Załącznik nr 2

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta pomiędzy:

[...] z siedzibą we [...], przy ul. [...], 00-000 Miasto, wpisanym do rejestru przedsiębiorców przez Sąd Rejonowy dla [...], [...] Wydział Gospodarczy Krajowego Rejestru Sądowego, za numerem KRS **********, NIP **********, REGON *********, reprezentowanym przez:

[...] – [...]

zwaną dalej „**Administratorem**",

a

[...] z siedzibą we [...], przy ul. [...], 00-000 Miasto, wpisanym do rejestru przedsiębiorców przez Sąd Rejonowy dla [...], [...] Wydział Gospodarczy Krajowego Rejestru Sądowego, za numerem KRS **********, NIP **********, REGON *********, reprezentowanym przez:

[...] – [...]

zwaną dalej „**Podmiotem przetwarzającym**".

ZWAŻYWSZY, ŻE:

a. Od dnia 25 maja 2018 r. znajduje zastosowanie 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 („**RODO**"),

b. Strony zawarły w dniu [...] umowę na usługę archiwizacji dokumentacji Administratora (dalej Umowa Główna),

c. Warunkiem realizacji Umowy Głównej jest przetwarzanie danych osobowych przez Podmiot przetwarzający,

STRONY POSTANOWIŁY, CO NASTĘPUJE:

§ 1
Przedmiot

1. Umowa powierzenia reguluje kwestię powierzenia i ochrony danych osobowych przetwarzanych przez Podmiot przetwarzający w związku z realizacją Umowy w związku z obowiązkiem stosowania RODO.
2. Postanowienia Umowy Głównej odnoszące się do powierzenia i ochrony danych osobowych przetwarzanych w związku z wykonywaniem Umowy pozostają w mocy, o ile nie są sprzeczne z postanowieniami niniejszego Umowy powierzenia.

§ 2

Powierzenie przetwarzania danych

1. Administrator oświadcza, że jest administratorem danych osobowych powierzanych w ramach niniejszej Umowy w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady z dnia 26 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, zwanego dalej RODO.
2. Dla potrzeb realizacji Umowy Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie niezbędnym do realizacji Umowy.
3. Niniejszy Umowa powierzenia stanowi polecenie przetwarzania w rozumieniu art. 28 ust. 3 lit. a) RODO.

   Podmiot przetwarzający przetwarza powierzone dane osobowe wyłącznie na rzecz Administratora i w celu wskazanym przez Administratora.
4. Powierzenie przetwarzania obejmuje w swoim zakresie wyłącznie dane osobowe niezbędne do realizacji Umowy przez Podmiot przetwarzający. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych na potrzeby związane z przechowywaniem archiwalnej dokumentacji medycznej zawierającej dane określone w art. 25 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzecznik Praw Pacjenta (t.j. Dz. U. z 2023 r. poz. 1545 z późn. zm.) a także w przepisach wykonawczych do tej ustawy.
5. Podmiot przetwarzający zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
6. Podmiot przetwarzający dopuszcza do przetwarzania powierzonych danych osobowych wyłącznie osoby posiadające upoważnienia.
7. Procesor wskazuje, że powołał Inspektora ochrony danych osobowych: Bartosz Terlecki, tel. 32/7219954 , e-mail iod@archidoc.pl
8. Administrator wskazuje, że powołał Inspektora ochrony danych osobowych, z którym można się kontaktować w sprawie danych osobowych przetwarzanych na podstawie niniejszej umowy na adres korespondencyjny Administratora lub poprzez _e-mail iod@wss5.pl.
9. Z zastrzeżeniem postanowień Umowy Głównej, Podmiot przetwarzający ponosi odpowiedzialność za rzeczywistą szkodę względem Administratora w przypadku wystąpienia przeciwko Administratorowi z roszczeniami przez osoby, których bezpieczeństwo danych osobowych naruszono w wyniku realizacji niniejszego Porozumienia z przyczyn leżących po stronie Podmiotu przetwarzającego.
10. Podmiot przetwarzający prowadzić będzie dokumentację opisującą sposób przetwarzania danych osobowych, w szczególności rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zawierający informacje o:
    a. nazwie oraz danych kontaktowych Podmiotu przetwarzającego oraz Administratora, a także inspektora ochrony danych;
    b. kategoriach przetwarzań dokonywanych w imieniu Administratora;

c. ogólnym opisie technicznych i organizacyjnych środków bezpieczeństwa, służących do zabezpieczenia powierzonych danych osobowych.

