Términos de Tratamiento de Datos para Servicios

A partir de: 30 de abril de 2025, versión 1.0

SECCIÓN I

Cláusula 1
Finalidad y ámbito de aplicación

(a) La finalidad de los presentes Términos de Tratamiento de Datos (en lo sucesivo, «pliego de cláusulas») es garantizar que se cumpla el artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

(b) OLYMPUS IBERIA, S.A.U, con domicilio en Pl. Europa, nº10, 2ª Planta, 08902 L'Hospitalet de Llobregat (encargado) y el responsable del tratamiento han dado su consentimiento a vincularse por el presente pliego de cláusulas a fin de garantizar el cumplimiento del artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 y/o del artículo 29, apartados 3 y 4, del Reglamento (UE) 2018/1725.

(c) El presente pliego de cláusulas se aplica al tratamiento de datos personales especificado en el anexo II.

(d) Los anexos I a IV forman parte del pliego.

(e) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el responsable en virtud del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

(f) El presente pliego de cláusulas no garantiza por sí mismo el cumplimiento de las obligaciones relativas a las transferencias internacionales contempladas en el capítulo V del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

Cláusula 2
Interpretación

(a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679 o en el Reglamento (UE) 2018/1725, se entiende que tienen el mismo significado que en el Reglamento correspondiente.

(b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

(c) No se podrán realizar interpretaciones del presente pliego de cláusulas que entren en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679 y el Reglamento (UE) 2018/1725 y/o que perjudiquen los derechos o libertades fundamentales de los interesados.

SECCIÓN II – OBLIGACIONES DE LAS PARTES

Cláusula 3
Descripción del tratamiento o tratamientos

En el anexo II se especifican los pormenores de las operaciones de tratamiento y, en particular, las categorías de datos personales y los fines para los que se tratan los datos personales por cuenta del responsable.

Cláusula 4
Obligaciones de las partes

4.1. Instrucciones

(a) El encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado. En tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. El responsable también podrá dar instrucciones ulteriores en cualquier momento del período de tratamiento de los datos personales. Dichas instrucciones deberán estar siempre documentadas.

(b) El encargado informará inmediatamente al responsable si las instrucciones dadas por el responsable infringen, a juicio del encargado, el Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 o las disposiciones aplicables del Derecho de la Unión o de los Estados miembros en materia de protección de datos.

4.2. Limitación de la finalidad

El encargado tratará los datos personales únicamente para los fines específicos del tratamiento indicados en el anexo II, salvo cuando siga instrucciones adicionales del responsable.

4.3. Duración del tratamiento de datos personales

El tratamiento por parte del encargado solo se realizará durante el período especificado en el anexo II.

4.4. Seguridad del tratamiento

(a) El encargado aplicará, como mínimo, las medidas técnicas y organizativas especificadas en el anexo III para garantizar la seguridad de los datos personales. Una de estas medidas podrá consistir en la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos («violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados.

(b) El encargado solo concederá acceso a los datos personales tratados a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. El encargado garantizará que las personas autorizadas para tratar los datos personales recibidos se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

4.5. Datos sensibles

Si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales («datos sensibles»), el encargado aplicará restricciones específicas y/o garantías adicionales.

4.6 Documentación y cumplimiento

(a) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas.

(b) El encargado resolverá con presteza y de forma adecuada las consultas del responsable relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

(c) El encargado pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y que deriven directamente del Reglamento (UE) 2016/679 y del Reglamento (UE) 2018/1725. A instancia del responsable, el encargado permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el responsable podrá tener en cuenta las certificaciones pertinentes que obren en poder del encargado.

d) El responsable podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías también podrán consistir en inspecciones de los locales o instalaciones físicas del encargado y, cuando proceda, realizarse con un preaviso razonable.

e) Las partes pondrán a disposición de las autoridades de control competentes, a instancia de estas, la información a que se refiere la presente cláusula y, en particular, los resultados de las auditorías.

4.7. Recurso a subencargados

(a) El encargado cuenta con una autorización general del responsable para contratar a subencargados que figuren en una lista acordada en el Anexo III. El encargado informará al responsable específicamente de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos cuatro semanas de antelación, de modo que el responsable tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El encargado del tratamiento proporcionará al responsable la información necesaria para que pueda ejercer su derecho a formular objeción.

