

Zważywszy, że Personel Przyjmującego zamówienie będzie udzielał świadczeń na terenie Przyjmującego z wykorzystaniem infrastruktury Przyjmującego zamówienie (pomieszczenia, system informatyczny PACS/RIS, stacje opisowe) strony postanawiają co następuje:

1. Definicje:

**RODO - 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 (ogólne rozporządzenie o ochronie danych)

**Personel** – osoby zatrudnione przez Przyjmującego zamówienie na podstawie umowy o pracę, posiadający wymagane przepisami prawa oraz określone w SKWO kwalifikacje delegowane do realizacji zadań określonych w umowie. Wykaz Personelu stanowi Załączniku nr 7 do Umowy

**opis badania w wersji elektronicznej** – opis badania diagnostyki obrazowej w postaci dokumentu elektronicznego podpisanego podpisem elektronicznym (kwalifikowanym lub potwierdzonym profilem zaufanym ePUAP przez lekarza) stanowiący elektroniczną dokumentację medyczną w rozumieniu ustawy o systemie informacji w ochronie zdrowia

**opis badania w postaci komunikatu** - komunikat zgodny z protokołem HL7 zawierający informacje o opisie badania, przekazywany w sposób zautomatyzowany z dziedzicznego systemu Wykonawcy do dziedzicznego systemu Zamawiającego

**opis badania w formie papierowej** - opis badania diagnostyki obrazowej w postaci autoryzowanego dokumentu w formie papierowej (pieczęć i podpis lekarza wykonującego opis) stanowiący dokumentację medyczną w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta

2. Na podstawie art. 31 ustawy z dnia 29.08.1997r. o ochronie danych osobowych zwanej dalej Ustawą (t.j. Dz.U.2016 poz. 922 ) Udzielający Zamówienie powierza Przyjmującemu zamówienie przetwarzanie danych osobowych:

- dane zwykłe: imię i nazwisko, Nr PESEL, data urodzenia , numer historii choroby
- dane wrażliwe: informacje o stanie zdrowia

3. Określono następujący zakres przetwarzania powierzonych danych:

- a) Odebrania z systemu Udzielającego zamówienie komunikatów zleceń opisów badań
- b) Odebrania z systemu Udzielającego zamówienie oraz przechowywania w systemie Przyjmującego zamówienie badań diagnostyki obrazowej (pliki DICOM) zgodnie z §2,
- c) wykonania autoryzowanego opisu badania wersji elektronicznej oraz wysłania go drogą elektroniczną do Udzielającego zamówienie zgodnie §2,
- d) wykonania opisu badania w wersji papierowej oraz odpowiednie przechowywanie sporządzonych dokumentów do czasu ich wysłania do Udzielającego zamówienie zgodnie z §2,
- e) odpowiedniego zabezpieczenia danych, o których mowa w wyżej przed ich zniszczeniem, ujawnieniem, utratą, dostępem osób nieupoważnionych,
- f) usunięcia powierzonych do przetwarzania danych zgodnie z zasadami określonymi w §2.

4. Na podstawie art. 37 ustawy o ochronie danych osobowych Przyjmujący Zamówienie upoważni Personel do przetwarzania powierzonych do przetwarzania danych osobowych w zakresie objętym umową. W tym celu Przyjmujący zamówienie wyda stosowne upoważnienia Personelowi.

5. Personel zostanie upoważniony w zakresie:

- wglądu do danych,
- edycji danych polegającej na wykonaniu i autoryzowaniu opisu badania radiologicznego na zasadach opisanych w ust.3,
- sporządzenia opisu badania w wersji papierowej i elektronicznej,
- przechowywania sporządzonych dokumentów w wersji papierowej na zasadach obowiązujących u Przyjmującego zamówienie gwarantujących odpowiedni poziom ochrony dokumentów do czasu ich wysyłki do Udzielającego zamówienie,

