Adendo de Processamento de Dados

Este Adendo sobre Processamento de Dados (doravante: "**Adendo**") é acordado por e entre: Cliente

e suas Afiliadas conforme definido pela SOW:

– doravante denominado "**Cliente**" -

e

Entidade da Datasite conforme definido pela SOW:

– doravante denominada "**Datasite**" –

Cada um individualmente referido também como a "**Parte**" e coletivamente como as "**Partes.**"

Preâmbulo:

(A) As Partes firmaram um Contrato que descreve os Serviços a serem fornecidos (definições fornecidas na Seção 1 abaixo). Como parte da prestação de Serviços pela Datasite, os Dados Pessoais podem ser transferidos pelo Cliente para a Datasite.

(B) Os termos em maiúsculas não definidos neste Adendo são definidos no Contrato. No caso de qualquer conflito entre as disposições deste Adendo e as disposições estabelecidas no Contrato, a disposição ou disposições deste Adendo prevalecerão.

(C) Para garantir o cumprimento pelas Partes das obrigações de Processamento de acordo com as Regras de Proteção de Dados, conforme alteradas de tempos em tempos, as Partes concordam com o seguinte:

1. Definições

1.2 "**Apêndice**" significa os apêndices anexos e que fazem parte integrante deste Adendo.

1.3 "**Categorias Especiais de Dados**" significa os Dados Pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos Processados com o objetivo de identificar exclusivamente uma pessoa física, bem como Dados Pessoais relativos à saúde, vida sexual ou orientação sexual, ou conforme definido nas Regras de Proteção de Dados aplicáveis.

1.4 "**Cláusulas Contratuais Padrão**" ou "**SCCs**" significa as cláusulas contratuais padrão de Controlador para Processador (Módulo 2) para a transferência de Dados Pessoais a entidades não sujeitas ao GDPR/Lei Suíça de Proteção de Dados, de acordo com os requisitos do GDPR e da Lei Suíça de Proteção de Dados, conforme aplicável.

1.5 "**Contrato**" significa a Declaração de Serviço e os Termos e Condições Gerais aplicáveis entre o Cliente e a Datasite.

1.6 "**Contrato Internacional de Transferência de Dados**" ou "**IDTA**" significa o contrato internacional de transferência de dados para a transferência de Dados Pessoais para processadores estabelecidos em países terceiros de acordo com o Artigo 46 e Capítulo V da GDPR do Reino Unido.

1.7 "**Controlador**" significa uma entidade que determina as finalidades e os meios do Processamento de Dados Pessoais.

1.8 "**Dados Pessoais**" significa qualquer informação relativa a um Titular dos Dados contidos no Conteúdo.

1.9 "**GDPR**" significa a GDPR do Reino Unido e o Regulamento Geral de Proteção de Dados da UE 2016/679.

1.10 **"GDPR do Reino Unido"** significa s.3(10), 205(4) e as disposições gerais de processamento da Lei de Proteção de Dados de 2018, conforme atualizadas, alteradas, ou substituídas de tempos em tempos.

1.11 "**Lei Suíça de Proteção de Dados**" significa a Lei Federal Suíça de Proteção de Dados de 19 de junho de 1992 (SR 235.1) e as Portarias SR 235.11 e SR 235.13, conforme alteradas e após a entrada em vigor de sua versão revisada de 25 de setembro de 2020 em 1 de janeiro de 2023 (ou em data posterior sujeita ao procedimento legislativo), sujeito a tal versão revisada, conforme alterada, ou substituída de tempos em tempos, na medida em que se apliquem ao Processamento de Dados Pessoais.

1.12 "**Leis de Proteção de Dados dos EUA**" significa as seguintes leis na medida aplicável aos Dados Pessoais e à prestação dos Serviços assim que entrarem em vigor: a Lei de Privacidade do Consumidor da Califórnia (e a Lei de Direitos de Privacidade da Califórnia uma vez em vigor), Código Civil da Califórnia § 1798.100 *et seq.*; e outras leis dos EUA materialmente semelhantes que possam ser promulgadas e que se apliquem aos Dados Pessoais de tempos em

tempos.

