Data Processing Addendum

数据处理补充协议

This Addendum on Data Processing (hereinafter: “Addendum”) is by and between:

本数据处理补充协议（以下简称“**补充协议**”） 由以下各方订立：

Customer and its Affiliates as defined by the SOW:

– hereinafter referred to as “**Customer**”–

and

Datasite entity as defined by the SOW:

– hereinafter referred to as “**Datasite**”–

Hereinafter each individually referred to also as the “**Party**” and collectively as the “**Parties.**”

SOW 定义的客户及其**关联公司** ：

– 以下简称 “**客户**”。–

以及

SOW 定义的 Datasite 实体：

– 以下简称 “**Datasite“**。–

以下各单独称为 “**一方**“，统称为”**双方“。**

Preamble:

序言：

(A) The Parties have entered into an Agreement which outlines the Services to be provided (definitions provided in Section 1 below). As part of the provision of Services by Datasite, Personal Data may be transferred by the Customer to Datasite.

（A） 双方已签订概述了将会提供的服务的协议（定义见下文第 1 节）。作为 Datasite 提供服务的一部分，客户可能会将个人数据转移到 Datasite。

(B) Capitalized terms not defined in this Addendum are defined in the Agreement. In the event of any conflict between the provisions in this Addendum and the provisions set forth in the Agreement, the provision or provisions of this Addendum will prevail.

（B） 协议中的定义适用于在本补充协议中未定义的用词。如果本补充协议中的条款与协议中规定的条款之间存在任何冲突，则以本补充协议的条款为准。

(C) To ensure compliance by the Parties with Processing obligations pursuant to the Data Protection Rules, as amended from time to time, the Parties hereby agree as follows:

（C） 为确保双方遵守不时修订的数据保护规则所规定的处理义务，双方特此同意如下：

1. Definitions

1. 定义

1.1. “**Agreement**” means the Statement of Work and the applicable General Terms and Conditions between the Customer and Datasite.

1.1. “**协议**”是指客户与 Datasite 之间的工作说明书以及适用的一般条款及条件。

1.2. “**Appendix**” means the appendices annexed to and forming an integral part of this Addendum.

1.2. “**附录**” 是指本补充协议所附并构成本补充协议一部分的附录。

1.3. “**Business Operations**” means: (1) billing, payments, and account management; (2) for the purposes of direct marketing; (3) internal reporting and business modeling (e.g. forecasting, revenue, capacity planning, product strategy); (4) improving and developing new products and services; (5) combatting fraud, cybercrime, or cyber-attacks that may affect Datasite or Datasite products; (6) improving the core functionality of accessibility, or privacy of the Website; and

(7) financial reporting and compliance with legal obligations.

1.3. “**业务运营**” 是指：（1）出具账单、付款和账户管理;（2） 以直接促销为目的;（3）内部报告和业务建模（例如预测、收入、产能规划、产品策略）;（4）改进和开发新产品和服务;（5） 打击可能影响 Datasite 或 Datasite 产品的诈骗、网络犯罪或网络攻击;（6）改进网站可存取性的核心功能或其隐私性;（7）财务报告和遵守法律义务。

1.4. “**Controller**” means an entity that determines the purposes and means of the Processing of Personal Data.

1.4. “**控制者**”是指决定个人数据处理目的和方式的实体。

1.5. “**Data Protection Rules**” means the relevant national laws that apply to the Processing of Personal Data, including but not limited to: European Data Protection Laws, US Data Protection Laws, and the Australian Privacy Principles, as applicable.

1.5.“**数据保护规则**”是指相关国家/地区适用于个人数据处理的法律， 包括但不限于：欧洲数据保护法、美国数据保护法和澳大利亚隐私原则（如适用）。

1.6. “**Data Subject**” means an identified or identifiable natural person whose Personal Data is subject to Processing; an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity, or as otherwise defined in applicable Data Protection Rules.

1.6. “**数据主体**”是指其个人数据受到处理的已识别或可识别的自然人 ; 可识别的人是指可以通过参考识别特征（例如姓名、身份证明号码、位置数据和在线标识码）， 或特定于物理、生理、遗传、精神、经济、文化或社会身份的一个或多个因素，而识别到的人，或适用数据保护规则中就“数据主体”所作出的另有定义。

1.7. “**European Data Protection Laws**” means the GDPR and the Swiss Data Protection Act collectively.

1.7. “**欧洲数据保护法**”是指 GDPR 和瑞士数据保护法。

1.8. “**GDPR**” means UK GDPR and the EU General Data Protection Regulation 2016/679.

1.8. “**GDPR**”是指英国 GDPR 和欧盟通用数据保护条例 2016/679。

1.9. “**International Data Transfer Agreement**” or “**IDTA**” means the international data transfer agreement for the transfer of Personal Data to processors established in third countries pursuant to Article 46 and Chapter V of UK GDPR.

1.9“**国际数据转移协议**”或“**IDTA**”是指根据英国 GDPR 第 46 条和第 V 章就向第三国成立的处理者转移个人数据的国际数据转移协议。

1.10.“**Personal Data**” means any information relating to a Data Subject contained within the Content.

1.10.“**个人数据**”是指与内容中数据主体有关的任何信息。

1.11. “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed, or as otherwise defined in applicable Data Protection Rules.

1.11.“**个人数据泄露**”是指导致经转移、存储或处理的个人数据的意外或非法破坏、遗失、更改、未经授权披露或存取的安全违反, 或适用的数据保护规则中就“个人数据泄露” 所作出的另有定义。

1.12. “**Process**”, “**Processing**” or “**Processed**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction, or as otherwise defined in applicable Data Protection Rules.

