Warunki Przetwarzania Danych dla usług serwisowych

Stan na dzień 30 kwietnia 2025, wersja 1.0

SEKCJA I

Klauzula 1
Cel i zakres

(a) Celem niniejszych Warunków przetwarzania danych ("Klauzule") jest zapewnienie zgodności z art. 28 ust. 3 i 4 Rozporządzenia 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.

(b) OLYMPUS POLSKA Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, przy ul. Wynalazek 1 (procesor) wyrażają zgodę na niniejsze klauzule w celu zapewnienia zgodności z art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 lub art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725.

(c) Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonych w Załączniku I.

(d) Załączniki nr I to III stanowią integralną część Klauzul.

(e) Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator na mocy rozporządzenia (UE) 2016/679 i/lub rozporządzenia (UE) 2018/1725.

(f) Niniejsze klauzule same w sobie nie zapewniają zgodności z obowiązkami związanymi z międzynarodowymi transferami zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

Klauzula 2
Interpretacja

(a) W przypadku użycia w niniejszych klauzulach terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725, terminy te mają takie samo znaczenie jak w tym rozporządzeniu.

(b) Niniejsze klauzule należy odczytywać i interpretować w świetle przepisów odpowiednio rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

(c) Niniejsze klauzule nie mogą być interpretowane w sposób sprzeczny z prawami i obowiązkami przewidzianymi w rozporządzeniu (UE) 2016/679 / rozporządzeniu (UE) 2018/1725 lub w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

SEKCJA II - OBOWIĄZKI STRON

Klauzula 3
Opis przetwarzania(-ń)

Szczegóły operacji przetwarzania, w szczególności kategorie danych osobowych i cele przetwarzania, dla których dane osobowe są przetwarzane w imieniu administratora, są określone w załączniku I.

Klauzula 4
Obowiązki Stron

4.1. Instrukcje

a) Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego,

któremu podlega podmiot przetwarzający. W takim przypadku podmiot przetwarzający informuje administratora o tym wymogu prawnym przed rozpoczęciem przetwarzania, chyba że prawo zabrania tego z uwagi na ważne względy interesu publicznego. Późniejsze instrukcje mogą być również wydawane przez administratora przez cały okres przetwarzania danych osobowych. Instrukcje te powinny być zawsze udokumentowane.

(b) Podmiot przetwarzający niezwłocznie informuje administratora, jeżeli w jego opinii instrukcje wydane przez administratora naruszają rozporządzenie (UE) 2016/679 / rozporządzenie (UE) 2018/1725 lub obowiązujące przepisy Unii lub państwa członkowskiego dotyczące ochrony danych.

4.2. Ograniczenie celu

Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnych celach przetwarzania określonych w załączniku I, chyba że otrzyma dalsze instrukcje od administratora.

4.3. Czas przetwarzania danych osobowych

Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez czas określony w załączniku I.

4.4. Bezpieczeństwo przetwarzania

(a) Podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III w celu zapewnienia bezpieczeństwa danych osobowych. Obejmuje to ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, Strony należycie uwzględniają aktualny stan wiedzy, koszty wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko dla osób, których dane dotyczą.

(b) Podmiot przetwarzający udziela dostępu do przetwarzanych danych osobowych członkom swojego personelu wyłącznie w zakresie ściśle niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, że osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

4.5. Dane wrażliwe

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, dane genetyczne lub biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia lub życia seksualnego lub orientacji seksualnej osoby lub dane dotyczące wyroków skazujących i naruszeń prawa ("dane wrażliwe"), podmiot przetwarzający stosuje szczególne ograniczenia i/lub dodatkowe zabezpieczenia.

4.6 Dokumentacja I zgodnosć

(a) Strony muszą być w stanie wykazać zgodność z niniejszymi klauzulami.

