**UMOWA POWIERZENIA**

**PRZETWARZANIA DANYCH OSOBOWYCH ( dalej: UPD)**

zawarta w dniu . w Lublinie

pomiędzy:

**Regionalnym Centrum Krwiodawstwa i Krwiolecznictwa w Lublinie**, 20-078 ul. Żołnierzy Niepodległej 8, wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Lublin-Wschód w Lublinie z siedzibą w Świdniku, VI Wydział Gospodarczy KRS pod numerem 0000003874, NIP: 712-24-27-252; REGON: 431029412, nazywanym w treści umowy „Administratorem”,

reprezentowanym przez:

**Z-ca Dyrektora ds. Ekonomiczno-Administracyjnych - mgr inż. Krzysztof Skubis**

a:

 reprezentowanym przez:

……………………………. - …………………………

**§ 1.**

**Powierzenie przetwarzania danych osobowych**

1. W związku z zawarciem i realizacją umowy nr ……..r. dotyczącej wykonywania usługi: przeglądów serwisowych i napraw urządzeń medycznych będących na wyposażeniu Zamawiającego (dalej: Umowa), Administrator powierza Przetwarzającemu dane osobowe przetwarzane w związku ze świadczoną umową. Kategorie danych określa załącznik nr 1.

2. Przedmiotem przetwarzania są dane wskazane w ust. 1. Dane osobowe wymienione w ust. 1 będą przetwarzane w zakresie niezbędnym do realizacji usługi.

3. Z tytułu wykonywania świadczeń określonych w UPD Przetwarzającemu nie przysługuje dodatkowe wynagrodzenie ponad to, które zostało określone w Umowie.

4. Przetwarzający zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z poleceniem Administratora, przestrzegając postanowień UPD, Umowy oraz obowiązujących przepisów regulujących kwestię ochrony danych osobowych, w szczególności rozporządzenia UE 2016/679 z dnia 27 kwietnia 2016 r. (dalej RODO).

5. Administrator oświadcza, że jest uprawniony do przetwarzania danych osobowych w zakresie, w jakim powierzył je Przetwarzającemu.

6. Przetwarzający oświadcza, że w ramach prowadzonej działalności profesjonalnie zajmuje się przetwarzaniem danych osobowych, ma niezbędną wiedzę, wdrożył odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania postanowień UPD.

7. Poprzez zawarcie UPD Administrator poleca przetwarzanie danych osobowych Przetwarzającemu, a także każdej osobie działającej z upoważnienia Przetwarzającego mającej dostęp do danych osobowych, co stanowi udokumentowane polecenie w rozumieniu art. 28 ust. 3 lit. a w zw. z art. 29 RODO.

8. Przetwarzanie danych osobowych wskazanych w ust. 1 odbywa się w miejscu określonym w załączniku nr 2. Zawierając UPD, Administrator udziela wyraźnej zgody na przetwarzanie danych osobowych w miejscach wymienionych w załączniku nr 2 w przypadku Przetwarzającego.

9. Jeżeli przetwarzanie danych osobowych będzie odbywać się poza Europejskim Obszarem Gospodarczym, takie przetwarzanie nastąpi wyłącznie w przypadku, gdy Administrator wyrazi uprzednią pisemną zgodę i pod warunkiem, że przetwarzanie będzie się odbywać w oparciu o odpowiednie środki bezpieczeństwa, które zapewnią odpowiedni poziom ochrony danych osobowych.

**§ 2.**

**Charakter i cel przetwarzania danych**

1. Administrator upoważnia Przetwarzającego do przetwarzania w jego imieniu danych osobowych w celu i zakresie niezbędnym i koniecznym do realizacji Umowy, wykonywane w sposób zautomatyzowany za pośrednictwem systemów informatycznych wykorzystywanych w celu realizacji Umowy lub w sposób tradycyjny.

2. Charakter przetwarzania danych wynika z Umowy i określony jest rolą Przetwarzającego jako podmiotu realizującego w imieniu i na rzecz Administratora jednorazową/stałą usługę przeglądów serwisowych i napraw urządzeń medycznych w ramach której dochodzi do przetwarzania danych, przez pracowników Przetwarzającego.