1.12. “**处理**”、“**经处理**”或“**已处理**”是指对个人数据进行的任何操作或一组操作 ，无论该操作是否通过自动方式，例如收集、记录、组织、结构化、存储、改编或更改、读取、咨询、使用、透过传输、传播或以其他方式披露、校正或组合、封锁、删除或销毁，或适用的数据保护规则中就“处理”、“经处理”或“已处理”所作出的另有定义。

1.13. **“Processor”** means an entity that Processes Personal Data on behalf of a Controller.

1.13.“**处理者**”是指代表控制者处理个人数据的实体。

1.14. “**Services**” means the provision of services as described in the Agreement and this Addendum.

1.14. “**服务**”是指提供协议和本补充协议中所述的服务。

1.15."**Special Categories of Data**" means the Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data Processed for the purpose of uniquely identifying a natural person, as well as Personal Data concerning health, sex life or sexual orientation, or as otherwise defined in applicable Data Protection Rules.

1.15. "**特殊类别的数据**"是指为了唯一识别某一自然人而处理的揭示种族或族裔、政治观点、宗教或哲学信仰、工会会员资格、遗传数据、生物特征数据的个人数据， 以及有关健康、性生活或性取向的个人数据，或适用数据保护规则中就"特殊类别的数据" 所作出的另有定义。

1.16. "**Standard Contractual Clauses**" or "**SCCs**" means the Controller to Processor (Module 2) standard contractual clauses for the transfer of Personal Data to entities not subject to the GDPR/Swiss Data Protection Act, in line with the requirements of the GDPR and Swiss Data Protection Act, as applicable.

1.16. "**标准合同条款**"或"SCCs"是指根据 GDPR 和瑞士数据保护法（如适用）的要求，就将个人数据转移到不受 GDPR/瑞士数据保护法约束的实体的控制者与处理者 （模组 2）标准合同条款。

1.17."**Subprocessor**" means an entity engaged by a Processor to Process Personal Data on behalf of a Controller.

1.17. "**子处理者**"是指处理者聘请代表控制者处理个人数据的实体。

1.18."**Swiss Data Protection Act**" means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1) and Ordinances SR 235.11 and SR 235.13, as amended and following the coming into force of its revised version of 25 September 2020 on 1 January 2023 (or at the later date subject to the legislative procedure), subject to such revised version, as amended, replaced, or superseded from time to time, insofar as these apply to the Processing of Personal Data.

1.18."**瑞士数据保护法**"是指适用于个人数据处理范围内的经修订后的 1992 年 6 月 19 日颁布的《瑞士联邦数据保护法》（SR 235.1） 和 SR 235.11 和 SR 235.13 条例，以及将于 2023 年 1 月 1 日（或受限于立法程序的往后日子）生效的其 2020 年 9 月 25 日修订版（受限于不时被修改、替换或取代的修订版本）。

1.19."UK GDPR" means s.3(10), 205(4) and the general processing provisions of the Data Protection Act of 2018, as updated, amended, replaced, or superseded from time to time.

1.19. "UK GDPR"是指不时更新、修订、替换或取代的《2018 年数据保护法》的第 3（10） 条、第 205（4） 条和一般处理条款。

1.20. "**US Data Protection Laws**" means the following laws to the extent applicable to Personal Data and the provision of the Services once they become effective: the California Consumer Privacy Act (and California Privacy Rights Act once effective), Cal. Civ. Code § 1798.100 *et seq.*; and other materially similar U.S. laws that may be enacted and that apply to Personal Data from time to time.

1.15. "美国数据保护法"是指（在其生效后）适用于个人数据以及服务提供的范围内的以下法律：《加州消费者隐私法》（和《加州隐私权法》一旦生效）、加州公民法典 § 1798.100 及其后各条;以及其他可能不时制定、并适用于个人数据的实质上相似的美国法律。

2. Processing Activities

2. 处理活动

2.1. Customer and Datasite agree that: (a) Customer is the Controller of Personal Data and Datasite is the Processor of such data, except when Customer acts as a Processor of Personal Data on behalf a third-party Controller ("Third-Party Controller"), in which case Datasite is a Subprocessor; and (b) this Addendum applies where and only to the extent that Datasite Processes Personal Data on behalf of Customer as Processor or Subprocessor in the course of providing the Services.

2.1. 客户和 Datasite 同意：（a）除非客户代表第三方控制者（"第三方控制者"）作为个人数据处理者，客户是个人数据的控制者，而 Datasite 是此类数据的处理者。如客户代表第三方控制者，则 Datasite 是子处理者;和（b） 本补充协议仅适用于 Datasite 在提供服务的过程中代表客户作为处理者或子处理者处理个人数据的情况。

2.2. The Customer agrees that: (a) it has obtained all relevant consents or ensured it has other lawful legal basis (as applicable), permissions and rights and provided all relevant notices necessary under Data Protection Rules for Datasite to lawfully Process Personal Data in accordance with this Agreement including, without limitation, Customer's sharing and/or receiving of Personal Data with third-parties via the Services; (b) it shall comply with, and is responsible for its Affiliates and invited Users' compliance with applicable Data Protection Rules; and (c) its Processing instructions to Datasite are consistent with Data Protection Rules and all instructions from Third-Party Controllers, if applicable.