1.13 "**Leis Europeias de Proteção de Dados**" significa a GDPR e a Lei Suíça de Proteção de Dados coletivamente.

1.14 "**Operações Comerciais**" significa: (1) faturamento, pagamentos e gerenciamento de contas; (2) para fins de marketing direto; (3) relatórios internos e modelagem de negócios (por exemplo, previsão, receita, planejamento de capacidade, estratégia de produto); (4) melhorar e desenvolver novos produtos e serviços; (5) combater fraudes, crimes cibernéticos ou ataques cibernéticos que possam afetar a Datasite ou os produtos da Datasite; (6) melhorar a funcionalidade principal de acessibilidade ou privacidade do Website; e (7) relatórios financeiros e cumprimento das obrigações legais.

1.15 **"Processador"** significa uma entidade que processa Dados Pessoais em nome de um Controlador.

1.16 "**Processo**", "**Processamento**" ou "**Processado**" significa qualquer operação ou conjunto de operações que seja realizada sobre Dados Pessoais, seja por meios automáticos ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização de outra forma, alinhamento ou combinação, bloqueio, supressão ou destruição, ou conforme definido nas Regras de Proteção de Dados aplicáveis.

1.17 "**Regras de Proteção de Dados**" significa as leis nacionais relevantes que se aplicam ao Processamento de Dados Pessoais, incluindo, mas não se limitando a: Leis Europeias de Proteção de Dados, Leis de Proteção de Dados dos EUA e Princípios de Privacidade Australianos, conforme aplicável.

1.18 "**Serviços**" significa a prestação de serviços conforme descrito no Contrato e neste Adendo.

1.19 "**Subprocessador**" significa uma entidade contratada por um Processador para Processar Dados Pessoais em nome de um Controlador.

1.20 "**Titular dos Dados**" significa uma pessoa física identificada ou identificável cujos Dados Pessoais estão sujeitos a Processamento; uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos de identidade física, fisiológica, genética, mental, econômica, cultural ou social, ou conforme definido nas Regras de Proteção de Dados aplicáveis.

1.21 "**Violação de Dados Pessoais**" significa uma violação de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada de, ou acesso a Dados Pessoais transmitidos, armazenados ou processados de outra forma, ou conforme definido de outra forma nas Regras de Proteção de Dados aplicáveis.

2. Atividades de Processamento

2.1. O Cliente e a Datasite concordam que: (a) o Cliente é o Controlador de Dados Pessoais e a Datasite é a Processadora de tais dados, exceto quando o Cliente atua como Processador de Dados Pessoais em nome de um Controlador terceirizado ("Controlador Terceirizado"), hipótese em que a Datasite será um Subprocessador; e (b) este Adendo se aplica onde e somente na medida em que Processe Dados Pessoais em nome do Cliente como Processador ou Subprocessador durante a prestação dos Serviços.

2.2. O Cliente concorda que: (a) obteve todos os consentimentos relevantes ou garantiu que tem outra base legal válida (conforme aplicável), permissões e direitos e forneceu todos os avisos relevantes necessários sob as Regras de Proteção de Dados para a Datasite processar legalmente Dados Pessoais de acordo com este Contrato incluindo, sem limitação, o compartilhamento e/ou recebimento de Dados Pessoais do Cliente com terceiros por meio dos Serviços; (b) deve cumprir e é responsável pelo cumprimento de suas Afiliadas e Usuários convidados com as Regras de Proteção de Dados aplicáveis; e (c) suas instruções de Processamento para a Datasite são consistentes com as Regras de Proteção de Dados e todas as instruções de Controladores Terceiros, quando aplicável.

2.3. A Datasite concorda em Processar os Dados Pessoais de acordo com: (a) este Adendo e o Contrato; (b) instruções escritas do Cliente conforme estabelecido no Apêndice 1 deste Adendo; e (c) eventual comunicado pelo Cliente de tempos em tempos, caso exigido pelas Regras de Proteção de Dados. Quaisquer instruções adicionais solicitadas requerem o acordo prévio por escrito da Datasite.

