

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu roku w Jastrzębie - Zdrój („Umowa”) pomiędzy:

1. **Samodzielnym Publicznym Zakładem Opieki Zdrowotnej Wojewódzkim Szpitalem Specjalistycznym Nr 2 w Jastrzębiu-Zdroju przy Al. Jana Pawła II 7, zarejestrowanym w Sądzie Rejonowym w Gliwicach Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000048508, nr NIP: 633-10-45-778, reprezentowanym przez:**

zwanym dalej „Administratorem”,

a

2.
.....
.....

**wpisaną do Rejestru pod numerem
prowadzonego przez, której kapitał zakładowy wynosi
..... i która posługuje się numerem NIP oraz
numerem REGON,**

zwanym dalej "Podmiotem przetwarzającym".

w dalszej części Umowy zwanymi indywidualnie „Stroną” lub łącznie „Stronami”

ZWAŻYWSZY, ŻE:

- a) Od dnia 25 maja 2018 r. znajduje zastosowanie Rozporządzenie Parlamentu Europejskiego i Rady 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) („**RODO**”);
- b) RODO wprowadza nowe obowiązki w zakresie powierzenia przetwarzania danych osobowych;
- c) Podmiot Przetwarzający świadczy na podstawie umowy nr z dnia („**Umowy Właściwej**”) usługi na rzecz Administratora, które mogą być powiązane z przetwarzaniem w imieniu Administratora danych osobowych, w tym danych szczególnej kategorii;
- d) Strony postanowiły niniejszą Umową określić zasady powierzenia Podmiotowi Przetwarzającemu danych osobowych do przetwarzania, w tym wzajemne prawa i obowiązki w trakcie współpracy w zakresie przetwarzania danych osobowych, spełniając przy tym wymogi obowiązującego prawa.

STRONY POSTANOWIŁY, CO NASTĘPUJE:

§ 1

Przedmiot Umowy

1. Umowa reguluje kwestię powierzenia i ochrony danych osobowych przetwarzanych przez Podmiot przetwarzający w związku z realizacją Umowy Właściwej zawartej pomiędzy stronami.
2. Umowa reguluje również zasady zachowania w poufności przez Podmiot przetwarzający wszelkich informacji uzyskanych w toku świadczenia na podstawie Umowy Właściwej, w szczególności wszelkich informacji stanowiących tajemnicę prawnie chronioną, w tym tajemnicę ustawową lub zawodową Administratora lub osób działających w imieniu lub na rzecz Administratora.

§ 2

Powierzenie przetwarzania danych

1. Dla potrzeb realizacji usług, opisanych w Umowie Właściwej lub zleconych do realizacji w innej formie, Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie niezbędnym do realizacji ww. usług.
2. Niniejsza Umowa stanowi polecenie przetwarzania w rozumieniu art. 28 ust. 3 lit. a) RODO.
3. Rodzaj danych osobowych, kategorie osób, których dane dotyczą, jak również przedmiot, czas trwania oraz charakter i cel przetwarzania danych osobowych są wskazane w załącznikach do Umowy Właściwej (Szczegółowy opis przedmiotu zamówienia):
 - a) Załącznik nr 1a;
 - b) Załącznik nr 1b;
 - c) Załącznik nr 1c;
 - d) Załącznik nr 1d;
 - e) Załącznik nr 1e;
 - f) Załącznik nr 1f.
4. Administratorem danych powierzanych w związku z realizacją Umowy Właściwej jest Administrator. Podmiot przetwarzający przetwarza powierzone dane osobowe wyłącznie na rzecz Administratora i w celu wskazanym przez Administratora.

§ 3

Bezpieczeństwo danych osobowych

1. Podmiot przetwarzający zapewnia, że osoby upoważnione przez niego do przetwarzania powierzonych danych osobowych nie będą przetwarzały danych osobowych w jakimkolwiek innym zakresie lub celu niż wynika to z potrzeb realizacji usług serwisowych, a także, że takie osoby zobowiążą się do zachowania ich w bezwzględnej tajemnicy w trakcie trwania Umowy oraz po jej zakończeniu, zgodnie z zasadami określonymi w § 7 Umowy.
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.

§ 4

Zakaz dalszego powierzania przetwarzania danych

Podmiot przetwarzający nie będzie korzystać z usług innych podmiotów przy przetwarzaniu powierzonych danych, bez uzyskania uprzedniej pisemnej zgody Administratora. Korzystania z dalszych podwykonawców w zakresie realizacji usług, opisanych w Umowie Właściwej, nie może być powiązane z dalszym powierzeniem przetwarzania danych osobowych, bez uzyskania uprzedniej pisemnej zgody Administratora.

§ 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 polecenie 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 Umowy, a także inne obowiązki podmiotu przetwarzającego wynikające z przepisów o ochronie danych osobowych, w szczególności RODO. Podmiot przetwarzający umożliwi Administratorowi lub upoważnionemu przez Administratora audytorowi przeprowadzenie audytów, w tym inspekcji 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 w ocenie Podmiotu przetwarzającego polecenie otrzymane od Administratora jest niezgodne z RODO lub innymi powszechnie obowiązującymi przepisami o ochronie danych osobowych niezwłocznie informuje o tym Administratora.

§ 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. Zgłoszenie stwierdzonego naruszenia ochrony danych powinno zawierać: (i) opis naruszenia, w tym kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; (ii) wskazywać imię i nazwisko osoby, od której Administrator może niezwłocznie uzyskać więcej informacji; (iii) opisywać możliwe konsekwencje naruszenia ochrony danych dla osób, których dane dotyczą; (iv) opisywać środki zastosowane lub proponowane przez Podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Administrator ma prawo żądać od Podmiotu przetwarzającego informacji o incydentach lub podejrzeniach naruszeń ochrony danych osobowych, innych niż określone w ustępie 2.