2.2. 客户同意：（a）其已获得所有相关同意或确保其具有其他合法法律依据（如适用）、许可和权利，并已提供数

据保护规则所必需的所有相关通知，以让 Datasite 可根据本协议合法处理个人数据，包括但不限于客户通过服务与第三方分享和/或接收个人数据;（b） 其应遵守，并负责其关联公司和受邀用户遵守，适用的数据保护规则;（c） 其对 Datasite 发出的处理指令符合数据保护规则和第三方控制者的所有指令（如适用）。

2.3. Datasite agrees to Process the Personal Data in accordance with: (a) this Addendum and the Agreement; (b) Customer's written instructions as set forth in Appendix 1 of this Addendum; and (c) as may be communicated by the Customer from time to time, if required under Data Protection Rules. Any additional requested instructions require the prior written agreement of Datasite.

2.3. Datasite 同意根据以下条款处理个人数据:(a） 本补充协议和协议;（b）本补充协议附录 1 中规定的客户书面指示;（c）（如果数据保护规则要求）客户不时作出的沟通 。任何要求的额外指示均需事先获得 Datasite 的书面同意。

2.4. To the extent Feedback, Usage Data, or User Data (collectively for purposes of this paragraph only, "Data") relate to an identified or identifiable person, the Parties agree that Datasite: (a) will act as an independent "controller" and/or "business" (as such terms are defined under Data Protection Rules) with respect to such Data; and (b) shall process such Data only for its Business Operations and in compliance with all applicable Data Protection Rules. Customer agrees that it has obtained all relevant consents, permissions and rights and provided all relevant notices necessary under Data Protection Rules for Datasite to lawfully process Data as an independent "controller" and/or "business" (as such terms are defined under Data Protection Rules) for Datasite's Business Operations.

2.4. 在回馈、使用数据或用户数据（仅就本段而言统称为"数据"）与已识别或可识别的人员相关的情况下，则双方同意 Datasite：（a） 将作为与此类数据的独立"控制者"和/或"业务"（此类术语在数据保护规则中定义）;以及 （b） 应仅出于其业务运营处理此类数据并在处理此类数据时遵守所有适用数据保护规则。客户同意，其已获得所有相关的同意、许可和权利，并已提供数据保护规则所必需的所有相关通知，以让 Datasite 可以作为的独立"控制者"和/或"业务"（此类术语在数据保护规则中定义）为 Datasite 业务运营合法处理数据。

2.5. If Datasite believes that an instruction infringes upon Data Protection Rules, it will notify the Customer without undue delay. Where the Customer is acting as Processor, it shall be responsible for any notification, assistance or authorization that may be required to be given to or received by its Third-Party Controller. Datasite acknowledges, when acting as a Service Provider, it does not receive any Personal Data as consideration for the Services (as such terms are defined under US Data Protection Laws).

2.5. 如果 Datasite 认为指示违反了数据保护规则，Datasite 将立即通知客户。如果客户作为处理者，则其应负责第三方控制者可能需要提供或接收的任何通知、协助或授权。Datasite 承认，在作为服务提供商时，Datasite 不会以收到任何个人数据作为服务的对价（此术语在美国数据保护法中定义）。

3. Duration and Termination of this Addendum

3. 本补充协议的期限和终止

3.1. This Addendum is effective as of the Effective Date and shall remain in force during the term of the Agreement. This Addendum will terminate automatically with the termination or expiry of any SOW.

3.1. 本补充协议自生效日期起生效，并在协议期限内持续有效。本补充协议将在任何 SOW 终止或到期时自动终止。

3.2. Notwithstanding the termination of this Addendum, Datasite shall continue to be bound by its obligation of confidentiality.

3.2 即使本补充协议已终止，Datasite 仍应继续受其保密义务的约束。

4. International Transfers

4. 国际转移

All Personal Data is stored at third-party hosting facilities within the United States, European Economic Area ("EEA") or Australia. Customer acknowledges that Processor may transfer Personal Data to countries in which it and or its Subprocessors operate; however, Personal Data will continue to be stored in the United States, EEA or Australia. Unless transferred on the basis of an adequacy decision issued by the applicable national authority, all transfers of Personal Data out of the United Kingdom, EEA and Switzerland shall be governed by the SCCs (as Appendix 3) and IDTA (as Appendix 4) incorporated into this Addendum. Datasite will abide by European Data Protection Laws regarding the collection, use, transfer, retention, and other processing of Personal Data from the EEA, UK and Switzerland.

所有个人数据都存储在美国、欧洲经济区（"EEA"）或澳大利亚境内的第三方托管设施中。客户同意 Datasite 可能会将个人数据转移到其和/或其子处理者运营的国家；但是，个人数据将继续存储于美国、EEA 或澳大利亚。除非根据适用国家当局发布的充分性决定进行转移，否则所有从英国、EEA 或瑞士转移至英国、EEA 或瑞士以外地区的个人数据都应受纳入本附录的 SCCs（见附录 3）和 IDTA（见附录 4）的约束。 Datasite 将遵守欧洲数据保护法关于收集、使用、转移、

保留和其他处理来自 EEA、英国和瑞士的个人数据的规定。

5. Confidentiality and Security

5. 保密性和安全性

5.1. Datasite shall: (a) keep Personal Data confidential; and (b) ensure that its employees who Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.1. Datasite 应：（a） 保密个人数据;以及 （b） 确保其处理个人数据的员工已承诺保密或负有适当的法定保密义务。

5.2. Subject to the Data Protection Rules, Datasite will implement appropriate operational, technical, and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access as described in Appendix 2.

