# Data Processing Addendum
# 數據處理補充協議

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

本數據處理補充協議（以下簡稱“**補充協議**”） 由以下各方訂立：

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 定義的客戶及其**關聯公司** ：

– 以下簡稱 “**客戶**”。–

*以及*

SOW 定義的 Datasite 實體：

– 以下簡稱 “**Datasite“**。–

以下各單獨稱為 “**一方**“，統稱為”**雙方“。**

**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） 雙方已簽訂概述了將會提供的服務的協議（定義見下文第 1 節）。作為 Datasite 提供服務的一部分，客戶可能會將個人數據轉移到 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） 協議中的定義適用於在本補充協議中未定義的用詞。如果本補充協議中的條款與協議中規定的條款之間存在任何衝突，則以本補充協議的條款為准。

(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） 為確保雙方遵守不時修訂的數據保護規則所規定的處理義務，雙方特此同意如下：

**1. Definitions**

**1. 定義**

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

1.1. “**協議**”是指客戶與 Datasite 之間的工作說明書以及適用的一般條款及條件。

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

1.2. “**附錄**” 是指本補充協議所附並構成本補充協議一部分的附錄。

**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.** “**業務運營**” 是指：（1）出具帳單、付款和帳戶管理;（2） 以直接促銷為目的;（3）內部報告和業務建模（例如預測、收入、產能規劃、產品策略）;（4）改進和開發新產品和服務;（5） 打擊可能影響 Datasite 或 Datasite 產品的詐騙、網絡犯罪或網絡攻擊;（6）改進網站可存取性的核心功能或其私隱性;（7）財務報告和遵守法律義務。

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

**1.4.** “**控制者**”是指決定個人數據處理目的和方式的實體。

**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**.“**數據保護規則**”是指相關國家/地區適用於個人數據處理的法律， 包括但不限於：歐洲數據保護法、美國數據保護法和澳大利亞私隱原則（如適用）。

**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.** “**數據主體**”是指其個人數據受到處理的已識別或可識別的自然人 ; 可識別的人是指可以通過參考識別特徵（例如姓名、身份證明號碼、位置數據和線上標識碼），或特定於物理、生理、遺傳、精神、經濟、文化或社會身份的一個或多個因素，而識別到的人，或適用數據保護規則中就“數據主體”所作出的另有定義。

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

**1.7.** “**歐洲數據保護法**”是指 GDPR 和瑞士數據保護法。

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

**1.8.** “**GDPR**”是指英國 GDPR 和歐盟通用數據保護條例 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.** “**國際數據轉移協議**”**或**“**IDTA**”是指根據英國 GDPR 第 46 條和第 V 章就向第三國成立的處理者轉移個人數據的國際數據轉移協議。

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

**1.10.** “**個人數據**”是指與內容中數據主體有關的任何信息。

**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.** “**個人數據洩露**”是指導致經轉移、存儲或處理的個人數據的意外或非法破壞、遺失、更改、未經授權披露或存取的安全違反, 或適用的數據保護規則中就“個人數據洩露” 所作出的另有定義。

**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.** “**處理**”、“**經處理**”或“**已處理**”是指對個人數據進行的任何操作或一組操作 ， 無論該操作是否通過自動方式，例如收集、記錄、組織、結構化、存儲、改編或更改、讀取、諮詢、使用、透過傳輸、傳播或以其他方式披露、校正或組合、封鎖、刪除或銷毀，或適用的數據保護規則中就“處理”、“經處理”或“已處理”所作出的另有定義。

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

**1.13.** “**處理者**”是指代表控制者處理個人數據的實體。

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

**1.14.** “**服務**”是指提供協議和本補充協議中所述的服務。

**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.** “**特殊類別的數據**”是指為了唯一識別某一自然人而處理的揭示種族或族裔、政治觀點、宗教或哲學信仰、工會會員資格、遺傳數據、生物特徵數據的個人數據， 以及有關健康、性生活或性取向的個人數據，或適用數據保護規則中就“特殊類別的數據” 所作出的另有定義。