*Zasady przetwarzania danych osobowych – Załącznik nr 5  
do Umowy 3D nr .....*

- odpowiedniego zabezpieczenia dokumentów, o których mowa w wyżej przed ich zniszczeniem, ujawnieniem, kradzieżą, nieuprawnionym dostępem,
  - przygotowania dokumentów papierowych do wysyłki zgodnie z §2 ust 4,
- Personel będzie upoważniony do przetwarzania tylko tych danych osobowych, których przetwarzanie będzie niezbędne do realizacji Umowy tzn. danych osobowych tych pacjentów, których badania będzie zobowiązany opisać (lub udzielić konsultacji w zakresie stanu zdrowia tych pacjentów).
6. Przyjmujący zamówienie oświadcza, że będzie:
    - a) przetwarzać dane osobowe zgodnie z obowiązującymi przepisami prawa,
    - b) nie będzie przetwarzać danych osobowych innych osób nie wskazanych w ust 5.
    - c) dane osobowe nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z określonymi w niniejszym Umowie zasadami,
  7. Strony wyłączają możliwość udostępnienia przez Przyjmującego zamówienie powierzonych do przetwarzania danych innym podmiotom z zastrzeżeniem ust.8
  8. Jeżeli niezbędna jest współpraca z innym podmiotem Podwykonawcą (Subprocesorem) w zakresie określonym w ust.1 to Wykonawca zobowiązany jest do podpisania trójstronnej (Zamawiający, Wykonawca, Podwykonawca) umowy powierzenia przetwarzania danych osobowych gwarantującej bezpieczeństwo informacji w tym danych osobowych na odpowiednim poziomie nie niższym niż określono w niniejszej umowie. Zamawiającemu przysługuje prawo odmowy podpisania takiej umowy w przypadku nie spełnienia tego warunku. Zamawiający zastrzega sobie prawo wypowiedzenia umowy trójstronnej w przypadku naruszenia zasad ochrony powierzonych do przetwarzania danych osobowych przez Podwykonawcę.  
W takim wypadku Wykonawca zobowiązany jest do zaprzestania podpowierzania przetwarzanych danych osobowych i spełniająca wymagania określone w RODO w szczególności, o których mowa w art. 28 ust.1 RODO.
  9. Za udostępnienie, o którym mowa w ust. 7 należy rozumieć m.in.:
    - a) umożliwienie wglądu do danych,
    - b) weryfikację danych,
    - c) wyzbycie się danych,
    - d) powierzenie danych,
    - e) przekazanie informacji lub nośnika z danymi,
    - f) upublicznienie danych.
  10. Personel będzie zobowiązany do zachowania w tajemnicy danych osobowych, które uzyska w trakcie realizacji umowy oraz stosowanych zabezpieczeń tych danych.

**§2**

11. Powierzone przez Udzielającego zamówienie pliki DICOM (zdjęcia z diagnostyki obrazowej) będą przechowywane przez Przyjmującego zamówienie na dedykowanych do tego elektronicznych nośnikach pamięci masowej, znajdujących się w pomieszczeniach będących w dyspozycji Przyjmującego zamówienie. W przypadku użytkowania nośników (o których mowa w zdaniu poprzednim) w postaci dysków HDD nie stanowiących macierzy dyskowych dyski te Przyjmujący zamówienie zobowiązany jest zaszyfrować by nie było możliwe przez osoby postronne odtworzenie danych osobowych znajdujących się na tych dyskach.
12. Pomieszczenia, w których przechowywane są nośniki informacji zawierające dane osobowe (np. urządzenia komputerowe, nośniki pamięci masowej, dokumentacja medyczna) Przyjmujący zamówienie zobowiązany jest zabezpieczyć przed dostępem do tych nośników osób nieupoważnionych.
13. System informatyczny Przyjmującego zamówienie, w którym przetwarzane są powierzone do przetwarzania dane osobowe Przyjmujący zamówienie zobowiązany jest zgodnie z wymogami prawa w tym zakresie, w szczególności poprzez zastosowanie zabezpieczeń uniemożliwiających dostęp do danych dla osób nieupoważnionych oraz przed działaniem złośliwego oprogramowania.
14. Dokumenty, o których mowa w §1 ust.3 lit. d) będą dostarczane Udzielającemu zamówienie listem poleconym za pośrednictwem operatora pocztowego zapakowane w dwie koperty. Koperta zewnętrzna opatrzona napisem: "Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi ul. Pabianicka 62" będzie zawierała fakturę oraz kopertę wewnętrzną. Koperta wewnętrzna będzie opatrzona napisem: „Dane wrażliwe – Wyniki Radiologiczne dostarczyć do

*Zasady przetwarzania danych osobowych – Załącznik nr 5  
do Umowy 3D nr .....*

..... Za przygotowanie dokumentów w sposób, o których mowa w zdaniu poprzednim odpowiedzialny jest Personel Przyjmującego zamówienie.