5.2. 受限于数据保护规则，Datasite 将如附录 2 中所述，实施适当的运营、技术和组织性措施以保护个人数据免遭意外或非法破坏、遗失、更改、未经授权的披露或存取。

5.3. Customer is solely responsible for making an independent determination as to whether the technical and organizational measures put in place by Datasite meet Customer’s requirements, including any of its security obligations under applicable Data Protection Rules. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to Data Subjects) the security practices and policies implemented and maintained by Datasite provide a level of security appropriate to the risk with respect to the Personal Data.

5.3. 客户应付所有责任独立决定 Datasite 实施的技术和组织性措施是否符合客户的要求，包括其在适用的数据保护规则下的任何安全义务。客户承认并同意（考虑到现有技术、实施成本、处理其个人数据的性质、范围、背景和目的以及对数据主体的风险），Datasite 实施和维持的安全实践和政策提供了与个人数据的风险相适应的安全水平。

5.4. Datasite will update the technical and organizational security measures in line with reasonable technological developments as determined by Datasite.

5.4. Datasite 将根据合理技术发展更新技术和组织安全措施（实质措施由 Datasite 决定）。

6. Cooperation and Notification Obligations

6. 合作和通知义务

6.1. The Parties will co-operate with each other to promptly and effectively handle enquiries, complaints, and claims relating to the Processing of Personal Data from any government authority or Data Subject.

6.1. 双方将相互合作以迅速及有效地处理来自任何政府机构或数据主体的与个人数据处理有关的查询、投诉和索赔。

6.2. If a Data Subject should apply directly to Datasite to exercise his/her Personal Data rights, Datasite will assist Customer with such request by forwarding this request to the Customer without undue delay if permitted by Data Protection Rules.

6.2. 如果数据主体应直接向 Datasite 申请行使其个人数据权利，Datasite 在数据保护规则允许的情况下会把此请求转发给客户来协助客户处理该请求，而不作不当拖延。

6.3. Unless prohibited by law, if the Personal Data is subject to a control, order, or investigation by public authorities, Datasite will: (a) promptly notify the Customer; and (b) disclose Personal Data only to the extent that is strictly necessary and proportionate to satisfy the request and in compliance with Data Protection Rules. Upon Customer’s request, Datasite will provide the public authorities with information regarding Processing under this Addendum as well as allow inspections within the scope stated in Section 7, as required by Data Protection Rules.

6.3. 除非法律禁止，否则如果个人数据受到公共机关的控制、命令或调查，Datasite 将：（a） 迅速通知客户; 和 （b） 仅在满足要求的严格必要和相称的范围内，及符合数据保护规则的范围内披露个人数据。根据客户的要求，Datasite 将向公共机关提供有关在本补充协议下之处理的信息，并根据数据保护规则要求允许在第 7 节所述的范围内进行检查。

6.4. Datasite will notify the Customer of a Personal Data Breach that is determined to affect Customer’s Personal Data without undue delay. Datasite shall provide Customer with the information to reasonably assist Customer as required by Data Protection Rules.

6.4. 如客户的个人数据被认定受个人数据泄露影响，Datasite 将在不作不当拖延的情况下通知客户。Datasite 应根

据数据保护规则的要求，向客户提供信息以合理协助客户。

6.5. Considering the nature of Processing and Personal Data, Datasite will provide reasonable assistance to Customer with carrying out a data protection impact assessment and prior consultation under Data Protection Rules to the extent Customer is not able to carry these out independently.

6.5. 考虑到处理和个人数据的性质，如果客户无法独立进行数据保护影响评估和事先咨询，Datasite 将向客户提供合理的协助，以根据数据保护规则进行数据保护影响评估和事先咨询。

7. Customer's Audit and Inspection Rights

7. 客户的审计和检查权利

Upon Customer's request, and subject to reasonable notice, time, place, frequency, and manner restrictions, and confidentiality requirements, Datasite shall make available to Customer information necessary to demonstrate compliance with Datasite's obligations under the Addendum and applicable Data Protection Rules. Datasite will allow for and contribute to audits, including inspections, conducted by Customer, or an independent third-party auditor appointed by Customer. To the extent Customer's rights under this section cannot reasonably be satisfied through audit reports, documentation, or compliance information Datasite makes generally available to its customers, Customer shall be responsible for all costs and fees related to such audit.

当客户要求，并在遵守合理通知、时间、地点、频率和方式限制以及保密要求的前提下 ，Datasite 应向客户提供必要的信息 ，以证明 Datasite 遵守了本补充协议和适用数据保护规则的义务。 Datasite 将允许由客户或客户指定的独立第三方审计师进行的审计， 包括检查，并为该等审计出力。在 Datasite 向其客户普遍提供的审计报告、文档或合规性信息无法合理地满足客户在本节下的权利的范围内，则客户应负责与此类审计相关的所有成本和费用。

8. Use of Subprocessors

8. 子处理者的使用

8.1 Customer hereby acknowledges and provides general authorization for Datasite to use Subprocessors to Process Personal Data. Datasite's current list of Subprocessors is available at https://www.datasite.com/us/en/legal/sub-processors.html. Datasite shall: (a) ensure that any Subprocessors Process Personal Data only to deliver the Services Datasite has retained them to provide; (b) impose on any Subprocessor contractual obligations relating to Personal Data no less protective than this Addendum; and (c) be liable for each Subprocessor's compliance with such obligations.