2.4. Na medida em que o Feedback, Dados de Uso ou Dados do Usuário (coletivamente para fins deste parágrafo apenas, "**Dados**") estejam relacionados a uma pessoa identificada ou identificável, as Partes concordam que a Datasite: (a) atuará como um "controlador" e /ou "negócio" independente (tais como definidos nas Regras de Proteção de Dados) com relação a esses Dados; e (b) processará tais Dados apenas para suas Operações Comerciais e em conformidade com todas as Regras de Proteção de Dados aplicáveis. O Cliente concorda que obteve todos os consentimentos, permissões e direitos relevantes e forneceu todos os avisos relevantes necessários sob as Regras de Proteção de Dados para que a Datasite processe legalmente os Dados como um "controlador" e/ou "negócio"

independente (tais como definidos nas Regras de Proteção de Dados) para as Operações Comerciais da Datasite.

2.5 Se a Datasite acreditar que uma instrução infringe as Regras de Proteção de Dados, notificará o Cliente sem demora injustificada. Quando o Cliente estiver atuando como Processador, ele será responsável por qualquer notificação, assistência ou autorização que possa ser solicitada ou recebida por seu Controlador Terceirizado. A Datasite reconhece que, ao atuar como Provedor de Serviços, não recebe quaisquer Dados Pessoais como contraprestação pelos Serviços (tais como definidos nas Leis de Proteção de Dados dos EUA).

3. Duração e Término deste Adendo

3.1. Este Adendo entra em vigor a partir da Data Efetiva e permanecerá em vigor durante a vigência do Contrato. Este Adendo terminará automaticamente com a rescisão ou decurso de prazo de qualquer SOW.

3.2. Não obstante o término deste Adendo, a Datasite continuará vinculado à sua obrigação de confidencialidade.

4. Transferências Internacionais

Todos os Dados Pessoais são armazenados em instalações de hospedagem de terceiros dentro dos Estados Unidos, Espaço Econômico Europeu ("EEA") ou Austrália. Cliente reconhece que a Datasite pode transferir Dados Pessoais para países nos quais ela e ou seus Subprocessadores operam; entretanto, os Dados Pessoais continuarão a ser armazenados nos Estados Unidos, EEA ou Austrália. A menos que transferidas com base em uma decisão de adequação emitida pela autoridade nacional aplicável, todas as transferências de Dados Pessoais para fora do Reino Unido, EEA e Suíça serão regidas pelas SCCs (como Apêndice 3) e IDTA (como Apêndice 4) incorporado a este Adendo. A Datasite cumprirá as exigências das Regras de Proteção de Dados da EEA, Reino Unido e Suíça relativas à coleta, uso, transferência, retenção e outros processamentos de Dados Pessoais da EEA, Reino Unido e Suíça.

5. Confidencialidade e Segurança

5.1. A Datasite deverá: (a) manter os Dados Pessoais confidenciais; e (b) garantir que seus funcionários que Processam Dados Pessoais se comprometeram com a confidencialidade ou estão sob uma obrigação estatutária apropriada de confidencialidade.

5.2. Sujeito às Regras de Proteção de Dados, a Datasite implementará medidas operacionais, técnicas e organizacionais apropriadas para proteger os Dados Pessoais contra destruição, perda, alteração, divulgação não autorizada ou acesso acidental ou ilegal, conforme descrito no Apêndice 2.

5.3. O Cliente é o único responsável por determinar de forma independente se as medidas técnicas e organizacionais implementadas pela Datasite atendem aos requisitos do Cliente, incluindo qualquer uma de suas obrigações de segurança sob as Regras de Proteção de Dados aplicáveis. O Cliente reconhece e concorda que (levando em consideração o estado da arte, os custos de implementação e a natureza, escopo, contexto e propósitos do Processamento de seus Dados Pessoais, bem como os riscos para os Titulares dos Dados) as práticas e políticas de segurança implementadas e mantidas pela Datasite fornecem um nível de segurança adequado ao risco em relação aos Dados Pessoais.