11. Podmiot przetwarzający niezwłocznie poinformuje Administratora o żądaniach na podstawie art. 15-22 RODO, z którymi osoby, których dane dotyczą zwróciły się bezpośrednio do Podmiotu przetwarzającego.

§ 3
Bezpieczeństwo danych osobowych

1. Podmiot przetwarzający zapewnia, że osoby upoważnione przez niego do przetwarzania powierzonych danych osobowych zobowiążą się do zachowania ich w tajemnicy w trakcie trwania Umowy oraz po jej zakończeniu.
2. Podmiot przetwarzający zobowiązuje się do spełnienia wszelkich wymogów w zakresie przetwarzania danych osobowych nałożonych na podmioty przetwarzające, wynikających z powszechnie obowiązujących przepisów prawa, w tym RODO, a w szczególności w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych określonych w art. 32 RODO. Podmiot przetwarzający zobowiązuje się do podjęcia środków zabezpieczenia określonych w Załączniku nr 1 do niniejszej Umowy.
3. Środki techniczne oraz organizacyjne są przedmiotem postępu technicznego oraz dalszego rozwoju, wobec czego Podmiot przetwarzający może, po uprzednim pisemnym poinformowaniu Administratora wdrażać adekwatne środki alternatywne, które nie doprowadzą do obniżenia poziomu bezpieczeństwa danych.

§ 4
Dalsze powierzanie przetwarzania danych

1. Administrator wyraża zgodę na dalsze powierzenie przetwarzania danych, o których mowa w § 2 niniejszego Aneksu, przez Podmiot przetwarzający podmiotom wskazanym w Załączniku nr 9 do Umowy Głównej.
2. W zakresie powierzonego przetwarzania Podmiot przetwarzający nie będzie korzystać z usług podmiotów innych niż wymienione w ust. 1 bez uprzedniej pisemnej zgody Administratora. W przypadku korzystania przez Podmiot przetwarzający z podmiotów trzecich, o których mowa w ustępie 1 i 2, Podmiot przetwarzający, w drodze pisemnej umowy, zapewni stosowanie przez te podmioty obowiązków i zobowiązań analogicznych do tych nałożonych przez RODO oraz stwierdzonych w niniejszej Umowie.

§ 5
Współpraca Stron

1. Podmiot przetwarzający zobowiązuje się w miarę możliwości pomagać Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, w realizacji obowiązków wobec podmiotów danych wskazanych w rozdziale III RODO. Jednocześnie Podmiot przetwarzający wspiera Administratora, uwzględniając charakter przetwarzania oraz dostępne mu informacje, w realizacji obowiązków wymienionych w art. 32- 36 RODO.
2. Na żądanie Administratora, Podmiot przetwarzający podejmuje wszelkie działania, jakie Administrator uzna za niezbędne do realizacji obowiązków, o których mowa w ustępie 1.

3. Na żądanie Administratora w terminie wskazanym przez Administratora, Podmiot przetwarzający udostępni Administratorowi wszelkie informacje niezbędne do wykazania, że Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy powierzenia, a także inne obowiązki podmiotu przetwarzającego, wynikające z przepisów o ochronie danych osobowych, w szczególności RODO. Podmiot przetwarzający umożliwi Administratorowi przeprowadzenie audytu w terminie uzgodnionym przez Strony w celu weryfikacji realizacji obowiązków, o których mowa powyżej, i zobowiązuje się do współpracy z Administratorem w tym zakresie. Jeżeli Podmiot przetwarzający zidentyfikuje polecenie otrzymane od Administratora jako niezgodne z RODO lub innymi powszechnie obowiązującymi przepisami o ochronie danych osobowych, niezwłocznie informuje o tym Administratora.

4. Administrator ma prawo wglądu do prowadzonego przez Podmiot przetwarzający rejestru kategorii czynności przetwarzania.