3. Przetwarzanie danych osobowych będzie dotyczyć następujących kategorii osób:

Pracownicy; Kontrahenci; Honorowi Dawcy Krwi oraz Kandydaci na Dawców Krwi; Uczestnicy programu lojalnościowego; Dawcy szpiku i Krwi Pępowinowej; Pacjenci.

**§ 3.**

**Obowiązki Przetwarzającego**

1. Przetwarzający zobowiązuje się:

1) przy przetwarzaniu powierzonych danych osobowych na podstawie Umowy, zabezpieczyć je poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, w sposób zapewniający adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, wykaz stosowanych środków technicznych i organizacyjnych w dniu zawarcia UPD stanowi załącznik nr 3;

2) nadać upoważnienia do przetwarzania danych osobowych wskazanych w § 1 ust. 1 UPD wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy;

3) prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych;

4) zapewnić zachowanie w tajemnicy przetwarzanych danych oraz sposobów ich zabezpieczenia przez osoby, które posiadają upoważnia do przetwarzania danych osobowych w celu realizacji Umowy lub UPD, zarówno w trakcie zatrudnienia lub współpracy z Przetwarzającym jak i po ustaniu zatrudnienia lub współpracy;

5) udostępniać Administratorowi na jego żądanie wszelkie informacje niezbędne do wykazania spełnienia obowiązków wskazanych w przepisach RODO oraz innych powszechnie obowiązujących przepisach;

6) stosować środki w celu zaradzenia naruszeniom ochrony danych osobowych oraz w stosownych przypadkach środki w celu zminimalizowania ich ewentualnych negatywnych skutków;

7) stosować się do pisemnych instrukcji wydanych przez Administratora w zakresie przetwarzania powierzonych danych osobowych, chyba że co innego wynika z wiążących Przetwarzającego obowiązujących przepisów prawa. W tym drugim przypadku Przetwarzający informuje Administratora o przepisach prawnych i wynikających z nich obowiązkach;

8) dokumentować wszelkie naruszenia ochrony danych w tym ich okoliczności, skutki oraz podjęte działania zaradcze w sposób określony w § 7.

2. Pomoc Przetwarzającego dla Administratora:

1) Przetwarzający niezwłocznie zawiadamia Administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że Administrator wyraził na to zgodę.

2) Przetwarzający pomaga Administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z ppkt. 1) i 2), Przetwarzający stosuje się do poleceń Administratora.

3) Oprócz spoczywającego na Przetwarzającym obowiązku pomagania Administratorowi zgodnie z punktem 2 ppkt 2) Przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje Przetwarzający:

a) obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych ("ocena skutków dla ochrony danych"), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;

b) obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu jego ograniczenia;

c) obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie Administratora, jeżeli Przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;

d) obowiązki określone w art. 32 RODO

4) Strony określają w załączniku 3 odpowiednie środki techniczne i organizacyjne, za pomocą których Przetwarzający jest zobowiązany pomagać Administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

3. Przetwarzający nie jest uprawniony do przekazywania informacji o naruszeniu ochrony powierzonych danych jakimkolwiek podmiotom bez uprzedniej konsultacji z Administratorem.

4. Przetwarzający jest zobowiązany do niezwłocznego poinformowania o wszelkich zgłoszeniach praw osób których dane dotyczą, jeżeli zgłoszenia te dotyczą powierzonych danych.

5. Przetwarzający po zakończeniu Umowy, nie później niż w ciągu 30 (trzydziestu) dni od jej zakończenia, jest zobowiązany do usunięcia lub zwrotu Administratorowi, wedle jego wyboru, powierzonych danych osobowych, o ile przepis prawa powszechnie obowiązującego nie stanowi inaczej.

6. Przetwarzający nie ma prawa do wykorzystywania powierzonych danych w jakimkolwiek celu po wygaśnięciu, rozwiązaniu lub odstąpieniu od Umowy, z wyjątkiem usunięcia lub zwrotu Administratorowi.