8.1 客户特此确认并提供 Datasite 使用子处理者处理个人数据的一般授权。Datasite 当前的子处理者列表请见 https://www.datasite.com/us/en/legal/sub-processors.html。Datasite 应：（a） 确保任何子处理者仅为提供 Datasite 聘请他们提供的服务而处理个人数据;（b） 对任何子处理者施加保护程度不低于本补充协议项下与个人数据相关的合同义务;并且 （c） 对每个子处理者遵守此类义务承担责任。

8.2 Datasite shall make available on its Subprocessor site a mechanism for Customers to subscribe to notifications of new Subprocessors by providing an email address. If Datasite intends to appoint or replace a Subprocessor covered by this Addendum, at least sixty (60) days prior to allowing the new Subprocessor to Process Personal Data, Datasite shall: (a) update its Subprocessor site; (b) provide notification to those emails that have subscribed; and (c) in respect to both (a) and (b) give Customer the opportunity to object to such changes on reasonable grounds related to data protection. If the parties are unable to achieve a resolution, Customer, as its sole and exclusive remedy, may provide written notice to Datasite terminating the SOW(s).

8.2 Datasite 应在其子处理者网站上提供一种机制，以让客户能通过提供电子邮件地址来订阅新子处理者的通知。 如果 Datasite 打算任命或替换本补充协议下的子处理者，Datasite 应在允许新的子处理者处理个人数据之前至少六十 （60） 天：（a） 更新其子处理者网站;（b） 向已订阅的电子邮件提供通知;（c）就（a）和（b）为客户提供机会以与数据保护相关的合理理由反对此类更改。如果双方无法达成解决方案，客户可以向 Datasite 提供书面通知以终止 SOW(s) 作为其唯一和排他性的补救措施。

9. Return and Deletion of Personal Data

9. 个人数据的归还和删除

Upon the request of the Customer or upon termination of this Addendum, Datasite will, return (in accordance with the SOW) or destroy all Personal Data and copies thereof, unless applicable Data Protection Rules or another legal obligation require Datasite to retain Personal Data for longer. Upon the request of the Customer, Datasite will certify that this has been done.

当客户要求或本补充协议终止，Datasite 将（根据 SOW）归还或销毁所有个人数据及其副本（除非适用的数据保护规则或其他法律义务要求 Datasite 将个人数据保留更长时间）。当客户要求，Datasite 将证明已完成此操作。

10. Liability

10. 责任

Without prejudice to the rights or remedies available to Data Subjects under Data Protection Rules, the liability of the Parties and the limitation thereof, including any claim brought by an Affiliate, shall be in accordance with the Agreement.

在不影响数据保护规则规定下数据主体可获得的权利或补救措施的情况下，双方的责任及其限制（包括关联公司提出的任何索赔）均应按照协议处理。

11. Language

11. 语言

If there is any discrepancy between the English version and Chinese version of this Addendum, the English version shall prevail.

如本补充协议英文版与中文版的内容有任何歧义，概以英文版为准。

客户:	**Datasite:**
By由:___________________________________	By由:_____________________________________
Name姓名: _____________________________	Name姓名: _____________________________
Title职位:________________________________	Title职位:_________________________________
Date日期:________________________________	Date日期:_________________________________

Appendix 1: Processed Personal Data and Purposes
附录 1：处理的个人数据和目的

Personal Data are transferred and Processed for the **following purposes**:

- Secure online repository and data sharing for corporate transactions or internal business purposes.

出于**以下目的**转移和处理**个人数据**:

□ 用于公司交易或内部业务目的的安全在线存储库和数据分享。

Subject Matter and Nature of Processing:

- As described in the Agreement, Datasite provides secure online repository tools for storing, managing, collaborating on, and distributing data and documents.

处理的主题和性质：

□ 如协议中所述，Datasite 将提供安全的在线存储库工具以作存储、管理、协作和分发数据和文件之用。

Categories of Personal Data:

The types of Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

- Names, address, company email address, company phone number, compensation and benefits, holiday and pension information, job titles and functions and potentially other types of Personal Data uploaded by Customer Administrator onto the Website.

个人数据的类别：

个人数据的类型由客户全权自行决定和控制，其可能包括但不限于：

□ 姓名、地址、 公司电子邮件地址、公司电话号码 、 薪酬和福利、假日和退休金信息、职位和职能以及可能包括客户管理员上传到网站的其他个人数据。

Special Categories of Data (if applicable):

Subject to any applicable condition in the Agreement, the types of Special Categories of Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

- None, unless otherwise identified by Customer

特殊类别的数据（如适用）：

受限于协议中的任何适用条件，特殊类别数据的类型由客户全权自行决定和控制，其可能包括但不限于：

□ 无，除非客户另有指明

Data Subjects:

The categories of Data Subjects to which Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

- Business information regarding current, past, and prospective owners, employees, agents, customers, advisors, business partner, contractors, and vendor data subjects.

数据主体：

与个人数据相关的数据主体类别由客户全权自行决定和控制，其可能包括但不限于：

□ 有关当前、过去和潜在拥有者、员工、代理、客户、顾问、业务合作伙伴、承包商和供货商数据主体的业务信息。

Retention:

- All Personal Data is permanently deleted after: (a) Customer Administrator closes the applicable project on the Website; or (b) termination of the Agreement between Customer and Datasite.