15. Dokumenty, o których mowa w §1 ust.3 lit. c) będą dostarczane Udzielającemu zamówienie drogą elektroniczną za pośrednictwa bezpiecznego kanału VPN do wskazanego systemu informatycznego Udzielającego zamówienie.
16. Po zakończeniu umowy jednak nie później niż w terminie 30 dni od dokonania statecznego rozliczenia umowy Przyjmujący zamówienie zobowiązany jest do usunięcia (lub ich zniszczenia) powierzonych do przetwarzania danych osobowych w sposób uniemożliwiający ich odtworzenie z wszelkich nośników m.in. w tym również: dokumentów, o których mowa w §1 ust.3 lit. c), wszelkich rekordów, zestawień, raportów itp. zawierających te dane.
17. Przed usunięciem danych, o którym mowa w ust. 6 Przyjmujący Zamówienie zobowiązany jest przekazać Udzielającemu zamówienie kopie wszystkich dokumentów, o których mowa w §1 ust.3 lit. c) i uzyskać od Udzielającego zamówienie potwierdzenia ich przekazania. Szczegółowy sposób przekazania tych danych zostanie ustalony z Działem Informatyki Udzielającego zamówienie.
18. Przyjmujący zamówienie zobowiązany jest dostarczyć Udzielającemu zamówienie raportu z przeprowadzonych czynności usunięcia danych (lub niszczenia nośników) nie później niż w ciągu 14 dni od chwili przeprowadzonej skutecznie procedury.

**§ 3**

19. Przetwarzanie danych osobowych będzie odbywało się w pomieszczeniach Przyjmującego zamówienie z wykorzystaniem jego infrastruktury (stacji opisowa radiologiczna) oraz systemu informatycznego należącego do Przyjmującego zamówienie. Personel zobowiązany jest do przetwarzania danych osobowych na urządzeniach należących tylko do Przyjmującego zamówienie i w systemie informatycznym należącym do Przyjmującego zamówienie (RIS/PACS).
20. Zabrania się Personelowi zamówienie wykonywania nieuzasadnionych kopii, wydruków przechowywania jakichkolwiek danych z wyłączeniem wydruku opisu badania wykonanego w celu autoryzacji opisu badania i przekazania tego opisu Udzielającemu zamówienie. Dokumenty w wersji papierowej generowane z systemu informatycznego Przyjmującego zamówienie będą przechowywane przez Personel zgodnie z obowiązującymi u Przyjmującego zamówienie normatywnymi aktami wewnętrznymi.
21. Zabronione jest wnoszenie poza obszar przetwarzania danych określony przez Przyjmującego zamówienie w aktach , o których mowa w §4 jakichkolwiek nośników zawierających dane osobowe.
22. **Personel** zobowiązany jest do zapoznania się i przestrzegania zasad określonych w § 5.
23. W przypadku naruszenia zasad bezpieczeństwa w zakresie poufności lub integralności danych osobowych Personel zobowiązany jest podjąć stosowne działania odpowiednie dla incydentów bezpieczeństwa informacji w tym niezwłocznego powiadomienia Udzielającego zamówienie zgodnie z art. 33 RODO.

