

TERMOS DE TRATAMENTO DE DADOS PARA SERVIÇOS

Com data de: 30 de abril de 2025, versão 1.0

SECÇÃO I

Cláusula 1

Finalidade e âmbito de aplicação

- (a) Os presentes Termos de Tratamento de Dados (cláusulas) visam assegurar a conformidade com o artigo 28.º, n.os 3 e 4, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- (b) OLYMPUS IBERIA, S.A.U. Sucursal em Portugal, Rua Castilho, nº39-15º, 1250-068 Lisboa - Portugal (subcontratante) e o responsável pelo tratamento acordam nas presentes cláusulas a fim de assegurar o cumprimento do disposto no artigo 28.º, n.os 3 e 4, do Regulamento (UE) 2016/679 e/ou no artigo 29.º, n.os 3 e 4, do Regulamento (UE) 2018/1725.
- (c) As presentes cláusulas são aplicáveis ao tratamento de dados pessoais, conforme especificado no anexo I.
- (d) Os anexos I a III são parte integrante das cláusulas.
- (e) As presentes cláusulas não prejudicam as obrigações a que o responsável pelo tratamento está sujeito por força do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725.
- (f) As presentes cláusulas não garantem, por si só, o cumprimento das obrigações relacionadas com as transferências internacionais em conformidade com o capítulo V do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725.

Cláusula 2

Interpretação

- (a) Caso as presentes cláusulas utilizem os termos definidos no Regulamento (UE) 2016/679 ou no Regulamento (UE) 2018/1725, respetivamente, esses termos terão o mesmo significado que lhes é atribuído no regulamento em causa.
- (b) As presentes cláusulas devem ser lidas e interpretadas à luz das disposições do Regulamento (UE) 2016/679 ou do Regulamento (UE) 2018/1725, respetivamente.
- (c) As presentes cláusulas não devem ser interpretadas de forma contrária aos direitos e obrigações previstos no Regulamento (UE) 2016/679/Regulamento (UE) 2018/1725, sem prejuízo dos direitos e das liberdades fundamentais dos titulares dos dados.

SECÇÃO II – OBRIGAÇÕES DAS PARTES

Cláusula 3

Descrição do(s) tratamento(s)

Os pormenores das operações de tratamento, em particular as categorias de dados pessoais e as finalidades do tratamento para as quais os dados pessoais são tratados por conta do responsável pelo tratamento, são especificados no anexo I.

Cláusula 4

Obrigações das Partes

4.1. Instruções

- (a) O subcontratante deve proceder ao tratamento de dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, salvo se for obrigado a fazê-lo pelo direito da União ou pelo direito do Estado-Membro a que esteja sujeito. Neste caso, o subcontratante deve informar o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei o proibir por motivos importantes de interesse público. O

responsável pelo tratamento pode dar instruções subsequentes ao longo de toda a duração do tratamento de dados pessoais. Estas instruções devem ser sempre documentadas.

- (b) O subcontratante deve informar imediatamente o responsável pelo tratamento se, no seu entender, as instruções dadas pelo responsável pelo tratamento violarem o Regulamento (UE) 2016/679/Regulamento (UE) 2018/1725 ou as disposições aplicáveis do direito da União ou do direito dos Estados-Membros em matéria de proteção de dados.

4.2. Limitação das finalidades

O subcontratante deve proceder ao tratamento dos dados pessoais apenas para a(s) finalidade(s) específica(s) do tratamento, conforme estabelecido no anexo I, salvo se receber instruções adicionais do responsável pelo tratamento.

4.3. Duração do tratamento de dados pessoais

O tratamento pelo subcontratante só pode ocorrer durante o período especificado no anexo I.

4.4. Segurança do tratamento

- (a) O subcontratante deve, pelo menos, aplicar as medidas técnicas e organizativas especificadas no anexo II para garantir a segurança dos dados pessoais. Tal inclui a proteção dos dados contra uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados aos dados (violação de dados pessoais). Ao avaliar o nível de segurança adequado, as Partes devem ter em devida conta as técnicas mais avançadas, os custos de aplicação, a natureza, o âmbito, o contexto e as finalidades do tratamento e os riscos para os titulares dos dados.
- (b) O subcontratante só deve conceder acesso aos dados pessoais objeto de tratamento aos membros do seu pessoal na medida estritamente necessária para a execução, a gestão e o acompanhamento do contrato. O subcontratante deve assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas às obrigações legais de confidencialidade adequadas.