保留:

□ 当（a）客户管理员关闭网站上的适用项目;或 （b）客户与 Datasite 之间的协议终止后，所有个人数据将被永久删除 。

Appendix 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

附录 2

技术和组织性措施，包括确保数据安全的技术和组织性措施

	Security Requirement 安全要求	How Datasite implements the specific information security measure Datasite 如何实施具体的信息安全措施
1.	*Measures for encryption of personal data* *个人数据加密措施*	Personal Data is encrypted at rest and in-transit using industry standard encryption technologies, currently at rest using AES 256-bit encryption and In-transit via Transport Layer Security (TLS) 1.2 protocol, which shall be updated from time to time in line with reasonable technological developments as determined by Datasite. 个人数据使用行业标准加密技术进行静态和传输中加密(目前使用 AES 256 位加密措施进行静态加密和通过传输层安全性（TLS） 1.2 规格进行传输中加密)。该等措施应根据合理技术发展不时更新（实质措施由 Datasite 决定）。
2.	*Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and ser- vices* *确保处理系统和服务的持续保密性、完整性、可用性和韧性*	Datasite is ISO 27001, 27701, 27017 and 27018 certified, SOC 2 Type II compliant ensuring that it maintains and enforces appropriate administrative, physical and technical safeguards to protect the integrity, availability and confidentially of Customer's Personal Data. Datasite 已通过 ISO 27001、27701、27017 和 27018 认证，以及 符合 SOC 2 Type II 标准，确保其维持和实施适当的管理、物理和技术性保护措施，以保护 客户个人数据的完整性、可用性和保密性。
3.	*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident* *确保在发生物理或技术性事件时及时恢复个人数据的可用性和可存取性的措施*	Datasite has redundancy with each platform and maintains logs of system availability. In addition, redundancy allows for continuous system backups. Datasite has Disaster Recovery and Business Continuity Plans that are reviewed, updated, and tested periodically. Datasite 就每个平台均拥有冗余，并保存系统可用性记录。此外，冗余允许连续的系统备份。Datasite 具有定期审查、更新和测试的灾难恢复和业务连续性计划。
4.	*Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing* *定期测试、评估和评价技术和组织性措施有效性的程序，以确保处理的安全性*	Datasite completes regular code reviews, vulnerability testing and annual penetration testing on the Website. Datasite 在网站上定期完成代码审查、漏洞测试和年度渗透测试。
5.	*Measures for user identification and authorization* *用户识别和授权措施*	Access is governed by Datasite's access management standard that follows roles-based access controls. Access to Personal Data is providing only to personnel as strictly necessary for the sole purpose of satisfying Customer's instructions. The Access Management Standard requires that (a) access rights be reviewed, updated, and approved by management on a regular basis, and (2) access rights be withdrawn within 24 hours of employee's termination. Other types of relevant controls are password requirements, multi- factor authentication and restriction on removable media which are implemented at the corporate

		level. 存取由Datasite的存取管理标准管辖，该标准遵循基于角色的访问控制。 仅严格必要且唯一目的是满足客户指示的人员会得到个人数据的存取权。 存取管理标准要求 （a） 存取权限应由管理层定期审查、更新和批准， 以及 （2） 存取权限在员工解雇后24小时内撤回 。其他类型的相关控制措施包括在公司级别实施的密码要求、多重身份验证和对可移动媒体的限制。
6.	*Measures for the protection of data during transmission* *传输过程中的数据保护措施*	Personal Data is encrypted in transit using industry standard encryption technologies, currently via Transport Layer Security (TLS) 1.2 protocol, which shall be updated from time to time in line with reasonable technological developments as determined by Datasite. 个人数据在传输过程中使用行业标准加密技术进行加密(目前通过传输层安全（TLS）1.2规格进行加密)。该等措施应根据合理技术发展不时更新（实质措施由Datasite决定）。
7.	*Measures for the protection of data during storage* *存储期间数据保护的措施*	Personal Data is encrypted at rest using industry standard encryption technologies, currently AES 256-bit encryption, which shall be updated from time to time in line with reasonable technological developments as determined by Datasite. 个人数据使用行业标准加密技术（目前为AES 256位加密）进行静态加密。该等措施应根据合理技术发展不时更新（实质措施由Datasite决定）。
8.	*Measures for ensuring physical security of locations at which personal data are processed* *确保个人数据处理地点的物理性安全的措施*	Datasite relies on cloud service providers for its data storage requirements. Information regarding Microsoft Azure’s physical security protocols for its server locations is available at: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security. All data centers hold ISO 27001:2013 and SOC 2 Type 2 certifications. With respect to Datasite’s facilities, all offices require badge access and utilize newly updated video surveillance using cameras with recordings stored in the cloud. Datasite依靠云服务提供商来满足其数据存储要求。 有关Microsoft Azure针对其服务器位置的物理性安全规格的信息，请访问： https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security。所有数据中心均持有ISO 27001：2013和SOC 2第2类认证。至于Datasite的 设施， 所有办公室都需要证件进入，并使用最近更新的、利用摄像机的视频监控 ，且该等录像记录存储在云端。
9.	*Measures for ensuring events logging* *确保事件记录的措施*	Datasite performs logging and monitoring that is centrally collected and normalized within its SIEM tool. Logs are retained for 180 days, and access is roles and responsibility based. Datasite进行在其SIEM工具中集中收集和常规化的事件记录和监测。记录将保留180天，并且存取权乃基于角色和责任来决定。
10.	*Measures for ensuring system configuration, including default configuration* *确保系统配置的措施，包括默认配置*	Datasite has standard build processes and applies CIS hardening standards. Datasite具有标准的构建流程，并应用CIS强化标准。
11.	*Measures for internal IT and IT security governance and management* *内部IT和IT安全治理和管理措施*	Datasite maintains a robust information security management system governed by Datasite’s PIMS Committee that is responsible for implementing and maintaining a stable and secure environment. Datasite维持着一个强大的由Datasite的PIMS委员会管理的信息安全管理系统，其负责实施和维持稳定和安全的环境。
12.	*Measures for certification/ assurance of processes and products* *程序和产品的认证/保证措施*	Datasite has maintained a SOC II Type II attestation and an ISO 27001 certification since 2007, ISO 27017 and 27018 since 2021 and ISO 27701 since 2023. 自2007年以来，Datasite一直保持着SOC II第II类认证和ISO