(b) Podmiot przetwarzający niezwłocznie i odpowiednio reaguje na zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami

(c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania zgodności z obowiązkami określonymi w niniejszych klauzulach i wynikającymi bezpośrednio z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi klauzulami i uczestniczy w nich w zasadnych odstępach czasu lub w przypadku stwierdzenia niezgodności. Podejmując decyzję o przeglądzie lub

audycie, administrator może wziąć pod uwagę odpowiednie certyfikaty posiadane przez podmiot przetwarzający.

(d) Administrator może przeprowadzić audyt samodzielnie lub zlecić go niezależnemu audytorowi. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego i w stosownych przypadkach są przeprowadzane z odpowiednim wyprzedzeniem.

(e) Strony udostępniają informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów, właściwym organom nadzorczym na żądanie.

4.7. Korzystanie z podwykonawców przetwarzania

(a) Podmiot przetwarzający posiada ogólne upoważnienie administratora do angażowania podwykonawców przetwarzania z uzgodnionej listy. Podmiot przetwarzający wyraźnie informuje administratora o wszelkich zamierzonych zmianach w tym wykazie poprzez dodanie lub zastąpienie podwykonawców przetwarzania z co najmniej czterotygodniowym wyprzedzeniem, dając w ten sposób administratorowi wystarczającą ilość czasu, aby mógł sprzeciwić się takim zmianom przed zaangażowaniem odpowiednich podwykonawców przetwarzania. Podmiot przetwarzający dostarcza administratorowi informacje niezbędne do umożliwienia administratorowi skorzystania z prawa do sprzeciwu.

(b) Jeżeli podmiot przetwarzający angażuje podwykonawcę przetwarzania do wykonywania określonych czynności przetwarzania (w imieniu administratora), czyni to w drodze umowy, która nakłada na podwykonawcę przetwarzania, co do istoty, te same obowiązki ochrony danych, co obowiązki nałożone na podmiot przetwarzający dane zgodnie z niniejszymi klauzulami. Podmiot przetwarzający dopilnowuje, by podwykonawca przetwarzania wypełniał obowiązki, którym podlega podmiot przetwarzający zgodnie z niniejszymi klauzulami oraz rozporządzeniem (UE) 2016/679 lub rozporządzeniem (UE) 2018/1725.

(c) Na żądanie administratora podmiot przetwarzający dostarcza administratorowi kopię takiej umowy podpowierzenia oraz wszelkich późniejszych zmian. W zakresie niezbędnym do ochrony tajemnicy przedsiębiorstwa lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może zredagować tekst umowy przed udostępnieniem kopii.

(d) Podmiot przetwarzający pozostaje w pełni odpowiedzialny wobec administratora za wykonanie obowiązków podwykonawcy przetwarzania zgodnie z umową zawartą z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia administratora o każdym przypadku niewywiązania się przez podwykonawcę przetwarzania ze swoich zobowiązań umownych.

4.8. Transfer międzynarodowy

(a) Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na podstawie udokumentowanych instrukcji administratora lub w celu spełnienia konkretnego wymogu wynikającego z prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

(b) Administrator zgadza się, że w przypadku, gdy podmiot przetwarzający angażuje podwykonawcę przetwarzania zgodnie z klauzulą 4.7. do wykonywania określonych czynności przetwarzania (w imieniu administratora), a te czynności przetwarzania wiążą się z przekazaniem danych osobowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, podmiot przetwarzający i podwykonawca przetwarzania mogą zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679, stosując standardowe klauzule umowne przyjęte przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, o ile spełnione są warunki stosowania tych standardowych klauzul umownych.

Klauzula 5

Pomoc dla administratora danych

(a) (Podmiot przetwarzający niezwłocznie powiadamia administratora o każdym żądaniu otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na wniosek samodzielnie, chyba że został do tego upoważniony przez administratora.

(b) Podmiot przetwarzający pomaga administratorowi wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do instrukcji administratora danych.