**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.** “**標準合同條款**”或“SCCs”是指根據 GDPR 和瑞士數據保護法（如適用）的要求，就將個人數據轉移到不受 GDPR/瑞士數據保護法約束的實體的控制者與處理者 （模組 2）標準合同條款。

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

**1.17.** “**子處理者**”是指處理者聘請代表控制者處理個人數據的實體。

**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**. “**瑞士數據保護法**”是指適用於個人數據處理範圍內的經修訂後的 1992 年 6 月 19 日頒佈的《瑞士聯邦數據保護法》（SR 235.1） 和 SR 235.11 和 SR 235.13 條例，以及將於 2023 年 1 月 1 日（或受限於立法程序的往後日子）生效的其 2020 年 9 月 25 日修訂版（受限於不時被修改、替換或取代的修訂版本）。

**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”**是指不時更新、修訂、替換或取代的《2018 年數據保護法》的第 3（10） 條、第 205（4） 條和一般處理條款。

**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.

**1.20. “美國數據保護法”**是指（在其生效後）適用於個人數據以及服務提供的範圍內的以下法律：《加州消費者私隱法》（和《加州私隱權法》一旦生效）、加州公民法典 § 1798.100 及其後各條;以及其他可能不時制定、並適用於個人數據的實質上相似的美國法律。

## 2. Processing Activities

## 2. 處理活動

**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.** 客戶和 Datasite 同意：（a）除非客戶代表第三方控制者（“第三方控制者”）作為個人數據處理者，客戶是個人數據的控制者，而 Datasite 是此類數據的處理者。如客戶代表第三方控制者，則 Datasite 是子處理者;和（b） 本補充協議僅適用於 Datasite 在提供服務的過程中代表客戶作為處理者或子處理者處理個人數據的情況。

**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.** 客戶同意：（a）其已獲得所有相關同意或確保其具有其他合法法律依據（如適用）、許可和權利，並已提供數據保護規則所必需的所有相關通知，以讓 Datasite 可根據本協議合法處理個人數據，包括但不限於客戶通過服務與第三

方分享和/或接收個人數據;（b） 其應遵守，並負責其關聯公司和受邀用戶遵守，適用的數據保護規則;（c） 其對 Datasite 發出的處理指示符合數據保護規則和第三方控制者的所有指令（如適用）。

**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 同意根據以下條款處理個人數據:(a） 本補充協議和協議;（b）本補充協議附錄 1 中規定的客戶書面指示;（c） （如果數據保護規則要求）客戶不時作出的溝通 。任何要求的額外指示均需事先獲得 Datasite 的書面同意。

**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.** 在回饋、使用數據或使用者數據（僅就本段而言統稱為"數據"）與已識別或可識別的人員相關的情況下，則雙方同意 Datasite：（a） 將作為與此類數據的獨立"控制者"和/或"業務"（此類術語在數據保護規則中定義）;以及 （b） 應僅出於其業務運營處理此類數據並在處理此類數據時遵守所有適用數據保護規則。客戶同意，其已獲得所有相關的同意、許可和權利，並已提供數據保護規則所必需的所有相關通知，以讓 Datasite 可以作為的獨立"控制者"和/或"業務"（此類術語在數據保護規則中定義）為 Datasite 業務運營合法處理數據。

**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 認為指示違反了數據保護規則，Datasite 將立即通知客戶。如果客戶作為處理者，則其應負責第三方控制者可能需要提供或接收的任何通知、協助或授權。Datasite 承認，在作為服務提供者時，Datasite 不會以收到任何個人數據作為服務的對價（此術語在美國數據保護法中定義）。

## 3. Duration and Termination of this Addendum

## 3. 本補充協議的期限和終止

**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.** 本補充協議自生效日期起生效，並在協議期限內持續有效。本補充協議將在任何 SOW 終止或到期時自動終止。

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

**3.2** 即使本補充協議已終止，Datasite 仍應繼續受其保密義務的約束。

## 4. International Transfers

## 4. 國際轉移

All Personal Data is stored at third-party hosting facilities within the United States, European Economic Area ("EEA") or Australia. Customer acknowledges that Datasite 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.