(b) Cuando el encargado contrate a un subencargado para llevar a cabo actividades de tratamiento específicas (por cuenta del responsable), lo hará por medio de un contrato que imponga al subencargado, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al encargado en virtud del presente pliego de cláusulas. El encargado se asegurará de que el subencargado cumpla las obligaciones a las que esté sujeto en virtud del presente pliego de cláusulas y del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

c) El encargado proporcionará al responsable, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el encargado podrá expurgar el texto del contrato antes de compartir la copia.

d) El encargado seguirá siendo plenamente responsable ante el responsable del cumplimiento de las obligaciones que imponga al subencargado su contrato con el encargado. El encargado notificará al responsable los incumplimientos por parte del subencargado de las obligaciones que le atribuya dicho contrato.

4.8. Transferencias internacionales

(a) Las transferencias de datos a un tercer país o a una organización internacional por parte del encargado solo podrán realizarse siguiendo instrucciones documentadas del responsable o en virtud de una exigencia expresa del Derecho de la Unión o del Estado miembro al que esté sujeto el encargado; se llevarán a cabo de conformidad con el capítulo V del Reglamento (UE) 2016/679 o del Reglamento (UE) 2018/1725.

(b) El responsable se aviene a que, cuando el encargado recurra a un subencargado de conformidad con la cláusula 4.7 para llevar a cabo actividades de tratamiento específicas (por cuenta del responsable) y dichas actividades conlleven una transferencia de datos personales en el sentido del capítulo V del Reglamento (UE) 2016/679, el encargado y el subencargado puedan garantizar el cumplimiento del capítulo V del Reglamento (UE) 2016/679 utilizando cláusulas contractuales tipo adoptadas por la Comisión, con arreglo al artículo 46, apartado 2, del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones para la utilización de dichas cláusulas contractuales tipo.

Cláusula 5
Ayuda al responsable del tratamiento

(a) El encargado notificará con presteza al responsable las solicitudes que reciba del interesado. No responderá a dicha solicitud por sí mismo, a menos que el responsable le haya autorizado a hacerlo.

b) El encargado ayudará al responsable a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos de los interesados teniendo en cuenta la naturaleza del tratamiento. En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el encargado cumplirá las instrucciones del responsable.

c) Además de la obligación del encargado de ayudar al responsable en virtud de la cláusula 5, letra b), el encargado también ayudará al responsable a garantizar el cumplimiento de las obligaciones siguientes teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el encargado:

1) la obligación de realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales («evaluación de impacto») cuando sea probable que un tipo de tratamiento suponga un alto riesgo para los derechos y libertades de las personas físicas;

2) la obligación de consultar a las autoridades de control competentes antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo;

3) la obligación de garantizar que los datos personales sean exactos y estén actualizados, informando sin demora al responsable si el encargado descubre que los datos personales que está tratando son inexactos o han quedado obsoletos;

4) las obligaciones contempladas en el artículo 32 del Reglamento (UE) 2016/679.

(d) Las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas que obliguen al encargado a ayudar al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

Cláusula 6

Notificación de violaciones de la seguridad de los datos personales

En caso de violación de la seguridad de los datos personales, el encargado colaborará con el responsable y le ayudará a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del Reglamento (UE) 2016/679 o los artículos 34 y 35 del Reglamento (UE) 2018/1725, en su caso, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el encargado.

6.1 Violación de la seguridad de datos personales tratados por el responsable

En caso de violación de la seguridad de los datos personales en relación con los datos tratados por el responsable, el encargado ayudará al responsable en lo siguiente.

a) Notificar la violación de la seguridad de los datos personales a las autoridades de control competentees sin dilación indebida una vez tenga constancia de ella, si procede (a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas).

(b) Recabar la información siguiente, que, de conformidad con el artículo 33, apartado 3, del Reglamento (UE) 2016/679, deberá figurar en la notificación del responsable, que debe incluir como mínimo:

(1) la naturaleza de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

2) las consecuencias probables de la violación de la seguridad de los datos personales;

3) las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

(c) Cumplir, con arreglo al artículo 34 del Reglamento (UE) 2016/679 la obligación de comunicar sin dilación indebida al interesado la violación de la seguridad de los datos personales cuando sea probable que la violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas.

6.2 Violación de la seguridad de datos personales tratados por el encargado

En caso de violación de la seguridad de datos personales tratados por el encargado, este lo notificará al responsable sin dilación indebida una vez que el encargado tenga constancia de ella. Dicha notificación deberá incluir como mínimo:

a) una descripción de la naturaleza de la violación de la seguridad (inclusive, cuando sea posible, las categorías y el número aproximado de interesados y de registros de datos afectados);

b) los datos de un punto de contacto en el que pueda obtenerse más información sobre la violación de la seguridad de los datos personales;

c) sus consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

Las partes establecerán en el anexo III los demás elementos que deberá aportar el encargado cuando ayude al responsable a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del Reglamento (UE) 2016/679.