5. Wynikiem audytu jest raport, który zostanie udostępniony Podmiotowi przetwarzającemu. W przypadku, gdy w wyniku raportu określone zostaną dodatkowe zalecenia, Strony wspólnie określą termin ich wdrożenia oraz ewentualny wpływ realizacji zaleceń na kalkulację wynagrodzenia Podmiotu przetwarzającego z tytułu realizacji Umowy Głównej, przy czym nie dotyczy to sytuacji gdy zalecenia dotyczą dostosowania się przez Podmiot przetwarzający do obowiązujących w zakresie ochrony danych osobowych przepisów

§ 6
Zgłaszanie naruszeń ochrony danych osobowych

1. Podmiot przetwarzający jest zobowiązany do opracowania i wdrożenia procedury stwierdzania naruszeń ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO.

2. Podmiot przetwarzający jest zobowiązany zgłosić Administratorowi każde stwierdzone naruszenie ochrony danych osobowych w ciągu 24 godzin od stwierdzenia na wskazany adres e-mail .

3. Podmiot przetwarzający jest zobowiązany zgłosić Administratorowi każdy stwierdzony incydent bezpieczeństwa informacji, nie stanowiący naruszenia danych osobowych a który dotyczył swoim zakresem informacji, w tym danych osobowych powierzonych Podmiotowi przetwarzającemu przez Administratora..

4. Zgłaszając naruszenie lub incydent bezpieczeństwa informacji Podmiot przetwarzający przekazuje Administratorowi co najmniej następujące informacje:
    a. na podstawie jakich czynników Podmiot przetwarzający uznaje zdarzenie za naruszenie ochrony danych osobowych/ incydent bezpieczeństwa informacji;
    b. czy naruszenie/incydent związane jest z utratą poufności;
    c. czy naruszenie/incydent związane jest z utratą dostępności;
    d. czy naruszenie/incydent związane jest z utratą integralności;
    e. czy i w jakim czasie możliwe jest całkowite odwrócenie skutków naruszenia/ incydentu przez Podmiot przetwarzający;
    f. czy wystąpienie naruszenia/ incydentu wynikło z celowego, nieautoryzowanego działania;
    g. jakie dane były przedmiotem naruszenia incydentu;
    h. czy dane, które były przedmiotem naruszenia / incydentu, były zaszyfrowane i przy użyciu jakiej metody szyfrowania;
    i. jak wielu osób dane osobowe objęte są naruszeniem;
    j. z jakiego okresu dane objęte są naruszeniem (np. dnia, z jednego miesiąca, z jednego roku, itp.);

k. jaki zakres danych osobowych objęty jest naruszeniem (w tym czy są to dane finansowe, dotyczące zdrowia, preferencji seksualnych, poglądów politycznych lub religijnych);
l. czy naruszeniem objęte są behawioralne dane osobowe;
m. jakie inne okoliczności i uwarunkowania wpływają na istotność naruszenia/ incydentu.

§ 7
Obowiązki po zakończeniu Umowy

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych wyłącznie na czas niezbędny do realizacji Umowy Głównej. Po zakończeniu Umowy Głównej Podmiot przetwarzający jest jednocześnie zobowiązany do zakończenia czynności przetwarzania danych na zlecenie Administratora i zwraca Administratorowi powierzone dane osobowe, a także usuwa wszelkie ich istniejące kopie, chyba że przepisy powszechnie obowiązującego prawa nakazują przechowywanie całości lub części tych danych.

§ 8
Postanowienia końcowe

1. Umowę powierzenia sporządzono w 2 egzemplarzach, po jednym dla każdej ze Stron.
2. Postanowienia Umowy o powierzeniu przetwarzania danych wchodzą w życie z dniem [...].
3. W sprawach nieuregulowanych w Umowie o powierzeniu przetwarzania danych znajdują zastosowanie postanowienia Umowy Głównej.
4. Spory wynikłe z niniejszej Umowy Strony poddają właściwości sądu rzeczowo właściwego dla obszaru właściwości miejscowej Sądu Rejonowego Katowice – Wschód w Katowicach.
5. Wszelkie zmiany niniejszej Umowy powierzenia wymagają formy pisemnej pod rygorem nieważności.
6. Umowa powierzenia może zostać rozwiązane przez Administratora ze skutkiem natychmiastowym w razie stwierdzenia rażącego naruszenia zasad przetwarzania danych osobowych przez Podmiot przetwarzający, pod warunkiem wcześniejszego pisemnego, bezskutecznego wezwania Podmiotu przetwarzającego do zaprzestania i usunięcia skutków naruszeń w wyznaczonym terminie, nie krótszym niż 14 dni.