5.4. A Datasite atualizará as medidas de segurança técnicas e organizacionais de acordo com os desenvolvimentos tecnológicos razoáveis, conforme determinado pela Datasite.

6. Obrigações de Cooperação e Notificação

6.1. As Partes cooperarão umas com as outras para lidar de forma rápida e eficaz com consultas, reclamações e requisições relacionadas ao Processamento de Dados Pessoais de qualquer autoridade governamental ou Titular dos Dados.

6.2. Se um Titular dos Dados solicitar o exercício de seus direitos de Dados Pessoais diretamente à Datasite, a Datasite atenderá ao Cliente com tal solicitação, encaminhando-a ao Cliente sem atraso indevido, se permitido pelas Regras de Proteção de Dados.

6.3. A menos que proibido por lei, se os Dados Pessoais estiverem sujeitos a controle, ordem ou investigação por autoridades públicas, a Datasite irá: (a) notificar imediatamente o Cliente; e (b) divulgar Dados Pessoais apenas na medida estritamente necessária e proporcional para satisfazer o pedido e em conformidade com as Regras de Proteção de Dados. Ao pedido do Cliente, a Datasite fornecerá às autoridades públicas informações sobre o Processamento sob este Adendo, bem como permitir inspeções dentro do escopo estabelecido na Seção 7, conforme exigido pelas Regras de Proteção de Dados.

6.4. A Datasite notificará o Cliente, sem indevido atraso, sobre Violação de Dados Pessoais que possam afetar os Dados Pessoais do Cliente. A Datasite deve fornecer ao Cliente as informações para auxiliar o Cliente de forma razoável conforme exigido pelas Regras de Proteção de Dados.

6.5. Considerando a natureza do Processamento e dos Dados Pessoais, a Datasite fornecerá assistência razoável ao Cliente na realização de uma avaliação de impacto de proteção de dados e consulta prévia sob as Regras de Proteção de

Dados, na medida em que o Cliente não seja capaz de realizá-las de forma independente.

7. Direitos de Auditoria e Inspeção do Cliente

Diante de pedido do Cliente, e sujeito a prazo razoável, tempo, local, frequência e restrições de forma e requisitos de confidencialidade, a Datasite disponibilizará as informações do Cliente necessárias para demonstrar o cumprimento das obrigações da Datasite sob o Adendo e as Regras de Proteção de Dados aplicáveis. A Datasite permitirá e contribuirá para auditorias, incluindo inspeções, realizadas pelo Cliente, ou um auditor terceirizado independente indicado pelo Cliente. Na medida em que os direitos do Cliente sob esta seção não possam ser razoavelmente satisfeitos por meio de relatórios de auditoria, documentação ou informações de conformidade que a Datasite disponibiliza para seus clientes, o Cliente será responsável por todos os custos e taxas relacionados a tal auditoria.

8. Uso de Subprocessadores

8.1 O Cliente reconhece e fornece autorização geral para a Datasite para usar Subprocessadores para Processar Dados Pessoais. A lista atual dos Subprocessadores da Datasite está disponível nohttps://www.datasite.com/us/en/legal/sub- processors.html. A Datasite deve: (a) garantir que quaisquer Subprocessadores Processem Dados Pessoais apenas para entregar os Serviços que a Datasite os reteve para fornecer; (b) impor a quaisquer Subprocessadores obrigações contratuais relacionadas a Dados Pessoais não menos protetivas do que este Adendo; e (c) ser responsável pelo cumprimento de tais obrigações por parte de cada Subprocessador.

8.2 A Datasite disponibilizará em seu site de Subprocessadores um mecanismo para que os Clientes assinem notificações de novos Subprocessadores, fornecendo um endereço de e-mail. Se a Datasite pretender nomear ou substituir um Subprocessador coberto por este Adendo, pelo menos sessenta (60) dias antes de permitir que o novo Subprocessador Processe Dados Pessoais, a Datasite deverá: (a) atualizar seu site de Subprocessadores; (b) fornecer notificação aos e-mails que se inscreveram; e (c) em relação a (a) e (b), dar ao Cliente a oportunidade de se opor a tais alterações por motivos razoáveis relacionados à proteção de dados. Se as Partes não conseguirem chegar a uma resolução, o Cliente, como seu único e exclusivo recurso, poderá fornecer uma notificação por escrito à Datasite rescindindo a(s) SOW(s).