所有個人數據都存儲在美國、歐洲經濟區（“EEA”）或澳大利亞境內的第三方託管設施中 。客戶同意 Datasite 可能會將個人數據轉移到其或其子處理者營運的國家; 但是，個人數據將繼續存儲於美國、EEA 或澳大利亞。 除非根據適用國家當局發佈的充分性決定進行轉移，否則所有從英國、EEA 或瑞士至英國、EEA 或瑞士以外地區的個人數據轉移應受 SCCs （見附錄 3）及 IDTA （見附錄 4）約束。Datasite 將遵守歐洲數據保護法關於收集、使用、轉移、保留和其他處理來自 EEA、英國和瑞士個人數據的規定。

## 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 應：（a） 保密個人數據;以及 （b） 確保其處理個人數據的員工已承諾保密或負有適當的法定保密義務。

**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.** 受限於數據保護規則，Datasite 將如附錄 2 中所述，實施適當的運營、技術和組織性措施以保護個人數據免遭意外或非法破壞、遺失、更改、未經授權的披露或存取。

**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.** 客戶應付所有責任獨立決定 Datasite 實施的技術和組織性措施是否符合客戶的要求，包括其在適用的數據保護規則下的任何安全義務。客戶承認並同意（考慮到現有技術、實施成本、處理其個人數據的性質、範圍、背景和目的以及對數據主體的風險），Datasite 實施和維持的安全實踐和政策提供了與個人數據的風險相適應的安全水準。

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

**5.4.** Datasite 將根據合理技術發展更新技術和組織安全措施（實質措施由 Datasite 決定）。

## 6. Cooperation and Notification Obligations

## 6. 合作和通知義務

**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.** 雙方將相互合作以迅速及有效地處理來自任何政府機構或數據主體的與個人數據處理有關的查詢、投訴和索賠。

**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.** 如果數據主體應直接向 Datasite 申請行使其個人數據權利，Datasite 在數據保護規則允許的情況下會把此請求轉發給客戶來協助客戶處理該請求，而不作不當拖延。

**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，否則如果個人數據受到公共機關的控制、命令或調查，Datasite 將：（a） 迅速通知客戶;和 （b） 僅在滿足要求的嚴格必要和相稱的範圍內，及符合數據保護規則的範圍內披露個人數據。根據客戶的要求，Datasite 將向公共機關提供有關在本補充協議下之處理的信息，並根據數據保護規則要求允許在第 7 節所述的範圍內進行檢查。

**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.** 如客戶的個人數據被認定受個人數據洩露影響，Datasite 將在不作不當拖延的情況下通知客戶。Datasite 應根據數據保護規則的要求，向客戶提供信息以合理協助客戶。

**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.** 考慮到處理和個人數據的性質，如果客戶無法獨立進行數據保護影響評估和事先諮詢，Datasite 將向客戶提供合理的協助，以根據數據保護規則進行數據保護影響評估和事先諮詢。

## 7. Customer’s Audit and Inspection Rights

## 7. 客戶的審計和檢查權利

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.

當客戶要求，並在遵守合理通知、時間、地點、頻率和方式限制以及保密要求的前提下， Datasite 應向客戶提供必要的信息， 以證明 Datasite 遵守了本補充協議和適用數據保護規則的義務。 Datasite 將允許由客戶或客戶指定的獨立第三方審計師進行的審計， 包括檢查，並為該等審計出力。在 Datasite 向其客戶普遍提供的審計報告、文檔或合規性信息無法合理地滿足客戶在本節下的權利的範圍內，則客戶應負責與此類審計相關的所有成本和費用。