7. Przetwarzający zobowiązany jest na żądanie Administratora do złożenia pisemnego oświadczenia o zrealizowaniu ciążącego na nim zobowiązania o którym mowa w ust. 6 i 7.

8. Przetwarzający będzie przetwarzał dane osobowe wyłącznie w celach dla których otrzymał instrukcje oraz w celu wypełnienia zobowiązań wynikających z Umowy. Przetwarzający nie będzie wykorzystywać danych osobowych do innych celów.

9. Przetwarzający nie będzie przekazywał danych osobowych stronom trzecim, chyba że przekazanie to odbywa się zgodnie z instrukcjami Administratora w związku z realizacją Umowy lub gdy jest to konieczne w celu wywiązania się z obowiązku prawnego.

10. Przetwarzający nie będzie modyfikował danych osobowych bez instrukcji Administratora.

11. Przetwarzający jest zobowiązany prowadzić rejestr kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zgodnie z wymogami wynikającymi z RODO.

**§ 4.**

**Prawo do kontroli**

1. Administrator ma prawo kontroli (audytu), czy środki zastosowane przez Przetwarzającego przy przetwarzaniu danych spełniają postanowienia UPO i RODO. W tym celu Przetwarzający umożliwia Administratorowi lub upoważnionemu przez Administratora audytorowi przeprowadzenie audytów, w tym inspekcji i przyczynia się do nich.

2. Administrator informuje Przetwarzającego o zamiarze przeprowadzenia audytu. Przetwarzający wyznaczy terminy możliwych audytów w ciągu 14 (czternastu) dni kalendarzowych od otrzymania powiadomienia. Prawo audytu dotyczy wyłącznie danych powierzonych przez Administratora oraz miejsca ich przetwarzania. Audyt może odbyć się w wyznaczonym przez Przetwarzającego czasie

i pod kontrolą wyznaczonej przez niego osoby. Jeżeli w ciągu 14 (czternastu) dni kalendarzowych Przetwarzający nie wyznaczy terminów Administrator jest uprawniony do wskazania terminów audytów.

3. Niezależnie od postanowień ust. 2 Przetwarzający na każdy pisemny wniosek Administratora zobowiązany jest do udzielenia informacji dotyczących przetwarzania powierzonych mu danych osobowych w terminie 14 (czternastu) dni kalendarzowych od dnia otrzymania takiego wniosku.

4. Przetwarzający udostępni Administratorowi informacje niezbędne do wykazania spełnienia obowiązku określonego w art. 28 RODO.

5. Po stwierdzeniu przez Administratora naruszeń Przetwarzający jest zobowiązany do ich usunięcia w terminie i w sposób ustalony przez Strony.

**§5**

**Podpowierzenie**

1. Przetwarzający jest uprawniony do dalszego powierzania wskazanych w § 1 ust. 1 UPD danych osobowych w celu niezbędnym do wykonania Umowy lub UPD, podmiotom będącym podwykonawcami Przetwarzającego, po uprzednim przekazaniu informacji o tych podmiotach i miejscu przetwarzania przez nich danych. Administrator podpisując UPD udziela Przetwarzającemu zgody na zaangażowanie podwykonawców wymienionych w załączniku nr 2. Podmiot przetwarzający zobowiązany jest przekazać Administratorowi informacje w zakresie wskazanym w załączniku nr 2 dotyczących podwykonawcy lub dalszych podwykonawców. W okresie obowiązywania UPD Przetwarzający, w razie potrzeby i w rozsądnym terminie przed dokonaniem zmiany, będzie ten załącznik aktualizował przesyłając jego treść Administratorowi.

2. Przetwarzający poinformuje Administratora na piśmie o wszelkich zmianach polegających na zastąpieniu lub dodaniu podwykonawców. Administrator danych może sprzeciwić się takim zmianom w formie pisemnej, w terminie 14 (czternaście) dni kalendarzowych od pisemnego powiadomienia go o zaangażowaniu podwykonawców. W przypadku sprzeciwu Przetwarzający nie może skorzystać z takiego podwykonawcy.