9. Devolução e exclusão de dados pessoais

Mediante solicitação do Cliente ou após o término deste Adendo, a Datasite devolverá (de acordo com a SOW) ou destruirá todos os Dados Pessoais e suas cópias, a menos que as Regras de Proteção de Dados aplicáveis ou outra obrigação legal exijam que a Datasite retenha os Dados Pessoais por mais tempo. Mediante solicitação do Cliente, a Datasite certificará que isso foi feito.

10. Responsabilidade

Sem prejuízo dos direitos ou recursos disponíveis aos Titulares de Dados sob as Regras de Proteção de Dados, a responsabilidade das Partes e sua limitação, incluindo qualquer reclamação apresentada por uma Afiliada, estará de acordo com o Contrato.

Cliente:	**Datasite:**
Por:_____	Por:_____
Nome: _____	Nome: _____
Cargo:_____	Cargo:_____
Data:_____	Data:_____

Apêndice 1: Dados Pessoais Processados e Finalidades

Os Dados Pessoais são transferidos e processados para as **seguintes finalidades**:

- Repositório *online* seguro e compartilhamento de dados para transações corporativas ou fins comerciais internos.

Objeto e Natureza do Processamento:

- Conforme descrito no Contrato, a Datasite fornece ferramentas seguras de repositório *online* para armazenamento, gerenciamento, colaboração e distribuição de dados e documentos.

Categorias de Dados Pessoais:

Os tipos de Dados Pessoais são determinados e controlados pelo Cliente a seu exclusivo critério e podem incluir, mas não estão limitados a:

- Nomes, endereço, endereço de e-mail da empresa, telefone da empresa, remuneração e benefícios, informações sobre férias e pensões, cargos e funções, e potencialmente outros tipos de Dados Pessoais carregados pelo Administrador do Cliente no Website.

Categorias Especiais de Dados (se aplicável):

Sujeito a qualquer condição aplicável no Contrato, os tipos de Categorias Especiais de Dados são determinados e controlados pelo Cliente a seu exclusivo critério e podem incluir, mas não estão limitados a:

- Nenhum, a menos que identificado de outra forma pelo Cliente

Titulares dos Dados:

As categorias de Titulares de Dados aos quais os Dados Pessoais se relacionam são determinadas e controladas pelo Cliente a seu exclusivo critério e podem incluir, mas não se limitam a:

- Informações comerciais sobre proprietários, funcionários, agentes, clientes, consultores, parceiros de negócios, contratados e fornecedores atuais, passados e potenciais.

Retenção:

- Todos os Dados Pessoais são permanentemente apagados após: (a) o Administrador do Cliente fechar o projeto aplicável no Website; ou (b) término do Contrato entre Cliente e Datasite.

