

Definicje:

RODO –Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)

§ 1

1. Na podstawie art. 31 ustawy z dnia 27.08.1997 r. o ochronie danych osobowych zwanej dalej ustawą (Dz.U.2016.poz.982 z późn.zm.) Udzielający zamówienia powierza Przyjmującemu zamówienie przetwarzanie danych osobowych zwykłych (imię i nazwisko, adres zamieszkania, data urodzenia, PESEL) oraz danych sensytywnych (informacje o stanie zdrowia, materiał biologiczny), wyłącznie w celu realizacji postanowień Umowy na zasadach określonych poniżej.
2. Udzielający zamówienia powierza przetwarzanie danych osobowych:
 - a) tych pacjentów, których materiał biologiczny wraz ze skierowaniem na badanie wystawionym przez Udzielającego zamówienie przekazuje Przyjmującemu zamówienie,
 - b) tych pacjentów, których wyniki badań archiwalnych powierzy do używania w aplikacji webowej służącej do przeglądania wyników , do którego ma dostęp Przyjmujący zamówienie, a z którego korzysta w celu zapewnienia kompleksowości świadczeń personel Udzielającego zamówienie
 - c) Użytkowników aplikacji webowej służącej do przeglądania wyników badań wprowadzonych przez Przyjmującego zamówienie.
3. W odniesieniu do danych osobowych, o których mowa w:
 - a) pkt.2 lit. a) oraz lit c) Przyjmujący zamówienie zobowiązuje się prowadzić dokumentację zgodnie z obowiązującymi przepisami prawa w szczególności określonymi w:
 - ustawie z 6 listopada 2008r. o prawach pacjenta i rzeczniku Praw Pacjenta (t.j. Dz.U. 2017 poz. 1381 z późn.zm.),
 - ustawie z dnia 27 lipca 2001r. o diagnostyce laboratoryjnej (t.j. Dz. U. z 2016r. poz. 2245 z późn.zm.)
 - Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015r. poz. 2069),
 - Rozporządzenia Ministra Zdrowia z dnia 23 marca 2006 r. w sprawie standardów jakości dla medycznych laboratoriów diagnostycznych i mikrobiologicznych (Dz.U. 2016 nr 1665.),na podstawie tych przepisów Przyjmujący zamówienie staje się odrębnym administratorem danych osobowych i będzie przetwarzał dane osobowe zgodnie z obowiązującymi normami prawnymi. Udzielający zamówienia nie ponosi odpowiedzialności w tym zakresie.
 - b) pkt. 2 lit. b) administratorem tych danych jest wyłącznie Udzielający zamówienie. Przyjmujący zamówienie zobowiązany jest nie później niż 14 dni od chwili zakończenia niniejszej Umowy usunąć ze swoich zasobów te dane w sposób uniemożliwiający ich odtworzenie, chyba, że Przyjmujący zamówienie będzie kontynuował usługi laboratoryjne na podstawie nowo zawartej umowy. Z czynności brakowania tych danych Przyjmujący zamówienie sporządzi raport i dostarczy Udzielającemu zamówienie.
4. Przyjmujący zamówienie oświadcza, że powierzone do przetwarzania dane osobowe nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z określonym w ust. 1 lub ust. 3 niniejszego paragrafu.
5. Przyjmujący zamówienie zobowiązuje się do zachowania poufności informacji, o których jest mowa w ust.1 niniejszego paragrafu, w czasie trwania umowy i po ich zakończeniu.
6. Zabrania się wykonywania przez Przyjmującego zamówienie nieuzasadnionych kopii, gromadzenia, przechowywania jakichkolwiek danych, z wyłączeniem sytuacji gdy jest to niezbędne do realizacji umowy lub jest to obowiązkiem Przyjmującego zamówienie wynikającym z obowiązujących przepisów prawa. Zabrania się udostępniania danych nośników informacji zawierających dane o których mowa w ust. 1 osobom do tego nieuprawnionym.
7. Strony wyłączają możliwość udostępnienia przez Przyjmującego zamówienie powierzonych do przetwarzania danych, o których mowa w ust. 2 niniejszego paragrafu innym podmiotom bez zgody Udzielającego zamówienia, chyba że obowiązek taki będzie wynikać z przepisów prawa.
8. Jeżeli niezbędna jest współpraca Przyjmującego zamówienie z innym podmiotem (Subprocesorem) w zakresie określonym w ust.1 to Przyjmujący zamówienie zobowiązuje się do podpisania stosownej umowy