4.5. Dados sensíveis

Se o tratamento envolver dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, dados genéticos ou biométricos destinados a identificar uma pessoa singular de forma inequívoca, dados relativos à saúde, à vida sexual ou à orientação sexual de uma pessoa ou dados relacionados com condenações penais e com infrações («dados sensíveis»), o subcontratante deve aplicar limitações específicas e/ou garantias adicionais.

4.6 Documentação e cumprimento

- (a) As Partes devem poder demonstrar o cumprimento das presentes cláusulas.
- (b) O subcontratante deve responder, rápida e adequadamente, aos pedidos de informação do responsável pelo tratamento sobre o tratamento de dados, em conformidade com as presentes cláusulas.
- (c) O subcontratante deve disponibilizar ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas nas presentes cláusulas decorrentes diretamente do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725. A pedido do responsável pelo tratamento, o subcontratante deve igualmente facilitar e contribuir para as auditorias das operações de tratamento abrangidas pelas presentes cláusulas, a intervalos razoáveis ou se houver indícios de incumprimento. Ao decidir sobre uma revisão ou uma auditoria, o responsável pelo tratamento pode ter em conta as certificações pertinentes detidas pelo subcontratante.
- (d) O responsável pelo tratamento pode optar por realizar, ele próprio, a auditoria ou mandar um auditor independente. As auditorias podem igualmente incluir inspeções nos edifícios ou nas instalações físicas do subcontratante, devendo, se for caso disso, ser realizadas com uma antecedência razoável.
- (e) As Partes devem disponibilizar as informações referidas na presente cláusula, incluindo os resultados de quaisquer auditorias, à(s) autoridade de controlo competente(s), mediante pedido.

4.7. Recurso a subcontratantes ulteriores

- (a) O subcontratante tem a autorização geral do responsável pelo tratamento para a contratação de subcontratantes ulteriores a partir de uma lista acordada no Anexo III. O subcontratante

deve informar especificamente o responsável pelo tratamento, das alterações pretendidas a efetuar a essa lista quanto ao aumento do número ou à substituição de subcontratante ulteriores com uma antecedência mínima de duas semanas, dando assim ao responsável pelo tratamento tempo suficiente para se opor a essas alterações antes da contratação do(s) subcontratante(s) ulterior(es) em causa. O subcontratante deve fornecer ao responsável pelo tratamento as informações necessárias para que este último possa exercer o direito de oposição.

- (b) Caso o subcontratante contrate um subcontratante ulterior para realizar operações específicas de tratamento (por conta do responsável pelo tratamento), deve fazê-lo através de um contrato que imponha ao subcontratante ulterior, do ponto de vista material, as mesmas obrigações em matéria de proteção de dados que as impostas ao subcontratante em conformidade com as presentes cláusulas. O subcontratante deve assegurar o cumprimento, pelo subcontratante ulterior, das obrigações a que o subcontratante está sujeito nos termos das presentes cláusulas e do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725.
- (c) O subcontratante deve facultar ao responsável pelo tratamento, a pedido do mesmo, uma cópia do referido acordo de subcontratação e de quaisquer alterações subsequentes. Na medida do necessário para proteger segredos comerciais ou outras informações confidenciais, incluindo dados pessoais, o subcontratante pode editar o texto do acordo antes de partilhar a cópia.
- (d) O subcontratante continua a ser inteiramente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações que incumbem ao subcontratante ulterior em conformidade com o seu contrato com o subcontratante. O subcontratante deve notificar o responsável pelo tratamento de qualquer incumprimento, pelo subcontratante ulterior, das obrigações contratuais que lhe incumbem.