**§ 4**

1. W celu realizacji umowy Udzielający zamówienie wyraża zgodę na zestawienie połączenia zdalnego dostępu do systemu RIS/PACS Udzielającego zamówienie. Wszystkie połączenia i transmisja danych będzie się odbywała za pośrednictwem bezpiecznego połączenia VPN na wskazany przez Przyjmującego zamówienie numer statyczny IP należący do niego. Połączenie będzie szyfrowane w sposób bezpieczny.
2. Osobą upoważnioną do zestawienia połączenia zdalnego jest:
  - a) Ze strony Udzielającego zamówienie - ..... (imię i nazwisko, tel., adres e-mail)
  - b) Ze strony Przyjmującego zamówienie - ..... (imię i nazwisko, tel., adres e-mail)
3. W celu zapewnienia poufności danych podczas połączenia przy użyciu systemu zdalnego dostępu, Wykonawca zapewnia, że:
  - a) będzie korzystał ze środków technicznych i organizacyjnych zlokalizowanych na terenie UE,
  - b) wszystkie połączenia i transmisja danych będzie się odbywała za pośrednictwem bezpiecznego połączenia zestawionego na statyczny nr IP należący do Wykonawcy,
  - c) połączenie zdalnego dostępu będzie szyfrowane w sposób bezpieczny
  - d) będzie stosował się do zasad określonych w ust.4
4. Przyjmujący zamówienie nie może:
  - a) zmieniać przyznanego adresu IP,
  - b) rozdzielacza sygnału na inne komputery niż określony w umowie (np. stosowanie routera itp.),
  - c) dokonywać przecięcia sieci teleinformatycznej Udzielającego zamówienie,

- d) rozsyłać niechcianej poczty (SPAM),
- e) używać niedozwolonych narzędzi sieciowych, takich jak sniffery, skanery portów, exploity,
- f) wykorzystywać infrastruktury teleinformatycznej Udzielającego zamówienie w celu uruchamiania serwisów świadczących usługi komercyjne,
- g) rozpowszechniać informacji sprzecznych z obowiązującym prawem oraz naruszających w jakikolwiek sposób uczucia religijne lub normy społeczne i obyczajowe,
- h) świadczyć usług telekomunikacyjnych osobom trzecim, o ile wiążą się one z tranzytem informacji przez sieć Udzielającego zamówienie,
- i) prowadzić jakichkolwiek działań, które mogą powodować zakłócenia w działaniu sieci Zamawiającego,
- j) podejmować jakichkolwiek działań, które mogą uszkodzić infrastrukturę teleinformatyczną Zamawiającego, za pomocą której świadczona jest usługa lub mogących zakłócić poprawne funkcjonowanie systemów służących udostępnianiu i monitorowaniu usługi oraz urządzeń i łączy przeznaczonych do przekazywania informacji na odległość, za pomocą których świadczona jest Usługa,
- k) stosować urządzeń sieciowych i oprogramowania niedozwolonych przez prawo,
- l) kierować do sieci Udzielającego zamówienie ruch telekomunikacyjny z innych sieci telekomunikacyjnych bez zgody Udzielającego zamówienie,
- m) wykorzystywać urządzeń udostępnionych przez Udzielającego zamówienie lub innych przyłączonych do punktu styku z siecią publiczną Internet, niezgodnie z przepisami prawa lub niezgodnie z zawartą umową,
- n) uzyskiwać ani próbować uzyskiwać żadnych informacji z sieci Udzielającego zamówienie przy użyciu jakiegokolwiek metody, z wyjątkiem sytuacji kiedy będzie która nie została wyraźnie dopuszczona przez Zamawiającego,
- o) przechwytywać, badać lub w inny sposób analizować jakiegokolwiek komunikacyjnego protokołu używanego przez Udzielającego zamówienie, zarówno poprzez analizator sieci, program przechwytyjący (sniffer) lub inny program lub urządzenie.