Apêndice 2

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

	Requisito de segurança	Como a Datasite implementa a medida específica de segurança da informação
1.	*Medidas para criptografia de dados pessoais*	Os Dados Pessoais são criptografados em repouso e em trânsito usando tecnologias de criptografia padrão do setor, atualmente em repouso usando criptografia AES de 256 bits e em trânsito via protocolo Transport Layer Security (TLS) 1.2, que será atualizado periodicamente de acordo com desenvolvimentos tecnológicos razoáveis conforme determinado pela Datasite.
2.	*Medidas para garantir Confidencialidade, integridade, disponibilidade e resiliência contínuas de sistemas e serviços de processamento*	A Datasite é certificada pela ISO 27001, ISO 27701, ISO 27017, ISO 27018, Tipo SOC 2 II em conformidade, garantindo que mantém e aplica apropriadas salvaguardas administrativas, físicas e técnicas para proteger a integridade, disponibilidade e confidencialidade dos Dados Pessoais do Cliente.
3.	*Medidas para garantir a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais em tempo hábil em caso de incidente físico ou técnico*	A Datasite possui redundância com cada plataforma e mantém logs de disponibilidade do sistema. Além disso, a redundância permite backups contínuos do sistema. A Datasite possui Planos de Recuperação de Desastres e Continuidade de Negócios que são revisados, atualizados e testados periodicamente.
4.	*Processos para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento*	A Datasite conclui revisões regulares de código, testes de vulnerabilidade e testes de penetração anuais no Website.
5.	*Medidas para identificação e autorização do usuário*	O acesso é regido pelo gerenciamento padrão de acesso da Datasite que segue baseado em controle de funções. O acesso aos Dados Pessoais é fornecendo apenas aos funcionários estritamente necessários para o único propósito de satisfazer as instruções do Cliente. O padrão de gerenciamento de acesso requer que (a) os direitos de acesso sejam revistos, atualizado e aprovado pela administração regularmente, e (2) direitos de acesso sejam retirados no prazo de 24 horas após o desligamento do funcionário. Outros tipos de controles relevantes são requisitos de senha, autenticação multifator e restrição de mídia removível que são implementados no nível corporativo.
6.	*Medidas para a proteção de dados durante a transmissão*	Os Dados Pessoais são criptografados em trânsito usando tecnologias de criptografia padrão do setor, atualmente via protocolo Transport Layer Security (TLS) 1.2, que deve ser atualizado periodicamente de acordo com desenvolvimentos tecnológicos razoáveis, conforme determinado pela Datasite.
7.	*Medidas para a proteção de dados durante o armazenamento*	Os Dados Pessoais são criptografados em repouso usando tecnologias de criptografia padrão do setor, atualmente criptografia AES de 256 bits, que deve ser atualizada periodicamente de acordo com desenvolvimentos tecnológicos razoáveis, conforme determinado pela Datasite.

8.	*Medidas para garantir a segurança física dos locais em que os dados pessoais são processados*	A Datasite utiliza provedores de serviço na nuvem para seus requisitos de armazenamento de dados. Informações sobre os protocolos de segurança física do Microsoft Azure, das suas localizações de servidores estão disponíveis em: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security. Todos os data centers mantêm ISO 27001:2013 e Certificações SOC 2 Tipo 2. Com respeito às instalações da Datasite, todos os escritórios exigem acesso por crachá e utilizam vigilância recém-atualizada por vídeo usando câmeras com gravações armazenadas na nuvem.
9.	*Medidas para garantir o registro de eventos*	A Datasite realiza registro e monitoramento que são coletados e normalizados centralmente em sua ferramenta SIEM. Os logs são retidos por 180 dias e o acesso é baseado em funções e responsabilidades.
10.	*Medidas para garantir a configuração do sistema, incluindo a configuração padrão*	A Datasite possui processos de construção padrão e aplica os padrões de proteção CIS.
11.	*Medidas para governança e gerenciamento interno de TI e segurança de TI*	A Datasite mantém um sistema robusto de gerenciamento de segurança da informação regido pelo Comitê Datasite PIMS que é responsável por implementar e manter um ambiente estável e seguro.
12.	*Medidas para certificação/garantia de processos e produtos*	A Datasite mantém uma certificação SOC II Tipo II e uma certificação ISO 27001 desde 2007, ISO 27017 e ISO 27018 desde 2021, e ISO 27701 desde 2023.
13.	*Medidas para garantir a minimização de dados*	Dados Pessoais recolhidos e processados não serão mantidos ou usados a menos que necessários para fornecer os Serviços em conformidade com o Contrato de Serviço e as políticas e Aviso de Privacidade da Datasite.
14.	*Medidas para garantir a qualidade dos dados*	A Datasite utiliza um cliente anti-malware ligado a todos os sistemas. Dados Pessoais carregados para o Website são verificados pelo anti-malware da Datasite como parte das atividades de processamento de documentos que ocorrem dentro da plataforma.
15.	*Medidas para garantir a retenção de dados limitada*	Os Dados Pessoais são eliminados a partir de 30 dias após o encerramento do projeto ou após o término do Contrato de Serviço.
16.	*Medidas para garantir a prestação de contas*	Todas as atividades registradas são rastreadas e reportáveis. O Pessoal conclui o treinamento e reconhece a conformidade com o código de conduta e as políticas da Datasite anualmente. Todo o Pessoal é obrigado a assinar um NDA. O Código de Conduta é confirmado por todo o Pessoal em uma base anual.
17.	*Medidas para permitir a portabilidade de dados e garantir o apagamento*	O Cliente hospeda Dados Pessoais em servidores conforme definido no Contrato de Serviço que podem ser transferidos para outros locais em que a Datasite mantém servidores, mediante solicitação. Os Dados Pessoais podem ser devolvidos aos Clientes via dispositivo USB criptografado, se solicitado. A exclusão de Dados Pessoais ocorre 30 dias após o encerramento do projeto ou término do Contrato de Serviço.