4.8. Transferências internacionais

- (a) Qualquer transferência de dados para um país terceiro ou para uma organização internacional pelo subcontratante só pode ser efetuada com base em instruções documentadas do responsável pelo tratamento ou a fim de cumprir um requisito específico ao abrigo do direito da União ou do direito do Estado-Membro a que o subcontratante esteja sujeito e deve ter lugar em conformidade com o capítulo V do Regulamento (UE) 2016/679 ou do Regulamento (UE) 2018/1725.
- (b) O responsável pelo tratamento concorda que, caso o subcontratante contrate um subcontratante ulterior, em conformidade com a cláusula 4.7, para realizar operações específicas de tratamento (por conta do responsável pelo tratamento) e essas operações de tratamento envolvam uma transferência de dados pessoais na aceção do capítulo V do Regulamento (UE) 2016/679, o subcontratante e o subcontratante ulterior podem assegurar o cumprimento do capítulo V do Regulamento (UE) 2016/679 recorrendo às cláusulas contratuais-tipo adotadas pela Comissão em conformidade com o artigo 46.º, n.º 2, do Regulamento (UE) 2016/679, desde que as condições para o recurso a essas cláusulas contratuais-tipo sejam cumpridas.

Cláusula 5

Assistência ao responsável pelo tratamento

- (a) O subcontratante deve notificar imediatamente o responsável pelo tratamento de qualquer pedido que tenha recebido do titular dos dados. Não pode responder ele próprio a esse pedido, salvo se autorizado a fazê-lo pelo responsável pelo tratamento.
- (b) O subcontratante deve prestar assistência ao responsável pelo tratamento no cumprimento das suas obrigações de resposta aos pedidos de exercício de direitos apresentados pelos titulares dos dados, tendo em conta a natureza do tratamento. No cumprimento das obrigações que lhe incumbem por força das alíneas a) e b), o subcontratante deve cumprir as instruções do responsável pelo tratamento.
- (c) Para além da obrigação que incumbe ao subcontratante de prestar assistência ao responsável pelo tratamento nos termos da cláusula 5, alínea b), o subcontratante deve ainda prestar assistência ao responsável pelo tratamento para assegurar o cumprimento das obrigações a seguir indicadas, tendo em conta a natureza do tratamento de dados e as informações ao seu dispor:

- (1) a obrigação de proceder a uma avaliação do impacto das operações de tratamento previstas na proteção de dados pessoais (uma «avaliação de impacto relativa à proteção de dados») caso um tipo de tratamento seja suscetível de constituir um elevado risco para os direitos e as liberdades das pessoas singulares;
 - (2) a obrigação de consultar a(s) autoridade de controlo competente(s) antes de proceder ao tratamento quando a avaliação de impacto relativa à proteção de dados indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco;
 - (3) a obrigação de assegurar que os dados pessoais sejam exatos e atualizados, informando sem demora o responsável pelo tratamento se o subcontratante tomar conhecimento de que os dados pessoais que está a tratar são inexatos ou estão desatualizados;
 - (4) as obrigações previstas no artigo 32.º do Regulamento (UE) 2016/679.
- (d) As Partes devem estabelecer, no anexo III, as medidas técnicas e organizativas adequadas através das quais o subcontratante é obrigado a prestar assistência ao responsável pelo tratamento na aplicação da presente cláusula, bem como o âmbito e a amplitude da assistência necessária.

Cláusula 6

Notificação de violação de dados pessoais

Em caso de violação de dados pessoais, o subcontratante deve cooperar com o responsável pelo tratamento e prestar-lhe assistência para que este cumpra as obrigações que lhe incumbem por força dos artigos 33.º e 34.º do Regulamento (UE) 2016/679 ou dos artigos 34.º e 35.º do Regulamento (UE) 2018/1725, se aplicável, tendo em conta a natureza do tratamento e as informações ao seu dispor.

6.1 Violação de dados relativa a dados tratados pelo responsável pelo tratamento

Em caso de violação de dados pessoais relativa a dados tratados pelo responsável pelo tratamento, o subcontratante deve prestar assistência ao responsável pelo tratamento:

- (a) Na notificação da violação de dados pessoais à(s) autoridade de controlo competente(s), sem demora injustificada, após o responsável pelo tratamento ter tomado conhecimento da violação, quando pertinente/(salvo se essa violação não for suscetível de constituir um risco para os direitos e para as liberdades das pessoas singulares);
- (b) Na obtenção das informações a seguir enumeradas que, nos termos do artigo 33.º, n.º 3, do Regulamento (UE) 2016/679, devem ser indicadas na notificação do responsável pelo tratamento e têm de incluir, pelo menos:
 - (1) A natureza dos dados pessoais, incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, e as categorias e o número aproximado de registos de dados pessoais em causa;
 - (2) As consequências prováveis da violação de dados pessoais;
 - (3) As medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, incluindo, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