## § 5

1. Przyjmujący zamówienie oświadcza, że:
  - a) zobowiązuje się do stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych będących przedmiotem przetwarzania m.in. do:
    - ✓ zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem
    - ✓ dopuszczenia do przetwarzania powierzonych danych osobowych, w tym obsługi systemu informatycznego, aplikacji oraz urządzeń wchodzących w ich skład służących do przetwarzania danych, wyłącznie osób posiadających wydane przez niego stosowne upoważnienie do przetwarzania danych osobowych,
    - ✓ dochowania szczególnej staranności, aby osoby, o których mowa w pkt b) zachowały je w tajemnicy, również po zakończeniu realizacji Umowy powierzenia, między innymi poprzez poinformowanie ich o prawnych konsekwencjach naruszenia poufności danych oraz odebranie oświadczeń o zachowaniu w tajemnicy tych danych, o których mowa w art. 49-52 ustawy o ochronie danych osobowych,
    - ✓ zapewnienia kontroli nad prawidłowością przetwarzania danych
    - ✓ przygotowania i wdrożenia dokumentacji ochrony danych osobowych,
    - ✓ wyznaczenia administratora bezpieczeństwa informacji (ABI) nadzorującego przestrzeganie zasad ochrony, chyba że administrator danych sam wykonuje te czynności
  - b) dysponuje środkami umożliwiającymi prawidłowe przetwarzanie i zabezpieczenie danych osobowych, o których mowa w art. 36 - 39 ustawy z dnia 29.08.1997 o ochronie danych osobowych i są one wdrożone,
  - c) wykorzystywane przez niego systemy informatyczne spełniają wymagania określone w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczny służące do przetwarzania danych osobowych (Dz.U.2004.100.1024 z późn.zm.).

*Zasady przetwarzania danych osobowych – Załącznik nr 5  
do Umowy 3D nr .....*

- W zakresie przestrzegania tych przepisów Przyjmujący zamówienie ponosi odpowiedzialność jak administrator danych.
2. W celu spełnienia wymagań określony w §1 Przyjmujący zamówienie zobowiązany jest w szczególności do:
    - a) opracowania i wdrożenia Polityki ochrony danych osobowych
    - b) wdrożenia i zapoznania Personelu oraz pozostałych pracowników uczestniczących w procesie przetwarzania danych osobowych ,
    - c) zastosowania zabezpieczeń pomieszczeń, w których są przetwarzane dane osobowe przed dostępem osób nieupoważnionych (w tym personel sprzątający), kradzieżą, zniszczeniem danych lub dokumentów,
    - d) zabezpieczenia systemu informatycznego (m.in. infrastruktura informatyczna sieciowa, stacje opisowe) przed dostępem do przetwarzanych danych osób nieupoważnionych, działaniem złośliwego oprogramowania.
  3. W przypadku uchylenia lub zmian przepisów, o których mowa w ust. 1, Przyjmujący zamówienie zobowiązuje się do respektowania i przestrzegania norm prawnych zastępujących dotychczasowe przepisy.
  4. Przyjmujący zamówienie oświadcza, że zna i zobowiązuje się do stosowania zasad przetwarzania i ochrony danych osobowych określonych w RODO, a w szczególności przepis art. 28 tego Rozporządzenia
  5. W przypadku naruszenia zasad bezpieczeństwa w zakresie poufności lub integralności danych osobowych Przyjmujący zamówienie niezwłocznie powiadomi Udzielającego zamówienia tzn. w czasie umożliwiającym dokonanie przez Udzielającego zamówienia zgłoszenia w terminie, o którym mowa w art. 33 ust.1 RODO.

**§ 6**

1. Udzielający zamówienie uprawniony jest do przeprowadzenia kontroli w zakresie ochrony powierzonych do przetwarzania danych oraz zgodności z warunkami umowy w tym zakresie a Przyjmujący zamówienie zobowiązuje się do umożliwienia Udzielającemu zamówienie przeprowadzenia kontroli.
2. W ramach kontroli, o której mowa w ust. 1 Udzielający zamówienie uprawniony jest do:
  - a) Wstępu do pomieszczeń Przyjmującego zamówienie, w których przetwarzane są dane osobowe,
  - b) przeprowadzenia oględzin systemu informatycznego Przyjmującego w zakresie zgodności z umową w tym przeprowadzanych przez Przyjmującego zamówienie procedury usunięcia danych,
  - c) sporządzenia z raportu z przeprowadzonej kontroli oraz wydania zaleceń w przypadku stwierdzonych niezgodności z umową w zakresie przetwarzania danych.
3. W przypadku niedostosowania się przez Przyjmującego zamówienie do wydanych w ramach przeprowadzonej kontroli zaleceń Udzielającemu zamówienie przysługuje prawo rozwiązania umowy z winy Przyjmującego zamówienie.