(c) Oprócz obowiązku podmiotu przetwarzającego do udzielenia administratorowi pomocy zgodnie z klauzulą 5(b), podmiot przetwarzający udziela ponadto administratorowi pomocy w zapewnieniu zgodności z następującymi obowiązkami, biorąc pod uwagę charakter przetwarzania danych i informacje dostępne podmiotowi przetwarzającemu:

(1) 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;

(2) obowiązek skonsultowania się z właściwym organem nadzorczym (właściwymi organami nadzorczymi) przed przetwarzaniem, jeżeli ocena skutków dla ochrony danych wskazuje, że przetwarzanie spowodowałoby wysokie ryzyko w przypadku braku środków podjętych przez administratora w celu ograniczenia ryzyka;

(3) obowiązek zapewnienia dokładności i aktualności danych osobowych poprzez niezwłoczne poinformowanie administratora, jeśli podmiot przetwarzający dowie się, że przetwarzane przez niego dane osobowe są niedokładne lub nieaktualne;

(4) obowiązki określone w art. 32 rozporządzenia (UE) 2016/679.

(d) Strony określają w załączniku II odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający ma obowiązek pomagać administratorowi w stosowaniu niniejszej klauzuli, a także zakres i zasięg wymaganej pomocy.

Klauzula 6

Powiadomienie o naruszeniu ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnieniu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679 lub art. 34 i 35 rozporządzenia (UE) 2018/1725, w stosownych przypadkach, z uwzględnieniem charakteru przetwarzania i informacji dostępnych podmiotowi przetwarzającemu.

6.1. Naruszenie dotyczące danych przetwarzanych przez administratora

W przypadku naruszenia ochrony danych osobowych dotyczących danych przetwarzanych przez administratora, podmiot przetwarzający udzieli administratorowi pomocy:

(a) zgłaszając naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu (właściwym organom nadzorczym) bez zbędnej zwłoki po powzięciu przez administratora wiadomości o naruszeniu, w stosownych przypadkach (chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);

(b) uzyskując następujące informacje, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 należy podać w powiadomieniu administratora i które muszą 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 rekordów danych osobowych, których dane dotyczą;

(2) prawdopodobne konsekwencje naruszenia ochrony danych osobowych

(3) środki podjęte lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki mające na celu złagodzenie jego ewentualnych negatywnych skutków.

W przypadku, gdy nie jest możliwe dostarczenie wszystkich tych informacji w tym samym czasie, wstępne powiadomienie powinno zawierać informacje dostępne w danym momencie, a dalsze informacje powinny być dostarczane bez zbędnej zwłoki w miarę ich dostępności.

(c) przestrzegając, zgodnie z art. 34 rozporządzenia (UE) 2016/679, obowiązku bezzwłocznego zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

6.2 Naruszenie dotyczące danych przetwarzanych przez podmiot przetwarzający

W przypadku naruszenia ochrony danych osobowych w odniesieniu do danych przetwarzanych przez podmiot przetwarzający, podmiot przetwarzający zawiadamia administratora bez zbędnej zwłoki po powzięciu wiadomości o naruszeniu. Takie powiadomienie powinno zawierać co najmniej:

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

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

(c) jego prawdopodobne konsekwencje oraz środki podjęte lub proponowane do podjęcia w celu zaradzenia naruszeniu, w tym w celu złagodzenia jego ewentualnych negatywnych skutków.

W przypadku, gdy nie jest możliwe dostarczenie wszystkich tych informacji w tym samym czasie, wstępne powiadomienie powinno zawierać informacje dostępne w danym momencie, a dalsze informacje powinny być dostarczane bez zbędnej zwłoki w miarę ich dostępności.

Strony określają w załączniku III wszystkie inne elementy, które podmiot przetwarzający ma zapewnić, wspierając administratora w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679.