podpowierzenia przetwarzania danych osobowych pomiędzy: Udzielającym zamówienie, Przyjmującym zamówienie i Subprocesorem określonej jako Załącznik nr 13B do Umowy głównej. Udzielający zamówienie zastrzega sobie prawo wniesienia sprzeciwu wobec czynności podpowierzenia przetwarzania danych osobowych.

9. Za udostępnienie, o którym mowa w ust. 7 należy rozumieć m.in.:
 - a) przekazanie informacji lub nośnika z danymi,
 - b) weryfikację danych,
 - c) wyzbycie się danych,
 - d) powierzenie danych,
 - e) umożliwienie wglądu do danych,
 - f) upublicznienie danych.
10. Przyjmujący zamówienie zobowiązuje się do zachowania w tajemnicy wszelkich informacji, które uzyska w trakcie realizacji niniejszej umowy, chyba że obowiązek taki będzie wynikać z przepisów prawa.

§ 2

1. Przyjmujący zamówienia oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie i zabezpieczenie danych osobowych, co najmniej w zakresie, o którym mowa w art. 36 – 39 ustawy, a jego systemy informatyczne i aplikacje spełniają wymagania określone w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. 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.) m.in.:
 - politykę bezpieczeństwa informacji,
 - instrukcję zarządzania systemem informatycznym,
 - zabezpieczenia techniczne i organizacyjne.
2. Przyjmujący zamówienie zobowiązuje się do zastosowania przy przetwarzaniu danych osobowych, o których mowa w §1 środków technicznych i organizacyjnych zapewniających ochronę danych osobowych co najmniej w zakresie określonym w art. 36-39 ustawy o ochronie danych osobowych, w szczególności określonych w §3.
3. W zakresie przestrzegania przepisów, o których mowa w ust.1 Przyjmujący zamówienie ponosi odpowiedzialność jak administrator danych.
4. W przypadku uchylecia lub zmian przepisów, o których mowa w ust. 1, Przyjmujący zamówienie zobowiązuje się do respektowania i przestrzegania norm prawnych zastępujących dotychczasowe przepisy.
5. 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
6. 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.

§ 3

1. Przyjmujący zamówienie zobowiązuje się w szczególności do:
 - a) zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,
 - b) 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,
 - c) prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych,
 - d) 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,