SECCIÓN III – DISPOSICIONES FINALES

Cláusula 7
Incumplimiento de las cláusulas y resolución del contrato

(a) Sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725, en caso de que el encargado del tratamiento incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el responsable podrá ordenar al encargado que suspenda el tratamiento de datos personales hasta que este vuelva a dar cumplimiento al presente pliego de cláusulas, o resolver el contrato. El encargado informará con presteza al responsable en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

(b) El responsable estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

(1) el tratamiento de datos personales por parte del encargado haya sido suspendido por el responsable con arreglo a la letra a) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

(2) el encargado incumpla de manera sustancial o persistente el presente pliego de cláusulas o las obligaciones que le atribuye el Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725;

(3) el encargado incumpla una resolución vinculante de un órgano jurisdiccional competente o de las autoridades de control competentes en relación con las obligaciones que les atribuye el presente pliego de cláusulas, el Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725.

(c) El encargado estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando, tras haber informado al responsable de que sus instrucciones infringen los requisitos jurídicos exigidos por la cláusula 4.1, letra b), el responsable insiste en que se sigan dichas instrucciones.

(d) Tras la resolución del contrato, el encargado suprimirá, a petición del responsable, todos los datos personales tratados por cuenta del responsable y acreditará al responsable que lo ha hecho, o devolverá todos los datos personales al responsable y suprimirá las copias existentes, a menos que el Derecho de la Unión o de los Estados miembros exija el almacenamiento de los datos personales. Hasta que se destruyan o devuelvan los datos, el encargado seguirá garantizando el cumplimiento con el presente pliego de cláusulas.

ANEXO I

DESCRIPCIÓN DEL TRATAMIENTO

Actividad de tratamiento: Servicio, Soporte, Consultoría, Administración, Mantenimiento Remoto

- El inicio del tratamiento de datos es: inicio del contrato de servicio
- La duración prevista del tratamiento de datos es: Hasta la terminación del contrato de servicio

El contexto del tratamiento de datos y las obligaciones de las partes con respecto a la relación contractual comercial se especifican en el contrato de servicio entre el responsable y el encargado.

Las categorías de los interesados, la naturaleza/propósito del tratamiento, las categorías de datos y cualquier categoría especial de datos personales dependen del tipo de servicio proporcionado, los servicios a los que se relacionan los servicios y los datos personales almacenados por el cliente a los que Olympus tiene acceso en el curso de la prestación del servicio.

Categorías de interesados	**Operaciones de tratamiento**	**Categorías de datos**	**Categorías especiales de datos personales – si aplica**
☒ Pacientes ☒Personas de contacto ☒Empleados ☒Ex empleados ☒ Proveedores y sus empleados	☒ Operación y mantenimiento de sistemas e infraestructura de IT, por ejemplo, sistemas analíticos ☒ Consultoría sobre el uso del producto ☒Soporte de IT ☒ Soporte técnico ☒ Administración ☒ Reparación, prueba o mantenimiento en el sitio o en el centro de reparación de Olympus ☒ Diagnóstico remoto de hardware para productos de hardware ☒ Pruebas/mantenimiento remoto de servicios para productos de software ☒ Provisión de dispositivos de préstamo	☒Información de la cuenta ☒Empresa ☒Fecha de nacimiento ☒Consentimiento y permisos del dispositivo ☒ID del dispositivo, nombre del dispositivo ☒Datos de inicio de sesión del dispositivo ☒Dirección de correo electrónico ☒Género ☒ID (análisis de datos, contrato, dispositivo) ☒Idioma ☒Ubicación ☒Registros; ☒Nombre ☒Nombre de usuario ☒ Datos principales del usuario	☒Datos de salud (por ejemplo, nombre del paciente, información médica)

		☒Datos de uso (dirección IP, registro, grabación telefónica) ☒ Datos de uso de dispositivos, sistemas ☒ Datos de imagen y video	

El trabajo en el dispositivo puede requerir copiar y analizar el archivo de registro del dispositivo. El archivo de registro puede contener nombres de pacientes. El soporte de primer y segundo nivel se proporciona dentro de la UE. El soporte de tercer nivel es proporcionado por una entidad de Olympus con sede en los EE. UU. ("Olympus Surgical Technologies America"). Por lo tanto, si se requiere soporte de tercer nivel para la resolución de problemas, puede ser necesario transferir datos a los Estados Unidos. Para garantizar un nivel adecuado de protección, Olympus ha concluido acuerdos internos apropiados de tratamiento de datos con sus entidades afiliadas en los EE. UU.