18.	*Para transferências para (sub) processadores, descreva também as medidas técnicas e organizacionais específicas a serem tomadas pelo (sub) processador para poder prestar assistência ao controlador e, para transferências de um processador para um subprocessador, para o exportador de dados*	A Datasite mantém um Padrão de Segurança do Fornecedor que detalha os padrões mínimos de segurança do fornecedor necessários para armazenar, processar ou transmitir Dados Pessoais que fornecem uma linha de base das expectativas de controle para a avaliação de cada fornecedor, conformidade e aceitação de risco com base na natureza do relacionamento com o fornecedor. Cada fornecedor no escopo é obrigado a assinar contratos (DPA SCCs) que garantem o mesmo nível ou proteção à Datasite do que as obrigações da Datasite ao Cliente.

Appendix 3: Standard Contractual Clauses

For the purposes of applicable Data Protection Laws for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Customer as defined by the SOW, unless otherwise identified in Annex 1.A:

("**the data exporter**")

And

Name of the data importing organisation: Datasite LLC and its in-scope affiliates described in Annex 1.A

(collectively "**the data importer"**) each

a "party"; together "the parties",

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Data Exporter and Data Importer have agreed to these standard contractual clauses ("Clauses")

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f)

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the

transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Appendix 1.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing and signing Appendix 1.A.

(b) Once it has completed and signed Appendix 1.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Appendix 1.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix 1.B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal

data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 Use of sub-processors

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [3]The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual r esidence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

---

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex 1.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the

following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more

than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Anexo 1

A. LISTA DAS PARTES

Exportador de Dados:

Nome: Cliente conforme definido pela SOW, a menos que identificado de outra forma neste documento:

Endereço:

Nome da pessoa de contato, cargo e detalhes de contato:

Atividades relevantes para os dados transferidos sob estas Cláusulas: O Exportador de Dados usa ferramentas eletrônicas on-line seguras de repositório baseadas em SaaS ("Website") para armazenar, gerenciar, colaborar e distribuir dados e documentos ("**Conteúdo**") de acordo com um contrato de serviço entre Exportador de Dados e Importador de Dados ("Contrato de Serviço") (os "**Serviços**"). O Importador de Dados armazena o Conteúdo em servidores de terceiros na UE, EUA e Austrália para fornecer o Website ao Exportador de Dados e hospedar o seu Conteúdo, que embora não seja avaliado por sua substância, pode conter Dados Pessoais. O Conteúdo do Website permanece armazenado nesses servidores, mas pode ser acessado pelos funcionários do Importador de Dados com a finalidade de fornecer os Serviços conforme descrito em mais detalhes no Apêndice 1.

Função: Controlador

Importador de dados:

Nome: Datasite LLC, uma sociedade de responsabilidade limitada registrada em Delaware, EUA, e suas afiliadas dentro do escopo.