....

Administrator Podmiot przetwarzający

SPRAWDZONO POD WZGLĘDEM FORMALNO - PRAWNYM
Ewa Kafka
radca prawny

Załącznik nr 1

Techniczne i organizacyjne środki ochrony danych osobowych

Podmiot przetwarzający wdroży techniczne i organizacyjne środki ochrony w celu:

1.1 zapewnienia, że dostęp do Danych Osobowych będą miały lub zostaną dopuszczone do przetwarzania Danych Osobowych wyłącznie osoby należycie upoważnione, z zachowaniem poufności i na zasadzie ścisłej potrzeby;

1.2 uniemożliwienia osobom nieupoważnionym dostępu/wykorzystania obszarów przeznaczonych do przetwarzania Danych Osobowych oraz odmowy osobom nieupoważnionym dostępu/wykorzystywania ww. obszarów, m.in. poprzez:

1.2.1 wprowadzenie terenów zamkniętych, dostępnych wyłącznie dla osób upoważnionych do przetwarzania Danych Osobowych;

1.2.2 zapewnienie systemu telewizji przemysłowej (CCTV);

1.2.3 stosowanie się do zasady czystego biurka;

1.3 zapewnienia, że osoby wyznaczone do przetwarzania Danych Osobowych zobowiązane zostały do zachowania danych w poufności oraz przeszły wymagane przez Ustawę szkolenia;

1.4 zapewnienia, że Dane Osobowe nie będą bezzasadnie odczytywane, kopiowane, modyfikowane, przenoszone lub usuwane w czasie ich (elektronicznego) transferu lub przechowywania na nośnikach danych, m.in. poprzez:

1.4.1 funkcjonalne oddzielenie Danych Osobowych (przechowywanie, modyfikacja, usunięcie, przesłanie), stosownie do celów, dla których dane są przetwarzane;

1.4.2 zapewnienie, że dostęp do Danych Osobowych może uzyskać wyłącznie właściwa osoba (np. dane polskie nie powinny być bez powodu udostępniane podmiotowi francuskiemu).

1.5 Uniemożliwienia osobom nieupoważnionym dostępu/wykorzystania systemów używanych do procesów przetwarzania Danych Osobowych oraz odmowy osobom nieupoważnionym dostępu/wykorzystywania ww. systemów, m.in. poprzez:

1.5.1 kontrolę wprowadzania, modyfikowania, usuwania, zarządzania i przesyłania Danych Osobowych do systemu i z systemu, m.in. poprzez przestrzeganie stosownych zasad polityki firmy;

1.5.2 wymaganie loginu i hasła do sieci i kont użytkowników identyfikowanych jednoznacznie, a w szczególności wymaganie budowania hasła dostępu zgodnie z aktualnymi zaleceniami CSiRT NASK;

1.5.3 wymaganie każdorazowego wylogowania się z aplikacji lub użycia blokady pulpitu przed opuszczeniem stanowiska pracy;

1.5.4 kontrolę dostępu z użyciem kart magnetycznych;

1.5.5 wykorzystanie różnych form uprawnień dostępu (np. ze względu na funkcję, na przedmiot) i regularne kontrole tych form;

1.5.6 ograniczenie uprawnień administracyjnych na platformach wykorzystujących zaporę sieciową do pracowników działu IT;

1.5.7 określenie procedur modyfikowania/przerywania logicznego dostępu do aktywnych katalogów;

1.5.8 zwrócenie szczególnej uwagi na dane wychodzące poza obszary przeznaczone do przetwarzania Danych Osobowych, m.in. poprzez:

(i) zapewnienie, że osoby korzystające z komputerów przenośnych z Danymi Osobowymi zachowują szczególną ostrożność w czasie transportu, przechowywania i wykorzystywania danego urządzenia poza obszarami przeznaczonymi do przetwarzania Danych Osobowych (w tym poprzez szyfrowanie);

(ii) dla celów zachowania poufności i integralności danych, zabezpieczenie urządzeń/nośników danych zawierających Wrażliwe Dane Osobowe, przenoszonych poza obszary przeznaczone do przetwarzania;

(iii) usuwanie Danych Osobowych z nośników, które udostępniane są osobom nieupoważnionym (w tym dla celów naprawy lub zniszczenia);

1.5.9 podjęcie szczególnych działań w odniesieniu do sieci publicznych, w tym:

(i) zabezpieczenie systemów wykorzystywanych do celów przetwarzania Danych Osobowych przed zagrożeniami związanymi z sieciami publicznymi, poprzez wdrożenie fizycznych i logicznych środków ochrony przed nieupoważnionym dostępem. Do logicznych środków ochrony należą: kontrola przepływu informacji pomiędzy wewnętrznymi systemami IT i zewnętrznymi sieciami publicznymi oraz kontrola działań podejmowanych w sieciach publicznych oraz systemach wykorzystywanych do celów przetwarzania Danych Osobowych;

(ii) kryptograficzne zabezpieczenie danych wykorzystywane do uwierzytelniania przy przekazie w sieciach publicznych.

1.6 zapewnienia, że Dane Osobowe przetwarzane są wyłącznie na podstawie wytycznych przekazanych przez Klienta, m.in. poprzez:

1.6.1 wdrożenie i stosowanie zasad przechowywania dokumentacji;

1.6.2 wdrożenie i stosowanie zasad dotyczących udostępniania, wykorzystywania i ujawniania Danych Osobowych;

1.6.3 wdrożenie polityki prywatności, w tym polityki ochrony bezpieczeństwa danych oraz wytycznych dotyczących zarządzania systemami IT zgodnie z prawem;

1.6.4 współpracę z Klientem w możliwie najszerszym rozsądnym zakresie, m.in. poprzez odpowiadanie na jej zapytania, informowanie o kontrolach przeprowadzonych przez organ nadzorczy i przyjmowanie wniosków mających na celu przestrzeganie przepisów prawa;

1.6.5 powoływanie specjalisty ds. bezpieczeństwa informacji/inspektora ochrony danych, jeżeli wymagają tego przepisy prawa, odpowiedzialnego za zapewnienie zgodności z zasadami bezpieczeństwa/ochrony danych określonymi w tych przepisach. Podmiot przetwarzający udostępni Klientowi dane kontaktowe specjalisty/inspektora.

1.7 zapewnienia, że Dane Osobowe chronione są przed przypadkowym zniszczeniem lub utratą, m.in. poprzez:

1.7.1 określenie procedur tworzenia kopii zapasowych (np. automatycznych systemów tworzenia kopii zapasowych online i na nośnikach);

1.7.2 przechowywanie kopii zapasowych w miejscach zabezpieczonych przed zabraniem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem (oraz natychmiastowego usunięcia w momencie, gdy kopie te przestają być potrzebne);

1.7.3 wykorzystanie źródeł podtrzymujących zasilanie w przypadku urządzeń o fundamentalnym znaczeniu;

1.7.4 systemy ochrony antywirusowej w celu zabezpieczenia stanowisk pracy i serwerów;

1.7.5 stosowanie reguł zapory okresowo kontrolowanych przez pracowników działu IT;

1.7.6 przechowywanie wrażliwego sprzętu IT w bezpiecznych miejscach;

1.7.7 opracowanie planów awaryjnych dla celów odzyskania danych w sytuacjach kryzysowych, w tym w przypadku przerw w dopływie prądu oraz zakłóceń pracy pod wpływem sieci energetycznych.

Środki dodatkowe:

Podmiot przetwarzający będzie przestrzegał zobowiązań wynikających z przepisów prawa odnoszących się do technicznych i organizacyjnych środków ochrony.