§ 7

Obowiązek zachowania poufności

1. W rozumieniu Umowy informacjami poufnymi Administratora (dalej: „Informacje Poufne”) są:
 - a) Wszelkie informacje techniczne, technologiczne, organizacyjne Administratora lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, oraz wobec których Administrator podjął rozsądne w danych okolicznościach działania w celu utrzymania ich w poufności, chociażby poprzez umowne zastrzeżenie ich poufności;
 - b) Wszelkie informacje i dane osobowe lub nieosobowe, w tym dane osobowe szczególnej kategorii, których obowiązek utrzymania w tajemnicy obciąża Administratora lub osoby działające w imieniu lub z upoważnienia Administratora na podstawie bezwzględnie obowiązujących przepisów prawa, w szczególności ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentystry, ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, ustawy z 19 sierpnia 1994 r. o ochronie zdrowia psychicznego, ustawy z dnia 7 stycznia 1993 r. o planowaniu rodziny, ochronie płodu ludzkiego i warunkach dopuszczalności przerywania ciąży, ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów, a także RODO.
2. Podmiot przetwarzający zobowiązuje się do zachowania ścisłej poufności polegającej na tym, że nie ujawni jakiegokolwiek nieuprawnionej osobie trzeciej jakiegokolwiek Informacji Poufnych Administratora oraz będzie wykorzystywać Informacji Poufnych wyłącznie do celów świadczenia usług na podstawie Umowy Właściwej. Obowiązek zachowania ścisłej poufności ma zastosowanie niezależnie od formy udostępnienia lub przetwarzania Informacji Poufnych (w tym w formie przekazu ustnego, dokumentu, zapisu na komputerowym nośniku informacji).
3. Podmiot przetwarzający gwarantuje i zapewnia, że stosowane przez niego środki ostrożności i zabezpieczenia zapewniają odpowiednią ochroną Informacji Poufnych przed nieupoważnionym ujawnieniem, pozyskaniem, skopiowaniem, zniszczeniem, przekazaniem, zabraniem lub wykorzystaniem.
4. Obowiązek zachowania poufności, o którym mowa w niniejszym § 7 Umowy, nie dotyczy informacji:
 - a) które są powszechnie dostępne lub znane lub też zostały podane do publicznej wiadomości przez Administratora lub za jego zezwoleniem;
 - b) których ujawnienie jest wymagane przez bezwzględnie obowiązujący przepis prawa;
 - c) których ujawnienie lub przekazanie następuje za pisemną zgodą Administratora;
 - d) których przekazanie następuje w niezbędnym i uzasadnionym okolicznościami zakresie na żądanie podmiotu prowadzącego audyt, pod warunkiem, że podmiot ten zobowiązany jest do zachowania poufności i został uprzednio poinformowany przez Podmiot przetwarzający o poufnym charakterze informacji;
 - e) przekazanych profesjonalnym doradcom (takim jak adwokaci, radcowie prawni, doradcy podatkowi, notariusze), w zakresie niezbędnym do skorzystania przez Podmiot przetwarzający z ich pomocy, pod warunkiem, że są oni z mocy ustawy zobowiązani do zachowania poufności i zostali uprzednio poinformowani przez Podmiot przetwarzający o poufnym charakterze informacji.
5. W każdym przypadku, gdy Podmiot przetwarzający zamierza ujawnić lub udostępnić dane osobowe na podstawie ust. 4 powyżej, w szczególności w wypadku, gdy zostanie zobowiązany nakazem sądu bądź innego organu władzy publicznej do ujawnienia lub udostępnienia Informacji Poufnych, a konieczność ich ujawnienia lub udostępnienia będzie wynikała z bezwzględnie obowiązującego prawa, powinien poinformować o tym Administratora.

Załącznik nr 1 - Wymogi w zakresie bezpieczeństwa danych osobowych

Podmiot przetwarzający zobowiązany jest zapewnić, aby poufność, dostępność ani treść powierzonych mu danych osobowych nie zostały naruszone w nieautoryzowany sposób, w szczególności poprzez:

- 1) Zabezpieczenie komputerów osobistych oraz innych urządzeń przetwarzających dane przed dostępem osób niepowołanych, w tym z wykorzystaniem automatycznego blokowania ekranu po okresie bezczynności użytkownika;
- 2) Stosowanie oprogramowania antywirusowego (o ile jakiegokolwiek urządzenia , np. laptopy, będą wykorzystywane do naprawy);
- 3) Niezwłoczne usuwanie danych osobowych, których przetwarzanie nie jest już niezbędne;
- 4) Ograniczenie liczby komputerów osobistych oraz innych urządzeń przetwarzających dane do niezbędnego minimum;
- 5) Zwracanie szczególnej uwagi, czy dane osobowe przekazywane przez dostawcę osobom fizycznym są kierowane do właściwych osób;
- 6) W przypadku bezpośredniej korespondencji z osobami fizycznymi za pośrednictwem poczty elektronicznej, wprowadzanie adresu odbiorcy w polu „do ukrytej wiadomości” (BCC/DWW)
- 7) Nie kopiowania danych przechowywanych na serwisowanym urządzeniu (chyba, że jest to niezbędne w celu realizacji zlecenia serwisowego), jak również niewykorzystywania danych w jakimkolwiek innym celu niż realizacja zlecenia serwisowego.