## 8. Use of Subprocessors

## 8. 子處理者的使用

**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** 客戶特此確認並提供 Datasite 使用子處理者處理個人數據的一般授權。Datasite 當前的子處理者列表請見 https://www.datasite.com/us/en/legal/sub-processors.html。Datasite 應：（a） 確保任何子處理者僅為提供 Datasite 聘請他們提供的服務而處理個人數據;（b） 對任何子處理者施加保護程度不低於本補充協議項下與個人數據相關的合同義務;並且 （c） 對每個子處理者遵守此類義務承擔責任。

**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 應在其子處理者網站上提供一種機制，以讓客戶能通過提供電子郵寄地址來訂閱新子處理者的通知。 如果 Datasite 打算任命或替換本補充協議下的子處理者，Datasite 應在允許新的子處理者處理個人數據之前至少六十 （60） 天：（a） 更新其子處理者網站;（b） 向已訂閱的電子郵件提供通知;（c）就（a）和（b）為客戶提供機會以與數據保護相關的合理理由反對此類更改。如果雙方無法達成解決方案，客戶可以向 Datasite 提供書面通知以終止 SOW(s) 作為其唯一和排他性的補救措施。

## 9. Return and Deletion of Personal Data

## 9. 個人數據的歸還和刪除

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.

當客戶要求或本補充協議終止，Datasite 將（根據 SOW）歸還或銷毀所有個人數據及其副本（除非適用的數據保護規則或其他法律義務要求 Datasite 將個人數據保留更長時間）。當客戶要求，Datasite 將證明已完成此操作。

## 10. Liability

## 10. 責任

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.

在不損害數據保護規則下數據主體可獲得的權利或補救措施的情況下，雙方的責任及其限制（包括關聯公司提出的任何索賠）均應按照協議處理。

## 11. Language

## 11. 語言

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

如本補充協議英文版與中文版的內容有任何歧義，概以英文版為准。

**Customer/客戶:**

By 由:________________________________

Name 姓名: ___________________________

Title 職位:______________________________

Date 日期:______________________________

**Datasite:**

By由:___________________________________

Name姓名: _____________________________

Title職位:_______________________________

Date日期:_______________________________

## Appendix 1: Processed Personal Data and Purposes
## 附錄 1：處理的個人數據和目的

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

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

出於**以下目的**轉移和處理**個人數據**:

- 用於公司交易或內部業務目的的安全線上存儲庫和數據分享。

**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.

**處理的主題和性質：**

- 如協議中所述，Datasite 將提供安全的線上存儲庫工具以作存儲、管理、協作和分發數據和文檔之用。

**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.

**個人數據的類別：**

個人數據的類型由客戶全權自行決定和控制，其可能包括但不限於：

- 姓名、位址、 公司電子郵寄地址、公司電話號碼 、 薪酬和福利、假日和退休金信息、職位和職能以及可能包括客戶管理員上傳到網站的其他個人數據。

**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

**特殊類別的數據（如適用）：**

受限於協議中的任何適用條件，特殊類別數據的類型由客戶全權自行決定和控制，其可能包括但不限於：

- 無，除非客戶另有指明

**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.

**數據主體：**

與個人數據相關的數據主體類別由客戶全權自行決定和控制，其可能包括但不限於：

- 有關當前、過去和潛在擁有者、員工、代理、客戶、顧問、業務合作夥伴、承包商和供貨商數據主體的業務信息。

**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**:

- 當（a）客戶管理員關閉網站上的適用項目;或 （b）客戶與 Datasite 之間的協議終止後，所有個人數據將被永久刪除 。

## Appendix 2

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

## 附錄 2

## 技術和組織性措施，包括確保數據安全的技術和組織性措施

| | Security Requirement<br>安全要求 | How Datasite implements the specific information security measure<br>Datasite 如何實施具體的信息安全措施 |
|---|---|---|
| 1. | *Measures for encryption of personal data*<br>*個人數據加密措施* | 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.<br>個人數據使用行業標準加密技術進行靜態和傳輸中加密(目前使用 AES 256 位元加密措施進行靜態加密和通過傳輸層安全性 （TLS） 1.2 規格進行傳輸中加密)。該等措施應根據合理技術發展不時更新（實質措施由 Datasite 決定）。 |
| 2. | *Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and ser- vices*<br>*確保處理系統和服務的持續保密性、完整性、可用性和韌性* | 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.<br>Datasite 已通過 ISO 27001, 27701, 27017, 27018 認證，以及符合 SOC 2 Type II 標準，確保其維持和實施適當的管理、物理和技術性保護措施，以保護 客戶個人數據的完整性、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*<br>*確保在發生物理或技術性事件時及時恢復個人數據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.<br>Datasite 就每個平臺均擁有冗餘，並保存系統可用性記錄。此外，冗餘允許連續的系統備份。Datasite 具有定期審查、更新和測試的災難恢復和業務連續性計畫。 |
| 4. | *Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing*<br>*定期測試、評估和評價技術和組織性措施有效性的程式，以確保處理的安全性* | Datasite completes regular code reviews, vulnerability testing and annual penetration testing on the Website.<br>Datasite 在網站上定期完成代碼審查、漏洞測試和年度滲透測試。 |
| 5. | *Measures for user identification and authorization*<br>*用戶識別和授權措施* | 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.<br>存取由 Datasite 的存取管理標準管轄，該標準遵循基於角色的存取控制。 僅嚴格必要且唯一目的是滿足客戶指示的人員會得到個人數據的存取權。 存取管理標準要求 （a） 存取許可權應由管理層定期審查、更新和批准， 以及 （2） 存取許可權在員工解僱後 24 小時內撤回 。其他類型的相關控制措施包括在公司級別實施的密碼要求、多重身份驗證和對可移動媒體的限制。 |
| 6. | *Measures for the protection of data during transmission*<br>*傳輸過程中的數據保護措施* | 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.<br>個人數據在傳輸過程中使用行業標準加密技術進行加密(目前通過傳輸層安全（TLS）1.2 規格進行加密)。該等措施應根據合理技術發展不時更新（實質措施由 Datasite 決定）。 |
| 7. | *Measures for the protection of data during storage*<br>*存儲期間數據保護的措施* | 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.<br>個人數據使用行業標準加密技術（目前為 AES 256 位元加密）進行靜態加密。該等措施應根據合理技術發展不時更新（實質措施由 Datasite 決定）。 |
| 8. | *Measures for ensuring physical security of locations at which personal data are processed*<br>*確保個人數據處理地點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.<br>Datasite 依靠雲服務提供者來滿足其數據存儲要求。 有關 Microsoft Azure 針對其伺服器位置的物理性安全規格的信息，請訪問： https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security。所有數據中心均持有 ISO 27001：2013 和 SOC 2 第 2 類認證。至於 Datasite 的 設施， 所有辦公室都需要證件進入，並使用最近更新的、利用攝像機的視頻監控 ，且該等錄影記錄存儲在雲端。 |
| 9. | *Measures for ensuring events logging*<br>*確保事件記錄的措施* | 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.<br>Datasite 進行在其 SIEM 工具中集中收集和常規化的事件記錄和監測。記錄將保留 180 天，並且存取權乃基於角色和責任來決定。 |
| 10. | *Measures for ensuring system configuration, including default configuration*<br>*確保系統配置的措施，包括預設配置* | Datasite has standard build processes and applies CIS hardening standards.<br>Datasite 具有標準的構建流程，並應用 CIS 強化標準。 |
| 11. | *Measures for internal IT and IT security governance and management*<br>*內部 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.<br>Datasite 維持著一個強大的由 Datasite 的 PIMS 委員會管理的信息安全管理系統，其負責實施和維持穩定和安全的環境。 |
| 12. | *Measures for certification/ assurance of processes and products* | 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. |