SEKCJA III - POSTANOWIENIA KOŃCOWE

Klauzula 10
Nieprzestrzeganie klauzul i rozwiązanie umowy

(a) Bez uszczerbku dla jakichkolwiek przepisów rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725, w przypadku gdy podmiot przetwarzający narusza swoje zobowiązania wynikające z niniejszych klauzul, administrator może polecić podmiotowi przetwarzającemu zawieszenie przetwarzania danych osobowych do czasu, gdy ten ostatni zastosuje się do niniejszych klauzul lub umowa zostanie rozwiązana. Podmiot przetwarzający niezwłocznie poinformuje administratora, jeśli z jakiegokolwiek powodu nie będzie w stanie przestrzegać niniejszych klauzul.

(b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:

(1) przetwarzanie danych osobowych przez podmiot przetwarzający zostało zawieszone przez administratora zgodnie z lit. a) i jeśli zgodność z niniejszymi klauzulami nie zostanie przywrócona w zasadnym terminie, a w każdym razie w ciągu jednego miesiąca od zawieszenia;

(2) podmiot przetwarzający istotnie lub uporczywie narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725;

(3) podmiot przetwarzający nie zastosuje się do wiążącej decyzji właściwego sądu lub właściwego organu nadzorczego w odniesieniu do jego obowiązków wynikających z niniejszych klauzul lub rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

(c) Podmiot przetwarzający jest uprawniony do rozwiązania w zakresie, w jakim dotyczy ono przetwarzania danych osobowych na mocy niniejszych klauzul, jeżeli po poinformowaniu administratora, że jego instrukcje naruszają obowiązujące wymogi prawne zgodnie z klauzulą 4.1 (b), administrator nalega na przestrzeganie instrukcji.

(d) Po rozwiązaniu umowy podmiot przetwarzający, zgodnie z wyborem administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i zaświadcza administratorowi, że to zrobił, lub zwraca wszystkie dane osobowe administratorowi i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego wymaga przechowywania danych osobowych. Do czasu usunięcia lub zwrotu danych podmiot przetwarzający nadal zapewnia zgodność z niniejszymi klauzulami.

ZAŁĄCZNIK NR I

OPIS PRZETWARZANIA

Czynność przetwarzania: Serwis, Wsparcie, Doradztwo, Ddministracja, Zdalna pomoc techniczna

- Rozpoczęcie przetwarzania danych to: rozpoczęcie umowy o świadczenie usług

- Planowany okres przetwarzania danych to: Po zakończeniu umowy o świadczenie usług

Kontekst przetwarzania danych i obowiązki Stron dotyczące komercyjnego stosunku umownego są określone w umowie o świadczenie usług między Administratorem a Podmiotem przetwarzającym.

Kategorie osób, których dane dotyczą, charakter/cel przetwarzania, kategorie danych oraz wszelkie szczególne kategorie danych osobowych zależą od rodzaju świadczonej usługi, usług, których usługi dotyczą, oraz danych osobowych przechowywanych przez klienta, do których Olympus ma dostęp w trakcie świadczenia usługi.

Kategorie osób, których dane dotyczą	**Operacje przetwarzania**	**Kategorie danych**	**Szczególne kategorie danych osobowych - jeśli dotyczy**
☒ Pacjenci ☒ Osoby kontaktowe ☒ Pracownicy ☒ Byli pracownicy ☒ Distawcy i ich pracownicy	☒ Obsługa I konserwacja systemów i infrastuktury IT, np. systemów analitycznych ☒ Doradztwo w zakresie użytkowania produktów ☒ IT Wsparcie ☒ Wsparcie Techniczne ☒ Administracja ☒ Naprawa, testowanie lub konserwacja na miejscu lub w centrum napraw Olmpus ☒ Zdalna diagnostyka dla produktów hardware ☒ Zdalne testowanie/konserwacja oprogramowania ☒ Udostępnianie urządzeń zastępczych	☒ Informacje o koncie ☒ Firma ☒ Data urodzenia ☒ Zgoda na urządzenie i uprawnienia ☒ ID Urządzenia, nazwa urzązenia ☒ Dane logowania do urządzenia ☒ Adres E-Mail ☒ Płeć ☒ Identyfikator (analityka, umowam urządzenie) ☒ Język ☒ Lokalizacja ☒ Logi; ☒ Imię I nazwisko ☒ Główne dane użytkownika ☒ Dane użytkowania (adres IP, logowanie, rekord telefonu)	☒ Dane dotyczące zdrowia (np. imię i nazwisko pacjenta, informacje medyczne)