Caso, e na medida em que, não seja possível comunicar todas estas informações ao mesmo tempo, a notificação inicial deve conter as informações então disponíveis, devendo outras informações, à medida que fiquem disponíveis, ser fornecidas posteriormente sem demora injustificada.

- (c) No cumprimento, nos termos do artigo 34.º do Regulamento (UE) 2016/679, da obrigação de comunicar, sem demora injustificada, a violação de dados pessoais ao titular dos dados, caso a violação de dados pessoais seja suscetível de constituir um elevado risco para os direitos e as liberdades das pessoas singulares.

6.2 Violação de dados relativa a dados tratados pelo subcontratante

Em caso de violação de dados pessoais relativa a dados tratados pelo subcontratante, o subcontratante deve notificar o responsável pelo tratamento, sem demora injustificada, após ter tomado conhecimento da violação. Esta notificação deve conter, pelo menos, os seguintes elementos:

- (a) Uma descrição da natureza da violação (incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados e de registos de dados em causa);

- (b) Os dados de um ponto de contacto onde possam ser obtidas mais informações relativas à violação de dados pessoais;
- (c) As consequências prováveis da violação e as medidas adotadas ou propostas para a reparar, incluindo para atenuar os seus eventuais efeitos negativos.

Caso, e na medida em que, não seja possível comunicar todas estas informações ao mesmo tempo, a notificação inicial deve conter as informações então disponíveis, devendo outras informações, à medida que fiquem disponíveis, ser fornecidas posteriormente sem demora injustificada.

As Partes devem estabelecer, no anexo III, todos os outros elementos a fornecer pelo subcontratante aquando da prestação de assistência ao responsável pelo tratamento no cumprimento das obrigações que lhe incumbem por força dos artigos 33.º e 34.º do Regulamento (UE) 2016/679.

SECÇÃO III – DISPOSIÇÕES FINAIS

Cláusula 7

Incumprimento das cláusulas e rescisão

- (a) Sem prejuízo de quaisquer disposições do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725, caso o subcontratante viole as obrigações que lhe incumbem por força das presentes cláusulas, o responsável pelo tratamento pode dar instruções ao subcontratante para suspender o tratamento de dados pessoais até que este último cumpra as presentes cláusulas ou até que o contrato seja rescindido. O subcontratante deve informar imediatamente o responsável pelo tratamento caso, por qualquer motivo, não possa cumprir as presentes cláusulas.
- (b) O responsável pelo tratamento tem o direito de rescindir o contrato, na medida em que este diga respeito ao tratamento de dados pessoais em conformidade com as presentes cláusulas, se:
 - (1) o tratamento de dados pessoais pelo subcontratante tiver sido suspenso pelo responsável pelo tratamento nos termos da alínea a) e o cumprimento das presentes cláusulas não for restabelecido num prazo razoável e, em todo o caso, no prazo de um mês após a suspensão;
 - (2) o subcontratante violar, de forma substancial ou persistente, as presentes cláusulas ou as obrigações que lhe incumbem por força do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725;
 - (3) o subcontratante não cumprir uma decisão vinculativa de um tribunal competente ou da(s) autoridade de controlo competente(s) relativamente às obrigações que lhe incumbem nos termos das presentes cláusulas ou do Regulamento (UE) 2016/679 e/ou do Regulamento (UE) 2018/1725.
- (c) O subcontratante tem o direito de rescindir o contrato, na medida em que este diga respeito ao tratamento de dados pessoais ao abrigo das presentes cláusulas, caso, após ter informado o responsável pelo tratamento de que as suas instruções violam os requisitos legais aplicáveis nos termos da cláusula 4.1, alínea b), o responsável pelo tratamento insista no cumprimento das instruções.
- (d) Na sequência da rescisão do contrato, o subcontratante deve, consoante a escolha do responsável pelo tratamento, apagar todos os dados pessoais tratados por conta deste último e certificar ao responsável pelo tratamento que o fez ou devolver todos os dados pessoais ao responsável pelo tratamento e apagar as cópias existentes, salvo se a conservação dos dados pessoais for exigida ao abrigo do direito da União ou do direito dos Estados-Membros. Até que os dados sejam apagados ou devolvidos, o subcontratante deve continuar a assegurar o cumprimento das presentes cláusulas.