ANEXO II

MEDIDAS TÉCNICAS Y ORGANIZATIVAS, INCLUIDAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

Teniendo en cuenta el estado de la técnica, los costes de implementación y la naturaleza, alcance, contexto y propósitos del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el encargado implementará las siguientes medidas técnicas y organizativas:

MEDIDA	DESCRIPCIÓN
1. CONFIDENCIALIDAD	
a) Control de acceso – ubicaciones de Olympus	Los edificios de Olympus están cerrados y vigilados en su totalidad. Los empleados solo pueden ingresar a los edificios utilizando su tarjeta de identificación personal. Los visitantes solo pueden ingresar a los edificios a través de la recepción y acompañados por el personal. Se niega el acceso a personas no autorizadas. Se implementan las siguientes medidas de seguridad: - Insignias para empleados/visitantes - Sistema de control de acceso, lector de tarjetas, transpondedor, tarjetas magnéticas o con chip - Vestíbulo/recepcionista/portero - Llaves controladas/asignación de llaves - Cerradura de puerta (abrepuertas eléctrico, puertas con perilla exterior, etc.) - Seguridad de fábrica, portero - Sistema de vigilancia, sistema de alarma, monitor de video/TV
b) Control de acceso – sistemas	Todos los sistemas están instalados en centros de datos seguros y protegidos por tarjetas de identificación personal en combinación con PIN. Se implementan las siguientes medidas de seguridad:

	- Procedimiento de contraseña segura (incluidos caracteres especiales, longitud mínima, cambios regulares de contraseña) - Mecanismos de bloqueo automático (por ejemplo, contraseña o interruptor de pausa, bloqueo automático del escritorio) - Instrucción para el bloqueo manual del escritorio - Configuración y gestión de un perfil de usuario y registro maestro - Firewall, software antivirus para servidores y clientes - Uso de VPN para acceso remoto - Política de dispositivos móviles
c) Control de acceso - gestión de derechos: autoridad de lectura y edición Sistemas internos de TI de Olympus	Se implementa una gestión sistemática de derechos para el uso de los sistemas de TI. El acceso a los sistemas solo es posible con nombres de usuario y contraseñas. Las autorizaciones difieren entre permisos de lectura y escritura. Se implementan las siguientes medidas de seguridad: - Concepto de autorización diferenciado y derechos de acceso basados en la necesidad de saber (perfiles, roles, transacciones y objetos)
d) Control de separación Sistemas internos de TI de Olympus	El mantenimiento remoto se lleva a cabo por separado para cada cliente. Se implementan las siguientes medidas de seguridad: - Capacidad multicliente de las aplicaciones relevantes - Asignación - Separación funcional del entorno productivo y de prueba - Separación física de sistemas, bases de datos y soportes de datos - Definición de derechos de base de datos
e) Cifrado	Se prefiere el cifrado de la comunicación. El método de cifrado es de última generación.
2. INTEGRIDAD	

a) Control de transferencia Sistemas internos de IT de Olympus	Se implementan las siguientes medidas de seguridad: - Es posible el cifrado de correos electrónicos en la red - No se permite la lectura, copia, modificación o eliminación no autorizada dentro del sistema - Uso de VPN, así como provisión a través de conexiones cifradas como sftp, https
b) Control de entrada	Los cambios en los sistemas se registran. Se implementan las siguientes medidas de seguridad: - Registro de accesos - Sistemas de evaluación de registros y trazabilidad de entrada, modificación y eliminación de datos por nombres de usuario individuales - Asignación de derechos a través de cuentas de usuario personalizadas - Gestión de documentos
3. DISPONIBILIDAD Y RESILIENCIA	
a) Control de disponibilidad; medidas de protección de datos Sistemas internos de IT de Olympus	Los datos personales están asegurados. Se garantizará la protección contra la destrucción o pérdida accidental o intencionada, así como el control de la disponibilidad de los datos. Se implementan las siguientes medidas de seguridad: - Procedimiento de respaldo: descripción del ritmo y medio del respaldo, tiempo de almacenamiento y ubicación del respaldo (en línea/fuera de línea, en el sitio/fuera del sitio) - Espejado de discos duros, por ejemplo, procedimiento RAID - Suministro ininterrumpido de energía (UPS) - Almacenamiento o partición separada para sistemas operativos y datos - Protección contra virus y firewall - Canales de reporte y planes de emergencia - Extintores y sistemas de alarma en edificios, en particular en la sala de servidores, donde también se monitorea la temperatura/humedad y se instalan regletas de enchufes protectores