		☒ Dane dotyczące użytkowania (adres IP, logowanie, rejestr połączeń ☒ Dane dotyczące użytkowania urządzeń, systemów ☒ Dane dotyczące obrazów i wideo	

Praca na urządzeniu może wymagać skopiowania i przeanalizowania pliku dziennika urządzenia. Plik dziennika może zawierać nazwiska pacjentów. Wsparcie pierwszego i drugiego poziomu jest świadczone na terenie UE. Wsparcie trzeciego poziomu jest świadczone przez podmiot Olympus z siedzibą w USA („Olympus Surgical Technologies America"). W związku z tym, jeśli wsparcie trzeciego poziomu jest wymagane do rozwiązywania problemów, może być konieczne przesłanie danych do Stanów Zjednoczonych. Aby zapewnić odpowiedni poziom ochrony, Olmpus zawarł odpowiednie wewnętrzne umowy o przetwarzaniu danych (DPA) ze swoimi podmiotami stowarzyszonymi w USA.

ZAŁĄCZNIK III

ŚRODKI TECHNICZNE I ORGANIZACYJNE, W TYM ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE BEZPIECZEŃSTWO DANYCH

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Podmiot przetwarzający wdraża następujące środki techniczne i organizacyjne:

MIARA	OPIS
1. POUFNOŚĆ	
a) Kontrola dostępu – lokalizacje Olympus	Budynki Olympus są zamknięte i strzeżone dookoła. Pracownicy mogą wchodzić do budynków wyłącznie przy użyciu osobistej karty identyfikacyjnej. Odwiedzający mogą wejść do budynków wyłącznie przez recepcję w towarzystwie personelu. Osobom nieupoważnionym odmawia się wstępu do budynków. Wdrożono następujące środki bezpieczeństwa: - Identyfikatory dla pracowników/gości - System kontroli dostępu, czytnik kart, transponder, karty magnetyczne lub chipowe - Lobby/recepcja/portier - Blokada drzwi (elektrozaczep, drzwi z gałką zewnętrzną itp.) - Ochrona, portier - System nadzoru, system alarmowy, monitor wideo/TV
b) Kontrola dostępu – systemy	Wszystkie systemy są zainstalowane w bezpiecznych centrach danych i chronione osobistymi kartami identyfikacyjnymi w połączeniu z kodem PIN. Wdrożono następujące środki bezpieczeństwa: - Procedura bezpiecznego hasła (w tym znaki specjalne, minimalna długość, regularne zmiany hasła) - Automatyczne mechanizmy blokujące (np. hasło lub przełącznik pauzy, automatyczna blokada pulpitu) - Instrukcja ręcznego blokowania pulpitu - Konfiguracja i zarządzanie profilem użytkownika i rekordem głównym - Firewall, oprogramowanie antywirusowe dla serwerów i klientów