- e) zapewnienia kontroli nad prawidłowością przetwarzania danych.
 - f) zapewnienia by dostęp do danych osobowych zawartych w zleceniach oraz wynikach zleconych przez Udzielającego zamówienie badań miały tylko osoby uprawnione tzn. po stronie Przyjmującego zamówienie: osoby zatrudnione przez Przyjmującego zamówienie lub Subprocesora realizujące zadania objęte niniejszą Umową, po stronie Udzielającego zamówienie: osoby wskazane przez Udzielającego zamówienie.
 - g) Zawarcia umów podpowierzenia przetwarzania danych osobowych z podmiotami świadczącymi usługi dla Przyjmującego zamówienie (np. serwis wyrobów medycznych, serwis systemów i aplikacji informatycznych) na zasadach określonych w §1.
2. Przyjmujący zamówienie zobowiązuje się, że powierzone do przetwarzania dane nie zostaną przekazane do państwa trzeciego, w tym również do podmiotów powiązanych (spółki macierzyste, etc.).
 3. Udzielający zamówienie jest uprawniony do kontrolowania Przyjmującego zamówienie w zakresie przetwarzania powierzonych danych osobowych, pod względem zgodności z umową oraz przepisami ochrony danych osobowych.
 4. W celu wykonania kontroli upoważnieni pracownicy Udzielającego zamówienia mają prawo:
 - a) wstępu do pomieszczeń, w których przetwarzane są powierzone do przetwarzania dane osobowe, i przeprowadzenia niezbędnych czynności kontrolnych,
 - b) żądania złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,
 - c) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych do przetwarzania danych osobowych,
 5. Z czynności kontrolnych sporządza się protokół, którego jeden egzemplarz doręcza się Przyjmującemu zamówienie.
 6. Po kontroli, o której mowa w pkt. 3 Udzielający zamówienia może zredagować i żądać wykonania zaleceń pokontrolnych, o ile są one zgodne z Umową powierzenia, oraz określić termin ich realizacji. Niezastosowanie się do zaleceń pokontrolnych będzie traktowane jako ciężkie naruszenie warunków Umowy i może skutkować rozwiązaniem Umowy z winy Przyjmującego zamówienie.
 7. Za naruszenie przepisów dotyczących ochrony danych osobowych z przyczyn leżących po stronie Przyjmującego zamówienie lub Subprocesora, w następstwie którego Udzielający zamówienia – jako Administrator Danych Osobowych – zostanie obciążony grzywną lub zobowiązany do wypłaty odszkodowania Przyjmujący zamówienie zobowiązuje się do zwrotu poniesionych z tego tytułu kwot.

§ 4

1. Udzielający zamówienie wyraża zgodę na zestawienie połączenia zdalnego dostępu do systemu HIS Udzielającego zamówienie w celu:
 - a) odbierania przez system prezentacji wyników lub dziedzinowy system medyczny LIS Przyjmującego zamówienie zleceń elektronicznych z systemu HIS Udzielającego zamówienie,
 - b) przesyłania komunikatów z systemu prezentacji wyników (np. LIS) do systemu HIS parametrów badań,
 - c) wysyłania wyników badań (w postaci elektronicznych dokumentów podpisanych podpisem elektronicznym) z systemu prezentacji wyników lub systemu dziedzinowego LIS do systemu dziedzinowego Udzielającego zamówienie,
 - d) zapisania na wskazanych przez Udzielającego zamówienie zasobach plików zawierających raporty z wykonanej usługi
 - e) zapisywania przez Przyjmującego zamówienie na wskazanych przez Udzielającego zamówienie wyników badań

W celu realizacji powyższych zadań Przyjmujący zamówienie zobowiązany jest spełnić wymagania określone w Załączniku nr 12 do Regulaminu „Wymagania systemu informatycznego”
2. 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. 3
3. Przyjmujący zamówienie nie może:

- a) zmieniać przyznanego adresu IP bez uzyskania zgody Udzielającego zamówienie,
- b) rozdzielać sygnału na inne komputery niż określony w umowie (np. stosowanie routera itp.),
- c) dokonywać przeciążenia sieci teleinformatycznej Udzielającego zamówienie,
- e) rozsyłać niechcianej poczty (SPAM),
- f) używać niedozwolonych narzędzi sieciowych, takich jak sniffery, skanery portów, exploity,
- g) wykorzystywać infrastruktury teleinformatycznej Udzielającego zamówienie w celu uruchamiania serwisów świadczących usługi komercyjne,
- h) rozpowszechniać informacji sprzecznych z obowiązującym prawem oraz naruszających
 - i) w jakikolwiek sposób uczucia religijne lub normy społeczne i obyczajowe,
 - j) świadczyć usług telekomunikacyjnych osobom trzecim, o ile wiążą się one z tranzytem informacji przez sieć Udzielającego zamówienie,
- k) prowadzić jakichkolwiek działań, które mogą powodować zakłócenia w działaniu sieci Udzielającego zamówienie,
- l) 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,
- n) stosować urządzeń sieciowych i oprogramowania niedozwolonych przez prawo,
- o) kierować do sieci Udzielającego zamówienie ruchu telekomunikacyjnego z innych sieci telekomunikacyjnych bez zgody Udzielającego zamówienie,
- q) 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,
- r) 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 Udzielającego zamówienie,
- s) 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.