b) Recuperación rápida	La recuperación de datos es responsabilidad del Controlador.
4. PROCEDIMIENTOS PARA REVISIÓN, EVALUACIÓN Y VALORACIÓN REGULARES	
a) Control de pedidos Sistemas internos de IT de Olympus	La efectividad de las medidas tomadas se revisa regularmente. El control de pedidos se verifica de manera aleatoria. Se implementan las siguientes medidas de seguridad: - Diseño claro del contrato - Colocación formalizada de pedidos - Selección del contratista bajo aspectos de diligencia debida (con respecto a la protección de datos y seguridad) - Conclusión del acuerdo necesario para el acuerdo de pedido o cláusulas contractuales estándar de la UE - Instrucciones por escrito o en forma de texto al contratista - Obligación de los empleados del contratista a la confidencialidad de los datos - Obligación de nombrar un oficial de protección de datos por parte del contratista si existe la obligación de ordenarlo - Acuerdo sobre derechos de control efectivos frente al contratista - Regulación sobre el uso de subcontratistas adicionales - Garantizar la destrucción de datos después de la finalización del pedido - Verificación continua del contratista y su nivel de protección

b) Gestión de privacidad y respuesta a incidentes	- Documentación central de todos los procedimientos y regulaciones para la protección de datos con acceso para empleados según sea necesario/autorizado - Responsable interno de Seguridad de la Información y Protección de Datos - Capacitación regular de empleados y compromiso con la confidencialidad/privacidad - Proceso documentado para el reconocimiento y reporte de incidentes de seguridad / fallos de datos (también con respecto a la notificación obligatoria a las autoridades de supervisión) - Procedimiento documentado para tratar incidentes de seguridad y violaciones de datos - Evaluación formalizada del impacto en la privacidad y proceso para manejar solicitudes de información de los interesados

ANEXO III

LISTA DE SUBPROCESADORES

El responsable ha autorizado el uso de los siguientes subencargados:

Nombre y dirección	**Nombre, posición y datos de contacto de la persona de contacto**	**Descripción del tratamiento**	**Si corresponde, salvaguardas para transferencias a terceros países**
Olympus Europa SE & Co. KG Wendenstraße 20 20097 Hamburgo Alemania	Stefan Limbacher Delegado de Protección de Datos EMEA privacy@olympus.com	Soporte de segundo nivel para reparación, mantenimiento y mantenimiento remoto de software y dispositivos médicos	n/a, los subencargados están ubicados en Hamburgo, Alemania
Olympus Surgical Technologies Europe **Olympus Winter & Ibe GmbH** Kuehnstraße 61 22045 Hamburgo Alemania	privacy@olympus.com	Soporte de tercer nivel para reparación, mantenimiento y mantenimiento remoto de software y dispositivos médicos	n/a, los subencargados están ubicados en Hamburgo, Alemania
Olympus Medical Systems Corporation 2951 Ishikawa-machi, Hachioji-shi Tokio 192-8507 Japón	privacy@olympus.com	Gestión de reclamaciones, incluida la investigación de fallos y errores inesperados.	Decisión de adecuación (UE) 2019/419 por la Comisión de la UE

Olympus Surgical Technologies America 800 W Park Dr. Westborough, MA 01581 EE. UU.	privacy@olympus.com	Gestión de reclamaciones, incluida la investigación de fallos y errores inesperados.	Cláusulas contractuales tipo
Tata Consultancy Services GmbH Friedrich-Ebert-Anlage 49 60308 Fráncfort del Meno Alemania	privacy@olympus.com	Proveedor de infraestructura y servicios de IT	n/a, los subencargados están ubicados en Frankfurt, Alemania
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Alemania	privacy@teamviewer.com	Monitoreo y control de computadoras	n/a, los subencargados están ubicados en Göppingen, Alemania
ImageStreamMedical One Monarch Drive Littleton, MA 01460 EE. UU.	privacy@cision.com	Soporte de tercer nivel para reparación, mantenimiento y mantenimiento remoto de software	Cláusulas contractuales tipo
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublín 18 D18 P521 Irlanda	privacy@microsoft.com	Varios servicios en la nube	n/a, los subencargados están ubicados en Irlanda

RealVNC Limited 50-60 Station Road Cambridge Cambridgeshire CB1 2JH Reino Unido de Gran Bretaña e Irlanda del Norte	privacy@realvnc.com	Proveedor de software de control remoto para la estación de trabajo portátil SPiN Planning – Sin almacenamiento de datos, solo uso compartido de pantalla cifrado	Decisión de adecuación para el Reino Unido