	- Korzystanie z VPN dla zdalnego dostępu - Polityka dotycząca urządzeń mobilnych
c) Kontrola dostępu - zarządzanie uprawnieniami: uprawnienia do odczytu i edycji Wewnętrzne systemy informatyczne Olympus	drożono systematyczne zarządzanie uprawnieniami do korzystania z systemów informatycznych. Dostęp do systemów jest możliwy tylko przy użyciu nazw użytkowników i haseł. Uprawnienia różnią się między uprawnieniami do odczytu i zapisu. Wdrożono następujące środki bezpieczeństwa: - Zróżnicowana koncepcja autoryzacji i prawa dostępu oparte na potrzebie wiedzy (profile, role, transakcje i obiekty)
d) Kontrola rozdzielenia Wewnętrzne systemy informatyczne Olympus	Zdalna konserwacja jest przeprowadzana oddzielnie dla każdego klienta. Wdrażane są następujące środki bezpieczeństwa: - Możliwość obsługi wielu klientów przez odpowiednie aplikacje - Oznaczanie - Separacja funkcjonalna środowiska produkcyjnego i testowego - Fizyczna separacja systemów, baz danych i nośników danych - Definicja praw do baz danych
e) Szyfrowanie	Wymagane jest szyfrowanie komunikacji w chmurze. Metoda szyfrowania jest najnowocześniejsza.
2. INTEGRALNOŚĆ	
a) Kontrola transferu Wewnętrzne systemy informatyczne Olympus	Wdrażane są następujące środki bezpieczeństwa: - Zakaz nieautoryzowanego odczytu, kopiowania, modyfikowania lub usuwania w ramach systemu. - Korzystanie z VPN, jeśli to możliwe, a także dostarczanie za pośrednictwem szyfrowanych połączeń, takich jak sftp, https
b) Kontrola wejścia	miany w systemach są rejestrowane. Wdrażane są następujące środki bezpieczeństwa: - Rejestrowanie dostępu - Systemy oceny dzienników i śledzenie wprowadzania, modyfikacji i usuwania danych przez poszczególne nazwy użytkowników - Przypisywanie uprawnień za pomocą spersonalizowanych kont użytkowników - Zarządzanie dokumentami
3. DOSTĘPNOŚĆ I WYTRZYMAŁOŚĆ	

a) Kontrola dostępności; środki ochrony danych Wewnętrzne systemy informatyczne Olympus	Dane osobowe są zabezpieczone. Zapewniona zostanie ochrona przed przypadkowym lub umyślnym zniszczeniem lub utratą, a także kontrola dostępności danych. Wdrożone są następujące środki bezpieczeństwa: - Procedura tworzenia kopii zapasowych: opis rytmu i nośnika kopii zapasowej, czas przechowywania i lokalizacja kopii zapasowej (online/offline, na miejscu/poza miejscem) - Dublowanie dysków twardych, np. procedura RAID - Zasilanie awaryjne (UPS) - Oddzielna pamięć lub partycja dla systemów operacyjnych i danych - Ochrona antywirusowa i zapora sieciowa - Kanały raportowania i plany awaryjne - Gaśnice i systemy alarmowe w budynkach, w szczególności w serwerowni, gdzie monitorowana jest również temperatura/wilgotność i zainstalowane są ochronne listwy gniazdowe.
b) Szybkie odzyskiwanie	Za odzyskanie danych odpowiada Administrator.
4. PROCEDURY REGULARNEGO PRZEGLĄDU, EWALUACJI I OCENY	
a) Kontrola zamówień Wewnętrzne systemy informatyczne Olympus	Skuteczność podjętych środków jest regularnie weryfikowana. Wdrożono następujące środki bezpieczeństwa: - Przejrzysty projekt umowy - Sformalizowane składanie zamówień - Wybór wykonawcy z zachowaniem należytej staranności (w odniesieniu do ochrony i bezpieczeństwa danych) - Zawarcie niezbędnej umowy zlecenia lub standardowych klauzul umownych UE - Instrukcje w formie pisemnej lub tekstowej dla wykonawcy - Zobowiązanie pracowników wykonawcy do zachowania tajemnicy danych - Obowiązek wyznaczenia inspektora ochrony danych przez wykonawcę, jeśli istnieje obowiązek zamówienia - Umowa w sprawie skutecznych praw kontroli wobec wykonawcy