		27001认证，自2021年起保持着ISO 27017和27018认证，自2023年起保持着ISO 27701认证。
13.	*Measures for ensuring data minimization* *确保数据最小化的措施*	Personal Data collected and processed will not be held or used unless necessary to provide the Services in compliance with the Service Agreement and Datasite’s policies and Privacy Notice. 除非有必要根据服务协议和Datasite的政策和隐私声明以提供服务，收集和处理的个人数据将不会被保留或使用。
14.	*Measures for ensuring data quality* *确保数据质量的措施*	Datasite utilizes an anti-malware client on all systems. Personal Data uploaded to the Website is scanned by Datasite’s anti-malware software as part of the document processing activities that occur within the platform. Datasite在所有系统上都使用反恶意软件客户端。 上传到网站的个人数据在平台内发生的文档处理活动过程中由Datasite的反恶意软件软件进行扫描。
15.	*Measures for ensuring limited data retention* *确保有限数据保留的措施*	Personal Data is purged beginning 30 days post project closure or upon termination of Service Agreement. 个人数据将在项目结束或服务协议终止后30天开始清除。
16.	*Measures for ensuring accountability* *确保问责制的措施*	All activity logged is tracked and reportable. Personnel complete training and acknowledge compliance with Datasite’s code of conduct and policies annually. All personnel are required to sign an NDA. The Code of Conduct is affirmed by all personnel on a yearly basis. 记录的所有活动都会被追踪和是可报告的。人员每年均需完成培训并确认遵守Datasite的行为准则和政策。所有人员都必须签保密协议。 全体人员每年都须确认行为准则。
17.	*Measures for allowing data portability and ensuring erasure* *允许数据可移植性和确保数据删除的措施*	Customer host Personal Data on servers as defined in the Service Agreement which may be transferred to other locations in which Datasite maintains servers, upon request. Personal Data can be returned to clients via encrypted USB device, if requested. Deletion of Personal Data beings 30 days from project closure or termination of the Service Agreement. 客户在服务协议中定义的服务器上寄存个人数据。当要求时，这些数据可被转移到Datasite设有服务器的其他位置。当要求时，个人数据可以通过加密的USB设备返还给客户。个人数据将在项目结束或服务协议终止后30天开始清除。
18.	*For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter* *对于向（子）处理者的转移，还要描述（子）处理者采取的具体技术和组织性措施，以便能够向控制者提供帮助，对于从处理者到子处理者的传输，还要描述采取的具体技术和组织性措施，以便能够向数据输出者提供帮助*	Datasite maintains a Vendor Security Standard that details minimum vendor security standards necessary to store, process or transmit Personal Data that provides a baseline of control expectations for the evaluation of each vendor, conformance and risk acceptance based on the nature of the vendor relationship. Each in scope vendor is required to sign contracts (DPA SCCs) that ensure the same level or protection to Datasite as Datasite obligations to Customer. Datasite设有供货商安全标准，其详细说明了存储、处理或传输个人数据所需的最低供货商安全标准，该标准为根据供货商关系的性质评估每个供货商、符合性和风险接受提供了期望的控制措施的基线。范围内的每个供货商都需要签署合同 （DPA SCCs），以确保其对Datasite负有Datasite对客户相同级别保护的义务。

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**

8.2

(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.

8.3 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.

8.4 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.

8.5 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.

8.6 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).

8.7 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.

8.8 **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.

8.9 **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.

8.10 **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.

Annex 1
附件一

A. LIST OF PARTIES
A．缔约方名单

Data exporter:
数据输出者：

Name: Customer as defined by the SOW, unless otherwise identified herein:
名称：SOW所定义的客户，除非本文另有说明：

Address:
地址：

Contact person's name, position and contact details:

联系人的姓名、职位和联系方式：

Activities relevant to the data transferred under these Clauses: Data Exporter uses SaaS-based electronic secure online repository tools ("Website") for storing, managing, collaborating on and distributing data and documents ("Content") pursuant to a service agreement between Data Exporter and Data Importer ("Service Agreement") (the "Services"). The Data Importer stores Content on third party servers within the EU, US, and Australia to provide the Website to Data Exporter and host their Content, which while not assessed for its substance, may contain Personal Data. Website's Content remains stored on those servers, but may be accessed from Data Importers' personnel for the purpose of providing the Services as further described in Appendix 1.
与根据这些条款转移的数据相关的活动：数据输出者根据数据输出者及数据输入者之间的服务协议（"服务协议"），使用基于 SaaS 的电子安全网上存储库工具（"网站"）以存储、管理、协作和分发数据和文件（"内容"）（"服务"）。数据输入者将内容存储在欧盟、美国和澳大利亚境内的第三方服务器上，以向数据输出者提供网站并托管其内容。这些内容虽然未经实质性评估，但可能包含个人数据。网站的内容仍然存储在这些服务器上，但可以从数据输入者的人员那里存取，以提供附录1中进一步描述的服务。

Role: Controller
角色：控制者

Data importer:
数据输入者：

Name: Datasite LLC, a limited liability company registered in Delaware, USA, and its in-scope Affiliates

名称：Datasite LLC，一家在美国特拉华州注册的有限责任公司，及其范围内的**关联公司**

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

Contact person's name, position and contact details: Patricia Elias, Director, Secretary and Data Protection Officer, patricia.elias@datasite.com, 651 632 4042

联系人的姓名、职位和联系方式：Patricia Elias，董事、秘书兼数据保护官，patricia.elias@datasite.com，651 632 4042

Activities relevant to the data transferred under these Clauses:

与根据这些条款转移的数据相关的活动：

Data Importer provides the Website to Data Exporter to host Data Exporters's Content on third party servers within the EU, US or Australia. The Content, while not assessed for its substance, may contain Personal Data. Content remains stored on those servers, but may be accessed from Data Importers' personnel for the purpose of providing the Services as further described in Appendix 1.