ANEXO I
DESCRIÇÃO DO TRATAMENTO

Atividade de Tratamento: Serviço, Suporte, Consultoria, Administração, Manutenção Remota

- O início do tratamento de dados é: início do contrato de serviço
- A duração planeada do tratamento de dados é: Após a cessação do contrato de serviço

O contexto do tratamento de dados e as obrigações das Partes em relação à relação contratual comercial estão especificados no acordo de serviço entre o Responsável e o Subcontratante.

As categorias dos titulares dos dados, a natureza/finalidade do tratamento, as categorias de dados e quaisquer categorias especiais de dados pessoais dependem do tipo de serviço prestado, dos serviços aos quais os serviços se referem e dos dados pessoais armazenados pelo cliente aos quais a Olympus tem acesso no decorrer da prestação do serviço.

Categorias de titulares de dados	Operações de tratamento	Categorias de dados	Categorias especiais de dados pessoais – se aplicável
☒ Pacientes ☒ Pessoas de contacto ☒ Empregados ☒ Ex-empregados ☒ Fornecedores e seus empregados	☒ Operação e manutenção de sistemas e infraestruturas de TI, por exemplo, sistemas analíticos ☒ Consultoria sobre utilização de produtos ☒ Suporte de TI ☒ Suporte técnico ☒ Administração ☒ Reparação, teste ou manutenção no local ou no centro de reparação da Olympus ☒ Diagnóstico remoto de hardware para produtos de hardware ☒ Teste/manutenção remota de serviços para produtos de software ☒ Fornecimento de dispositivos de empréstimo	☒ Informações de conta ☒ Empresa ☒ Data de nascimento ☒ Consentimento e permissões do dispositivo ☒ ID do dispositivo, Nome do dispositivo ☒ Dados de login do dispositivo ☒ Endereço de e-mail ☒ Género ☒ ID (análise, contrato, dispositivo) ☒ Idioma ☒ Localização ☒ Registos; ☒ Nome ☒ Nome de utilizador ☒ Dados principais do utilizador ☒ Dados de utilização (endereço IP, registo, gravação telefónica) ☒ Dados de utilização de dispositivos, sistemas ☒ Dados de imagem e vídeo	☒ Dados de saúde (por exemplo, nome do paciente, informações médicas)

O trabalho no dispositivo pode exigir a cópia e análise do ficheiro de registo do dispositivo. O ficheiro de registo pode conter nomes de pacientes. O suporte de primeiro e segundo nível é fornecido dentro da UE. O suporte de terceiro nível é fornecido por uma entidade da Olympus sediada nos EUA ("Olympus Surgical Technologies America"). Portanto, se for necessário suporte de terceiro nível para resolução de problemas, pode ser necessário transferir dados para os Estados Unidos. Para garantir

um nível adequado de proteção, a Olympus celebrou acordos internos apropriados de tratamento de dados (DPAs) com as suas entidades afiliadas nos EUA.

ANEXO II

MEDIDAS TÉCNICAS E ORGANIZACIONAIS, INCLUINDO MEDIDAS TÉCNICAS E ORGANIZACIONAIS PARA GARANTIR A SEGURANÇA DOS DADOS

Tendo em conta o estado da arte, os custos de implementação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, o Subcontrante implementará as seguintes medidas técnicas e organizacionais:

MEDIDA	DESCRIÇÃO
1. CONFIDENCIALIDADE	
a) Controlo de acesso – Localizações da Olympus	Os edifícios da Olympus estão fechados e guardados em toda a sua extensão. Os empregados só podem entrar nos edifícios utilizando o seu cartão de identificação pessoal. Os visitantes só podem entrar nos edifícios através da receção e acompanhados por funcionários. O acesso aos edifícios é negado a pessoas não autorizadas. As seguintes medidas de segurança são implementadas: - Crachás de empregado/visitante - Sistema de controlo de acesso, leitor de cartões, transponder, cartões magnéticos ou com chip - Receção/rececionista/porteiro - Chaves/atribuição de chaves (controladas) - Fechadura de porta (abertura elétrica, portas com maçaneta exterior, etc.) - Segurança da fábrica, porteiro - Sistema de vigilância, sistema de alarme, monitor de vídeo/TV
b) Controlo de acesso – sistemas	Todos os sistemas estão instalados em centros de dados seguros e protegidos por cartões de identificação pessoal em combinação com PIN. As seguintes medidas de segurança são implementadas: - Procedimento de palavra-passe segura (incluindo caracteres especiais, comprimento mínimo, alterações regulares de palavra-passe) - Mecanismos de bloqueio automático (por exemplo, palavra-passe ou interruptor de pausa, bloqueio automático do ambiente de trabalho) - Instrução para bloqueio manual do ambiente de trabalho - Configuração e gestão de um perfil de utilizador e registo principal - Firewall, software antivírus para servidores e clientes - Utilização de VPN para acesso remoto

	- Política de Dispositivos Móveis
c) Controlo de acesso - gestão de direitos: autoridade de leitura e edição Sistemas internos de TI da Olympus	Está em vigor uma gestão sistemática de direitos para a utilização dos sistemas de TI. O acesso aos sistemas só é possível com nomes de utilizador e palavras-passe. As autorizações diferem entre permissões de leitura e escrita. As seguintes medidas de segurança são implementadas: - Conceito de autorização diferenciado e direitos de acesso baseados na necessidade de saber (perfis, funções, transações e objetos)
d) Controlo de separação Sistemas internos de TI da Olympus	A manutenção remota é realizada separadamente para cada cliente. As seguintes medidas de segurança são implementadas: - Capacidade multi-cliente das aplicações relevantes - Afetação - Separação funcional do ambiente produtivo e de teste - Separação física de sistemas, bases de dados e suportes de dados - Definição de direitos de base de dados
e) Encriptação	É preferida a encriptação da comunicação. O método de encriptação é o estado da arte.
2. INTEGRIDADE	
a) Controlo de transferência Sistemas internos de TI da Olympus	As seguintes medidas de segurança são implementadas: - A encriptação de e-mails é possível na rede - Nenhuma leitura, cópia, modificação ou remoção não autorizada dentro do sistema - Utilização de VPN, bem como fornecimento através de conexões encriptadas, como sftp, https
b) Controlo de entrada	As alterações nos sistemas são registadas. As seguintes medidas de segurança são implementadas: - Registo de acessos - Sistemas de avaliação de registos e rastreabilidade de entrada, modificação e eliminação de dados por nomes de utilizador individuais - Atribuição de direitos através de contas de utilizador personalizadas - Gestão de documentos
3. DISPONIBILIDADE E RESILIÊNCIA	

a) Controlo de disponibilidade; medidas de proteção de dados Sistemas internos de TI da Olympus	Os dados pessoais estão protegidos. Será garantida a proteção contra destruição ou perda acidental ou intencional, bem como o controlo da disponibilidade dos dados. As seguintes medidas de segurança são implementadas: - Procedimento de backup: descrição do ritmo e meio do backup, tempo de armazenamento e localização do backup (online/offline, no local/fora do local) - Espelhamento de discos rígidos, por exemplo, procedimento RAID - Fonte de alimentação ininterrupta (UPS) - Armazenamento ou partição separada para sistemas operativos e dados - Proteção contra vírus e firewall - Canais de reporte e planos de emergência - Extintores e sistemas de alarme nos edifícios, em particular na sala de servidores, onde a temperatura/humidade também é monitorizada, e estão instaladas réguas de tomadas protegidas
b) Recuperação rápida	A recuperação de dados é da responsabilidade do Controlador.
4. PROCEDIMENTOS PARA REVISÃO, AVALIAÇÃO E AVALIAÇÃO REGULARES	
a) Controlo de encomendas Sistemas internos de TI da Olympus	A eficácia das medidas tomadas é regularmente revista. O controlo de encomendas é verificado de forma aleatória. As seguintes medidas de segurança são implementadas: - Design claro de contrato - Formalização da colocação de encomendas - Seleção do contratante sob aspetos de diligência devida (no que diz respeito à proteção e segurança de dados) - Conclusão do acordo necessário para acordo de encomenda ou cláusulas contratuais padrão da UE - Instruções por escrito ou em forma de texto para o contratante - Obrigação dos funcionários do contratante de manter o sigilo dos dados - Obrigação de nomear um encarregado de proteção de dados pelo contratante, caso exista a obrigação de nomeação - Acordo sobre direitos de controlo eficazes em relação ao contratante