	- Rozporządzenie w sprawie korzystania z dodatkowych podwykonawców - Zapewnienie zniszczenia danych po zakończeniu realizacji zamówienia - Bieżąca weryfikacja wykonawcy i jego poziomu ochrony
b) Zarządzanie prywatnością i reagowanie na incydenty	- Centralna dokumentacja wszystkich procedur i przepisów dotyczących ochrony danych z dostępem dla pracowników zgodnie z wymaganiami/upoważnieniami. - Wewnętrzny inspektor ds. bezpieczeństwa informacji i ochrony danych - Regularne szkolenia pracowników i zobowiązanie do zachowania poufności/prywatności. - Udokumentowany proces rozpoznawania i zgłaszania incydentów bezpieczeństwa / awarii danych - Udokumentowana procedura postępowania w przypadku incydentów bezpieczeństwa i naruszeń danych - Sformalizowana ocena wpływu na prywatność i proces obsługi wniosków o informacje od osób, których dane dotyczą

ANNEX III

LISTA PODWYKONAWCÓW PRZETWARZANIA

Administrator zezwolił na korzystanie z usług następujących podwykonawców przetwarzania:

Nazwa i adres	**Imię i nazwisko osoby kontaktowej, stanowisko i dane kontaktowe**	**Opis przetwarzania**	**W stosownych przypadkach, zabezpieczenia dotyczące przekazywania danych do państw trzecich**
Olympus Europa SE & Co. KG Wendenstraße 20 20097 Hamburg Germany	Stefan Limbacher Data Protection Officer EMEA privacy@olympus.com	Wsparcie drugiego poziomu w zakresie napraw, konserwacji i zdalnej obsługi oprogramowania i urządzeń medycznych	Nie dotyczy, Podwykonawca przetwarzania znajduje się w Hamburgu, Niemcy
Olympus Surgical Technologies Europe **Olympus Winter & Ibe GmbH** Kuehnstraße 61 22045 Hamburg Germany	privacy@olympus.com	Wsparcie trzeciego poziomu w zakresie napraw, konserwacji i zdalnej obsługi oprogramowania i urządzeń medycznych	Nie dotyczy, Podwykonawca przetwarzania znajduje się w Hamburgu, Niemcy
Olympus Medical Systems Corporation 2951 Ishikawa-machi, Hachioji-shi Tokyo 192-8507 Japan	privacy@olympus.com	Obsługa reklamacji, w tym dochodzenie w sprawie nieprawidłowego działania i nieoczekiwanych błędów.	Decyzja Komisji UE w sprawie adekwatności (UE) 2019/419

Olympus Surgical Technologies America 800 W Park Dr. Westborough, MA 01581 USA	privacy@olympus.com	Obsługa reklamacji, w tym dochodzenie w sprawie nieprawidłowego działania i nieoczekiwanych błędów.	Standardowe klauzule umowne (w ramach Grupy Olympus)
Tata Consultancy Services GmbH Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Germany	privacy@olympus.com	Infrastruktura IT i dostawca usług	Nie dotyczy, Podwykonawca przetwarzania znajduje się we Frankfurcie, Niemcy
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Germany	privacy@teamviewer.com	Monitorowanie i sterowanie komputerowe	Nie dotyczy, Podwykonawca przetwarzania znajduje się w Göppingen, Niemcy
ImageStreamMedical One Monarch Drive Littleton, MA 01460 USA	privacy@cision.com	Wsparcie trzeciego poziomu w zakresie napraw, konserwacji i zdalnej obsługi oprogramowania i urządzeń medycznych	Standardowe klauzule umowne
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521 Ireland	privacy@microsoft.com	Różne usługi w chmurze	Nie dotyczy, Podwykonawca przetwarzania znajduje się w Irlandii

RealVNC Limited 50-60 Station Road Cambridge Cambridgeshire CB1 2JH Vereinigtes Königreich von Großbritannien und Nordirland	privacy@realvnc.com	Dostawca oprogramowania do zdalnego sterowania dla stacji roboczej SPiN Planning Laptop - Brak przechowywania danych, tylko szyfrowane udostępnianie ekranu	Decyzja w sprawie adekwatności dla Zjednoczonego Królestwa