| | | |
|---|---|---|
| | *程序和產品的認證/保證措施* | 自 2007 年以來，Datasite 一直保持著 SOC II 第 II 類認證和 ISO 27001 認證，自 2021 年起保持著 ISO 27017 和 27018 認證，自 2023 年起保持著 ISO 27701 認證。 |
| 13. | *Measures for ensuring data minimization*<br>*確保數據最小化的措施* | 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.<br>除非有必要根據服務協議和 Datasite 的政策和私隱聲明以提供服務，收集和處理的個人數據將不會被保留或使用。 |
| 14. | *Measures for ensuring data quality*<br>*確保數據品質的措施* | 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.<br>Datasite 在所有系統上都使用反惡意軟體用戶端。 上傳到網站的個人數據在平臺內發生的文檔處理活動過程中由 Datasite 的反惡意軟體軟體進行掃描。 |
| 15. | *Measures for ensuring limited data retention*<br>*確保有限數據保留的措施* | Personal Data is purged beginning 30 days post project closure or upon termination of Service Agreement.<br>個人數據將在項目結束或服務協議終止後 30 天開始清除。 |
| 16. | *Measures for ensuring accountability*<br>*確保問責制的措施* | 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.<br>記錄的所有活動都會被追蹤和是可報告的。人員每年均需完成培訓並確認遵守 Datasite 的行為準則和政策。所有人員都必須簽保密協議。 全體人員每年都須確認行為準則。 |
| 17. | *Measures for allowing data portability and ensuring erasure*<br>*允許數據可攜性和確保數據刪除的措施* | 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.<br>客戶在服務協議中定義的伺服器上寄存個人數據。當要求時，這些數據可被轉移到 Datasite 設有伺服器的其他位置。當要求時，個人數據可以通過加密的 USB 設備返還給客戶。個人數據將在項目結束或服務協議終止後 30 天開始清除。 |
| 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*<br>*對於向（子）處理者的轉移，還要描述（子）處理者採取的具體技術和組織性措施，以便能夠向控制者提供幫助，對於從處理者到子處理者的傳輸，還要描述採取的具體技術和組織性措施，以便能夠向數據輸出者提供幫助* | 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.<br>Datasite 設有供應商安全標準，其詳細說明了存儲、處理或傳輸個人數據所需的最低供應商安全標準，該標準為根據供應商關係的性質評估每個供應商、符合性和風險接受提供了期望的控制措施的基線。範圍內的每個供應商都需要簽署合同 （DPA SCCs），以確保其對 Datasite 負有 Datasite 對客戶相同級別保護的義務。 |

## 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.

# Annex 1
# 附件一

## A. LIST OF PARTIES

## A. 締約方名單

***Data exporter:***
***數據輸出者：***

**Name:** Customer as defined by the SOW, unless otherwise identified herein:
**名稱：**SOW所定義的客戶，除非本文另有說明：

**Address:**
**地址：**

**Contact person's name, position and contact details:**

**聯繫人的姓名、職位和聯繫方式：**

**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.
**與根據這些條款轉移的數據相關的活動：**數據輸出者根據數據輸出者及數據輸入者之間的服務協議（"服務協議"），使用基於 SaaS 的電子安全網上存儲庫工具（"網站"）以存儲、管理、協作和分發數據和文檔（"內容"）（"服務"）。數據輸入者將內容存儲在歐盟、美國和澳大利亞境內的第三方服務器上，以向數據輸出者提供網站並託管其內容。這些內容雖然未經實質性評估，但可能包含個人數據。網站的內容仍然存儲在這些服務器上，但可以從數據輸入者的人員那裡存取，以提供附錄1中進一步描述的服務。

**Role:** Controller
**角色**：控制者

***Data importer:***

***數據輸入者：***

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

**名稱：**Datasite LLC，一家在美國特拉華州註冊的有限責任公司，及其範圍內的**關聯公司**

**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

**聯繫人的姓名、職位和聯繫方式：**Patricia Elias，董事、秘書兼數據保護官，patricia.elias@datasite.com，651 632 4042

**Activities relevant to the data transferred under these Clauses:**

**與根據這些條款轉移的數據相關的活動：**

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.