	- Regulamentação sobre o uso de subcontratantes adicionais - Garantia da destruição dos dados após a conclusão da encomenda - Verificação contínua do contratante e do seu nível de proteção
b) Gestão de privacidade e resposta a incidentes	- Documentação central de todos os procedimentos e regulamentos de proteção de dados com acesso para os funcionários conforme necessário/autorizado - Encarregado interno de segurança da informação e proteção de dados - Formação regular dos funcionários e compromisso com a confidencialidade/privacidade - Processo documentado para reconhecimento e reporte de incidentes de segurança/quebras de dados (também em relação à notificação obrigatória às autoridades de supervisão) - Procedimento documentado para lidar com incidentes de segurança e quebras de dados - Avaliação formalizada de impacto na privacidade e processo para lidar com pedidos de informação de titulares de dados

ANEXO III
LISTA DE SUBCONTRATANTES ULTERIORES

O controlador autorizou o uso dos seguintes subcontratantes ulteriores:

Nome e Endereço	Nome, posição e detalhes de contacto da pessoa de contacto	Descrição do Tratamentoo	Se aplicável, salvaguardas para transferências para países terceiros
Olympus Europa SE & Co. KG Wendenstraße 20 20097 Hamburgo Alemanha	Stefan Limbacher Encarregado de Proteção de Dados EMEA privacy@olympus.com	Suporte de 2º nível para reparação, manutenção e manutenção remota de software e dispositivos médicos	n/a, Subcontratantes Ulteriores localizados em Hamburgo, Alemanha
Olympus Surgical Technologies Europe Olympus Winter & Ibe GmbH Kuehnstraße 61 22045 Hamburgo Alemanha	privacy@olympus.com	Suporte de 3º nível para reparação, manutenção e manutenção remota de software e dispositivos médicos	n/a, Subcontratantes Ulteriores localizados em Hamburgo, Alemanha
Olympus Medical Systems Corporation 2951 Ishikawa-machi, Hachioji-shi Tóquio 192-8507 Japão	privacy@olympus.com	Gestão de reclamações, incluindo investigação de avarias e erros inesperados.	Decisão de Adequação (UE) 2019/419 pela Comissão Europeia
Olympus Surgical Technologies America 800 W Park Dr. Westborough, MA 01581 EUA	privacy@olympus.com	Gestão de reclamações, incluindo investigação de avarias e erros inesperados.	Cláusulas Contratuais Tipo

Tata Consultancy Services GmbH Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Alemanha	privacy@olympus.com	Fornecedor de infraestrutura e serviços de TI	n/a, Subcontratantes Ulteriores localizados em Frankfurt, Alemanha
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Alemanha	privacy@teamviewer.com	Monitorização e controlo de computadores	n/a, Subcontratantes Ulteriores localizados em Göppingen, Alemanha
ImageStreamMedical One Monarch Drive Littleton, MA 01460 EUA	privacy@cision.com	Suporte de 3º nível para reparação, manutenção e manutenção remota de software	Cláusulas Contratuais Tipo
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521 Irlanda	privacy@microsoft.com	Vários serviços de Cloud	n/a, Subcontratantes Ulteriores localizados na Irlanda
RealVNC Limited 50-60 Station Road Cambridge Cambridgeshire CB1 2JH Reino Unido da Grã-Bretanha e Irlanda do Norte	privacy@realvnc.com	Fornecedor de software de controlo remoto para SPiN Planning Laptop Workstation – Sem armazenamento de dados, apenas partilha de ecrã encriptada	Decisão de adequação para o Reino Unido