3. Przetwarzający jest zobowiązany do zapewnienia, że podmioty wskazane w ust. 1 spełniają takie same wymagania i obowiązki ochrony danych osobowych, jak Przetwarzający, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków organizacyjnych i technicznych, aby przetwarzanie odpowiadało wymogom aktualnie obowiązujących przepisów prawa w zakresie ochrony danych osobowych.

4. Zaangażowanie podwykonawcy nie wpływa na obowiązki Przetwarzającego względem Administratora. Za działania i zaniechania podwykonawców Przetwarzający odpowiada jak za działania i zaniechania własne. Dostęp do danych osobowych może zostać udzielony tylko wtedy, gdy podwykonawca przestrzega lub zapewnia przestrzeganie obowiązków wynikających z UPD. Przetwarzający zawiera pisemną umowę z podwykonawcą, która będzie zgodna z przepisami prawem oraz UPD.

**§ 6.**

**Odpowiedzialność**

1. Przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią UPD, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym. Przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na niego, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.

2. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych przez Przetwarzającego, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania danych osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzoru ochrony danych.

3. Przetwarzający będzie chronił, zabezpieczał i zwolni Administratora z odpowiedzialności za działania, szkody, straty, koszty i wydatki (w tym między innymi uzasadnione koszty obsługi prawnej, konsultingowej i audytowej), wynikające z lub będące następstwem roszczeń jakiejkolwiek strony trzeciej wobec Administratora, wynikających z lub będących następstwem niespełnienia przez Przetwarzającego jakichkolwiek obowiązków dotyczących ochrony powierzonych danych osobowych oraz wszelkich innych obowiązków nałożonych na niego na mocy UPD.

4. W przypadku jakichkolwiek roszczeń strony trzeciej Przetwarzający ma jest zobowiązany poinformować Administratora o wystąpieniu takiego roszczenia niezwłocznie nie później niż w ciągu 3 (trzech) dni kalendarzowych od momentu, w którym uzyskał informację na temat o roszczeniu strony trzeciej.

5. Przetwarzający ponosi odpowiedzialność za działania swoich pracowników i innych osób oraz podmiotów, przy pomocy których przetwarza powierzone dane osobowe, czy też umożliwia im dostęp do powierzonych danych, w tym podwykonawców jak za własne działanie i zaniechanie.

6. Za szkody wyrządzone Administratorowi z tytułu przetwarzania danych osobowych w sposób naruszający przepisy o ochronie danych osobowych lub UPD Administrator może dochodzić od Przetwarzającego odszkodowania na zasadach ogólnych, z zastrzeżeniem postanowień poniżej.

7. Za każde naruszenie postanowień UPD, zasad dotyczących przetwarzania i ochrony danych osobowych w niej określonych lub w powszechnie obowiązujących przepisach prawa, w tym RODO, Administrator może żądać od Przetwarzającego kary umownej za każdy przypadek naruszenia. Za przypadek naruszenia rozumie się w szczególności każde jednorazowe, niezgodne z prawem lub UPD przetwarzanie danych osobowych osoby fizycznej, której dane dotyczą. Administrator może dochodzić odszkodowania przewyższającego wysokość kar umownych.

8. Karę umowną Przetwarzający zobowiązany będzie zapłacić na wskazany przez Administratora rachunek bankowy przelewem, w terminie 7 (siedmiu) dni kalendarzowych od dnia doręczenia mu przez Administratora żądania zapłaty takiej kary umownej.

**§ 7.**

**Naruszenie bezpieczeństwa danych**

W przypadku naruszenia ochrony danych Przetwarzający współpracuje z Administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 RODO, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje Przetwarzający.

