczone/usunięte wszystkie dane osobowe (w tym kopie zapasowe), które były przetwarzane w związku z wykonywaniem umowy nr/...../...../ r.

Protokół zniszczenia danych dotyczy (należy podać krótki opis danych osobowych):

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

Termin usunięcia danych osobowych:

.....

Podmiot Przetwarzający

.....