数据输入者向数据输出者提供网站，以在欧盟、美国或澳大利亚的第三方服务器上托管数据输出者的内容。这些内容虽然未经实质性评估，但可能包含个人数据。内容仍存储在那些服务器上，但可以从数据输入者的人员那里存取，以便提供附录 1 中进一步描述的服务。

Role: Processor
角色：处理者

B. DESCRIPTION OF TRANSFER
B. 转让的说明

See Appendix 1 of the DPA

见DPA的附录1

C. COMPETENT SUPERVISORY AUTHORITY
C. 主管监督机构

- ***Germany Federal Commissioner for Data Protection and Freedom of Information***

  德国联邦数据保护和信息自由专员

Annex 2
附件二

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
技术和组织性措施，包括确保数据安全的技术和组织性措施

See Appendix 2 of the DPA

见DPA的附录2

APPENDIX 4
附录4
INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES
欧盟委员会标准合同条款的国际数据转移补充协议

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

本补充协议由信息专员为进行受限转移的各方发布。信息专员认为，在作为具有法律约束力的合同签订时，其为受限转移提供了适当保障措施。

Part 1: Tables

第 1 部分：表格

Table 1: PARTIES AND SIGNATURE
表格 1：缔约方和签署

Customer as defined by the SOW, unless otherwise identified herein:
SOW所定义的客户，除非本文另有说明：

Execution of the Data Processing Agreement (“DPA”) which this Addendum is appended to is deemed execution of this UK Addendum

*签署本**补充协议**所附的**数据处理协议**（“DPA”）即视为签署本**英国附录***

hereinafter the ‘**Exporter**;’ and

以下简称“**输出者**”，及

Datasite LLC, a limited liability company registered in Delaware, USA, and its in-scope Affiliates
Datasite LLC，一家在美国特拉华州注册的有限责任公司，及其范围内的**关联公司**

Key Contact: Patricia Elias, Director, Secretary and Data Protection Officer, patricia.elias@datasite.com, 651 632 4042

*主要联系人：*Patricia Elias，董事、秘书兼数据保护官，patricia.elias@datasite.com，651 632 4042

Execution of the DPA which this Addendum is appended to is deemed execution of this UK Addendum

签署本补充协议所附的数据处理协议（“DPA”）即视为签署本英国附录

hereinafter the **‘Importer.’**

以下简称“**输入者**”。

Table 2: Selected SCCs, Modules and Selected Clauses

表格 2：选定的 SCC、模组和选定的条款

Addendum EU SCCs:

欧盟 SCCs附录：

Controller to Processor (Module 2) standard contractual clauses for the transfer of Personal Data to Processors established in third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, adopted by Commission Implementing Decision (EU) 2021/914 of the European Commission dated 4 June 2021, as updated, amended, replaced or superseded from time to time (“EU SCCs”)

根据不时更新、修订、替换或取代的，由2021 年 6 月 4 日的欧盟委员会作出的委员会实施决定 (EU) 2021/914采纳的欧洲议会和理事会 2016 年 4 月 27 日的2016/679条例 (EU)项下关于将个人数据转移至在第三国的处理者的控制者到处理者（模组 2）标准合同条款（“欧盟 SCCs”）

Date: Effective Date of the Agreement

日期：协议生效日期

Reference: None

参考：无

Table 3: Appendix Information
表格 3：附录信息

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

“附录信息”是指必须为经批准的欧盟 SCCs（缔约方除外）的附录中列出的选定模组所提供的信息。对于本补充协议，这些信息列于：

Annex 1A: List of Parties: See Part A of Annex 1 of Approved EU SCC’s

附件 1A：缔约方名单：参见经批准的欧盟 SCC’s 附件 1 的 A 部分

Annex 1B: Description of Transfer: See Part B of Annex 1 of Approved EU SCC’s
附件 1B：转移说明：参见经批准的欧盟 SCC’s 附件 1 的 B 部分

Annex II: See Appendix 2 of the DPA
附件二：见 DPA 附录 2

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

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

Table 4: Ending this Addendum when the Approved Addendum Changes

表格 4：在批准的附录改变时终止本补充协议

Ending this Addendum when the Approved Addendum changes:

在批准的附录改变时结束本补充协议：
Which Parties may end this Addendum as set out in Section 19: Importer and Exporter
哪些缔约方可以按照第 19 节的规定终止本补充协议：输入者和输出者

Part 2: Mandatory Clauses
第 2 部分：强制性条款

Mandatory Clauses:
强制性条款：

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
第 2 部分：已批准附录的强制性条款，即 ICO 发布的、于 2022 年 2 月 2 日根据 2018 年数据保护法第 119A 条提交议会并根据这些强制性条款的第 18 条进行了修订的模板附录 B.1.0。