數據輸入者向數據輸出者提供網站，以在歐盟、美國或澳大利亞的第三方服務器上託管數據輸出者的內容。這些內容雖然未經實質性評估，但可能包含個人數據。內容仍存儲在那些服務器上，但可以從數據輸入者的人員那裡存取，以便提供附錄 1 中進一步描述的服務。

**Role**: Processor
角色：處理者

## B. DESCRIPTION OF TRANSFER

## B. 轉讓的說明

**See Appendix 1 of the DPA**

**見DPA的附錄1**

## C. COMPETENT SUPERVISORY AUTHORITY

## C. 主管監督機構

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

  *德國聯邦數據保護和信息自由專員*

# Annex 2
# 附件二

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
## 技術和組織性措施，包括確保數據安全的技術和組織性措施

**See Appendix 2 of the DPA**

見**DPA**的附錄**2**

# APPENDIX 4
# 附錄4
# INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES
# 歐盟委員會標準合同條款的國際數據轉移補充協議

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**補充協議**由**信息專員**為進行**受限轉移**的**各方**發布。**信息專員**認為，在作為具有法律約束力的合同簽訂時，其為**受限轉移**提供了**適當保障措施**。

## Part 1: Tables

## 第 1 部分：表格

### Table 1: PARTIES AND SIGNATURE
### 表格 1：締約方和簽署

Customer as defined by the SOW, unless otherwise identified herein:
SOW所定義的客戶，除非本文另有說明：

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

*簽署本補充協議所附的數據處理協議（“DPA”）即視為簽署本英國附錄*

hereinafter the ‘**Exporter**;’ and

以下簡稱“**輸出者**”，及

Datasite LLC, a limited liability company registered in Delaware, USA, and its in-scope Affiliates
Datasite LLC，一家在美國特拉華州註冊的有限責任公司，及其範圍內的關聯公司

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

*主要聯繫人*：Patricia Elias，董事、秘書兼數據保護官，patricia.elias@datasite.com，651 632 4042
*Execution of the DPA which this Addendum is appended to is deemed execution of this UK Addendum*

*簽署本補充協議所附的數據處理協議（“DPA”）即視為簽署本英國附錄*

hereinafter the **‘Importer.’**

以下簡稱“**輸入者**”。

### Table 2: Selected SCCs, Modules and Selected Clauses

### 表格 2：選定的 SCC、模組和選定的條款

Addendum EU SCCs:

歐盟 SCCs附錄：

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”)

根據不時更新、修訂、替換或取代的，由2021 年 6 月 4 日的歐盟委員會作出的委員會實施決定 (EU) 2021/914採納的歐洲議會和理事會 2016 年 4 月 27 日的2016/679條例 (EU)項下關於將個人數據轉移至在第

三國的處理者的控制者到處理者（模組 2）標準合同條款（“歐盟 SCCs”）

Date: Effective Date of the Agreement

日期：協議生效日期

Reference: None

參考：無

**Table 3: Appendix Information**
**表格 3：附錄信息**

“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:

“附錄信息”是指必須為經批准的歐盟 SCCs（締約方除外）的附錄中列出的選定模組所提供的信息。對於本補充協議，這些信息列於：

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

附件 1A：締約方名單：參見經批准的歐盟 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：轉移說明：參見經批准的歐盟 SCC’s 附件 1 的 B 部分

Annex II: See Appendix 2 of the DPA
附件二：見 DPA 附錄 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：在批准的附錄改變時終止本補充協議**

Ending this Addendum when the Approved Addendum changes:

在批准的附錄改變時結束本補充協議：

Which Parties may end this Addendum as set out in Section 19: Importer and Exporter
哪些締約方可以按照第 19 節的規定終止本補充協議：輸入者和輸出者

**Part 2: Mandatory Clauses**
**第 2 部分：強制性條款**

Mandatory Clauses:
強制性條款：

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：已批准附錄的強制性條款，即 ICO 發布的、於 2022 年 2 月 2 日根據 2018 年數據保護法第 119A 條提交議會並根據這些強制性條款的第 18 條進行了修訂的模板附錄 B.1.0。