Endereço: 733 S. Marquette Ave, Suite 600 Minneapolis, MN 55402

Nome da pessoa de contato, cargo e detalhes de contato: Patricia Elias, Diretora, Secretária e Oficial de Proteção de Dados, patricia.elias@datasite.com, 651 632 4042

Atividades relevantes para os dados transferidos sob estas Cláusulas:

O Importador de Dados fornece o Website ao Exportador de Dados para hospedar o Conteúdo dos Exportadores de Dados em servidores de terceiros na UE, nos EUA ou na Austrália. O Conteúdo, embora não seja avaliado por sua substância, pode conter Dados Pessoais. O Conteúdo permanece armazenado nesses servidores, mas pode ser acessado pelos funcionários dos Importadores de Dados com a finalidade de fornecer os Serviços conforme descrito no Apêndice 1.

Função: Processador

B. DESCRIÇÃO DA TRANSFERÊNCIA

Consulte o Apêndice 1 do DPA

C. AUTORIDADE DE SUPERVISÃO COMPETENTE

- ***Comissário Federal da Alemanha para Proteção de Dados e Liberdade de Informação***

Anexo 2

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

Consulte o Apêndice 2 do DPA

APÊNDICE 4

ADENDO A TRANSFERÊNCIA INTERNACIONAL DE DADOS ÀS CLÁUSULAS CONTRATUAIS PADRÃO DA COMISSÃO DA UE

Este Adendo foi emitido pelo Comissário de Informações para Partes que fazem Transferências Restritas. O Comissário de Informação considera que fornece Salvaguardas Apropriadas para Transferências Restritas quando um contrato juridicamente vinculativo é celebrado.

Parte 1: Tabelas

Tabela 1: PARTES E ASSINATURA

Cliente conforme definido pela SOW, a menos que identificado de outra forma neste documento:

A execução do Contrato de Processamento de Dados ("DPA"), no qual este Adendo está anexado, é considerada a execução deste Adendo do Reino Unido

*a seguir o '**Exportador**;' e*

Datasite LLC, uma sociedade de responsabilidade limitada registrada em Delaware, EUA, e incluindo suas Afiliadas

Contato Principal: Patricia Elias, Diretora, Secretária e Diretora de Proteção de Dados, patricia.elias@datasite.com, 651 632 4042

A execução do DPA, no qual este Adendo está anexado, é considerada a execução deste Adendo do Reino Unido

a seguir o **'Importador.'**

Tabela 2: SCCs selecionados, módulos e cláusulas selecionadas

Adendo SCCs da UE:

Cláusulas contratuais padrão de Controlador para Processador (Módulo 2) para a transferência de Dados Pessoais para Processadores estabelecidos em países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, adotado pela Decisão de Execução da Comissão (UE) 2021/914 da Comissão Europeia datado de 4 de junho de 2021, conforme atualizado, alterado, substituído ou suplantado de tempos em tempos ("EU SCCs")

Data: Data Efetiva do Contrato Referência: Nenhuma

Tabela 3: Informações do Apêndice

"Informações do Apêndice" significa as informações que devem ser fornecidas para os módulos selecionados, conforme estabelecido no Apêndice Aprovada das SCCs da UE (além das Partes), e que para este Adendo são definidas em:

Anexo 1A: Lista das Partes: Ver Parte A do Anexo 1 das SCCs Aprovadas da UE

Anexo 1B: Descrição da Transferência: Consulte a Parte B do Anexo 1 das SCCs Aprovadas da UE

Anexo II: Ver Apêndice 2 do DPA

Anexo III: https://www.datasite.com/us/en/legal/sub-processors.html

Tabela 4: Encerramento deste Adendo quando o Adendo Aprovado Mudar

Encerramento deste Adendo quando o Adendo Aprovado mudar:

Quais Partes podem rescindir este Adendo conforme estabelecido na Seção 19: Importador e Exportador

Parte 2: Cláusulas Obrigatórias

Cláusulas Obrigatórias:

Parte 2: Cláusulas Obrigatórias do Adendo Aprovado, sendo o modelo do Adendo B.1.0 emitido pela ICO e apresentado ao Parlamento de acordo com s119A da Lei de Proteção de Dados de 2018 em 2 de fevereiro de 2022, conforme revisado na Seção 18 dessas Cláusulas Obrigatórias.