1. Naruszenie ochrony danych dotyczące danych przetwarzanych przez Administratora.

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Administratora Przetwarzający wspomaga Administratora:

1) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorczemu(-ym) niezwłocznie po tym, jak Administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);

2) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 RODO powinny być zawarte w zgłoszeniu Administratora i obejmować co najmniej:

1. charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2. możliwe konsekwencje naruszenia ochrony danych osobowych;
3. 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.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;

3) przy wypełnianiu - zgodnie z art. 34 RODO - obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

2. Naruszenie ochrony danych dotyczące danych przetwarzanych przez Przetwarzającego.

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Przetwarzającego, Przetwarzający zgłasza naruszenie Administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu. , jednak nie później niż w terminie 24 (dwudziestu czterech) godzin od chwili stwierdzenia naruszenia. Zgłoszenie to powinno zawierać co najmniej:

1) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);

2) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;

3) wskazanie prawdopodobnych konsekwencji naruszenia

4) środki zastosowane lub proponowane przez Przetwarzającego w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki mające na celu złagodzenie jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

3. Przetwarzający powinien niezwłocznie poinformować Administratora w każdym przypadku, kiedy uzna, że przetwarzanie jest niezgodne z prawem.

**§ 8.**

**Okres obowiązywania umowy**

1. UPD obowiązuje przez okres obowiązywania Umowy oraz przez okres do 30 dni od jej zakończenia.

2. Administrator jest uprawniony do rozwiązania UPD w trybie natychmiastowym, jeżeli zaistnieje chociażby jedna z poniższych przesłanek:

1) Przetwarzający nie wypełnia obowiązków wskazanych w RODO lub innych powszechnie obowiązujących przepisach dotyczących ochrony danych osobowych;

2) Przetwarzający nie wypełnia obowiązków wskazanych w UPD.

3. Wystąpienie podstaw do wypowiedzenia UPD bez zachowania terminu wypowiedzenia stanowi podstawę do wypowiedzenia Umowy bez zachowania terminu wypowiedzenia.

**§ 9.**

**Poufność**

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).

2. Przetwarzający oświadcza, że z zastrzeżeniem § 5 UPD, w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie *Umowy* lub UPD, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub UPD.

3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, żeby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych gwarantowały zabezpieczenie danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

4. W zakresie nieuregulowanym postanowienia *Umowy* dotyczące poufności stosuje się odpowiednio.

**§ 10.**

**Postanowienia końcowe**

1. Zmiana UPD wymaga formy dokumentowej pod rygorem nieważności, z zastrzeżeniem zmian osób o których mowa w ust. 4.

2. Załączniki stanowią nierozerwalną część UPD.

3. Obowiązki informacyjne wynikające z UPD mogą być realizowane w formie elektronicznej.

4. Strony postanawiają, że osobami odpowiedzialnymi za realizację postanowień UPD, w tym uprawnionymi do kontaktu w zakresie realizacji praw osób których dane dotyczą oraz obowiązków wynikających z UPD jest:

a) ze strony Administratora – Mariusz Kasperek -mail m.kasperek@gmail.com.pl

b) ze strony Przetwarzającego – …………………… e-mail: ………………….

5. UPD sporządzono w dwóch jednobrzmiących egzemplarzach.

6. Sądem właściwym dla rozpatrywania sporów jest sąd właściwy dla siedziby Administratora.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Przetwarzający Administrator

 **Załącznik nr 1** - Kategorie danych powierzonych Przetwarzającemu

Kategorie osób, których dane osobowe są przetwarzane:

* 1. Pracownicy;
	2. Kontrahenci;
	3. Honorowi Dawcy Krwi oraz Kandydaci na Dawców Krwi;
	4. Uczestnicy programu lojalnościowego;
	5. Dawcy szpiku i Krwi Pępowinowej;
	6. Pacjenci;
	7. Kandydaci na Dawców Szpiku i Krwi Pępowinowej

Kategorie przetwarzanych danych osobowych

Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa.

~~...............................................................................................................................................~~

Charakter przetwarzania

Charakter przetwarzania danych wynika z Umowy i określony jest rolą Przetwarzającego jako podmiotu realizującego w imieniu i na rzecz Administratora jednorazową/stałą usługę przeglądów serwisowych i napraw urządzeń medycznych w ramach której dochodzi do przetwarzania danych, przez pracowników Przetwarzającego

Czas trwania przetwarzania

Czas trwania umowy głównej

W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania.

**Załącznik nr 2** – Podmiot przetwarzający, Dalsze podmioty przetwarzające i kolejne dalsze podmioty przetwarzające

Podmiot przetwarzający

|  |  |  |
| --- | --- | --- |
| Firma i adres | Lokalizacja przetwarzania | Świadczone usługi/cel |
|  |  | usługa przeglądów serwisowych i napraw urządzeń medycznych będących na wyposażeniu Zamawiającego |
|  |  |  |

Dalsze Podmioty Przetwarzające

|  |  |  |
| --- | --- | --- |
| Firma i adres | Lokalizacja przetwarzania | Świadczone usługi/cel |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Kolejne dalsze podmioty przetwarzające

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Podmiot powierzający przetwarzanie | Firma i adres | Lokalizacja przetwarzania | Kraj | Świadczone usługi/cel |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Załącznik nr 3** – Wykaz stosowanych środków technicznych i organizacyjnych

| **L.p.** | **Środek techniczny i organizacyjny** | **Tak** | **Nie/** **Nie dotyczy** | **Uwagi** |
| --- | --- | --- | --- | --- |
| 1.  | Powołano Inspektora Ochrony Danych lub wyznaczono pracownika do pełnienia zadań związanych z ochroną danych osobowych |  |  |  |
| 2. | Osoby biorące udział w przetwarzaniu danych osobowych posiadają stosowne upoważnienia i zostały zobowiązane do zachowania tych danych w tajemnicy. |  |  |  |
| 3. | Rejestr Kategorii Czynności Przetwarzania  |  |  |  |
| 4. | Ustanowiono i wdrożono Politykę bezpieczeństwa danych osobowych |  |  |  |
| 5. | Szkolenia pracowników |  |  |  |
| 6. | Audyt bezpieczeństwa w okresie ostatnich 2 lat |  |  |  |
| 7. | Testy penetracyjne  |  |  |  |
| 8. | Testy socjotechniczne |  |  |  |
| 9. | Procedura postępowania w przypadku naruszenia ochrony danych osobowych |  |  |  |
| 10. | Wdrożono SZBI |  |  |  |
| 11. | Wykonano analizę ryzyka w zakresie zagrożeń:a) przypadkowego lub niezgodnego z prawem zniszczenia danych,b) utraty, modyfikacji, nieuprawnionego ujawnienia danych,c) nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych |  |  |  |
| 12. | Zapewniono:b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, c) zdolność do szybkiego przywracania dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,  |  |  |  |
| 13.  | Fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych |  |  |  |
| 14. | Zabezpieczenie dostępu do sprzętu |  |  |  |
| 15. | Zabezpieczenie dostępu do serwerowni |  |  |  |
| 16. | Systemy alarmowe/ antywłamaniowe |  |  |  |
| 17. | Monitoring wizyjny |  |  |  |
| 18.  | Klimatyzacja serwerowni |  |  |  |
| 19. | Systemy antywirusowe |  |  |  |
| 20. | Serwery proxy i bramki filtrujące |  |  |  |
| 21. | Ochrona fizyczna obiektu |  |  |  |
| 22. | Zarządzanie pojemnością systemów |  |  |  |
| 23. | Kopie bezpieczeństwa |  |  |  |
| 24. | Kontrola dostępu i zarządzanie przywilejami w systemach teleinformatycznych |  |  |  |
| 25. | Lokalizacja infrastruktury informatycznej w lokalizacjach bezpiecznych |  |  |  |
| 26. | Umowy serwisowe |  |  |  |
| 27. | Umowy powierzenia przetwarzania danych  |  |  |  |
| 28. | Kary umowne z dostawcami usług |  |  |  |
| 29. | Zapasowe centrum danych |  |  |  |
| 30. | Zabezpieczenie dostępu do systemów |  |  |  |