データ処理に関する補遺

このデータ処理に関する補遺（以下、「補遺」）は、以下の当事者間で交わされるものです。

お客様及び SOW で定義されるその関連会社：

– 以下、**「お客様」**といいます。

および

SOW で定義された Datasite の事業体：

– 以下、**「Datasite」**といいます。

以下、それぞれを**「当事者」**といい、総称して**「両当事者」**といいます。

前文：

(A) 両当事者は、提供されるサービスの概要を記した本契約を締結しました（定義は下記第 1 条に記載）。Datasite によるサービス提供の一環として、お客様から Datasite へ個人データが転送されることがあります。

(B) 本補遺に定義されていない大文字の用語は、本契約に定義されています。 本補遺の規定と本契約に定める規定との間に矛盾がある場合には、本補遺の規定または条項が優先するものとします。

(C) 両当事者がデータ保護規則（随時改正される）に基づく処理義務を確実に遵守するために、両当事者はここに以下の通り合意します。

1. 定義

1.1.「本契約」とは、お客様と Datasite との間で交わされる作業明細書および適用される一般取引条件を意味します。

1.2.「別紙」とは、本補遺に添付され、本補遺と一体を成す付属資料を意味します。

1.3.「ビジネス運営」とは、(1) 請求、支払い、アカウント管理、(2) ダイレクトマーケティングの目的 、(3) 内部報告およびビジネスモデル（予測、収益、キャパシティ計画、製品戦略など）、(4) 新製品およびサービスの改善と開発、(5) Datasite または Datasite 製品に影響を及ぼす可能性のある詐欺、サイバー犯罪、サイバー攻撃への対処、(6) ウェブサイトの中核機能、アクセシビリティ、またはプライバシーの改善、(7) 財務報告および法的義務の遵守を意味します。

1.4.「管理者」とは、個人データの処理の目的および手段を決定する事業者をいいます。

1.5.「データ保護規則」とは、個人データの処理に適用される関連国内法を意味し、日本の個人情報保護法、欧州データ保護法、米国データ保護法、およびオーストラリアプライバシー原則（該当する場合）を含むがこれに限定されません。

1.6.「データ対象者」とは、その個人データが処理の対象となる、特定または識別可能な自然人を意味します。識別可能な人とは、名前、識別番号、位置情報、オンライン識別子などの識別子、または身体的、生理的、遺伝的、精神的、経済的、文化的、社会的アイデンティティに特有の 1 以上の要素を参照して、直接的または間接的に識別できる人、または適用されるデータ保護規則で別途定義される人を意味します。

1.7.「欧州データ保護法」とは、GDPR およびスイスデータ保護法を総称したものを意味します。

1.8.「GDPR」とは、英国 GDPR および EU の一般データ保護規則 2016/679 を意味します。

1.9.「国際データ移転協定」または**「IDTA」**とは、英国 GDPR 第 46 条および第 5 章に基づき、第三国に設立された処理業者への個人データの移転に関する国際データ移転協定を意味します。

1.10.「個人データ」とは、コンテンツに含まれるデータ対象者に関するあらゆる情報を意味します。

1.11.「個人データの侵害」とは、送信、保存、その他の処理を行った個人データの偶発的または違法な破壊、損失、改ざん、不正な開示、またはそれへのアクセスにつながるセキュリティ違反、または適用されるデータ保護規則で別途定義されるものを指します。

1.12.「処理」とは、収集、記録、整理、構造化、保存、適応または変更、検索、相談、使用、送信による開示、普及またはその他の利用可能化、整合または組み合わせ、ブロック、消去または破壊など、自動的な手段であるかどうかにかかわらず、個人データに対して行われるあらゆる操作または一連の操作を意味し、または適用あるデータ保

護規則で別途定義されているものを指します。

1.13. **「処理者」**とは、管理者に代わって個人データを処理する事業者をいいます。

1.14. **「サービス」**とは、本契約および本補遺に記載されたサービスの提供を意味します。

1.15. **「特別なカテゴリのデータ」**とは、人種または民族的出身、政治的意見、宗教的または哲学的信条、労働組合への加盟、遺伝情報、自然人を一意に特定する目的で処理される生体情報、健康、性生活または性的指向に関する個人データ、または適用されるデータ保護規則で別途定義されている個人データを指します。

1.16. **「標準契約条項」**または **「SCC」**とは、GDPR/スイスデータ保護法の適用を受けない事業者への個人データの移転に関する、GDPR およびスイスデータ保護法の要件に沿った、管理者と処理者（モジュール 2）との間の標準契約条項 を意味します。

1.17. **「サブ処理者」**とは、管理者の代理として個人データを処理するために処理者が従事する事業者を意味します。

1.18. **「スイスデータ保護法」**とは、1992 年 6 月 19 日付データ保護に関するスイス連邦法（SR235.1）ならびに条例 SR235.11 および SR235.13 を意味し、2020 年 9 月 25 日付で改正され 2023 年 1 月 1 日（または立法手続に従ってより遅い日）付で施行される改正版を含み、それらが個人データの処理に適用される限り、適宜改正、置換、または優先される改正版を含みます。

1.19. **「英国 GDPR」**とは、2018 年データ保護法の 3(10)、205(4)および一般処理規定を意味し、随時更新、修正、置換、または優先される改正版を含みます。

1.20. **「米国データ保護法」**とは、個人データおよびサービスの提供に適用される限りにおいて、発効後に、カリフォルニア州消費者プライバシー法（および発効後はカリフォルニア州プライバシー権法）、Cal. Civ. Code § 1798.100 *et seq.*、および随時制定され個人データに適用されるその他の実質的に類似した米国法を意味します。

2. 処理活動

2.1. お客様および Datasite は、以下のことに同意します。(a) お客様は個人データの管理者であり、Datasite はそのデータの処理者です。ただし、お客様が第三者の管理者（「第三者管理者」）に代わって個人データの処理者として行動する場合は、Datasite はサブ処理者であるものとします。 (b) 本補遺は、Datasite がサービスを提供する過程で処理者またはサブ処理者としてお客様に代わって個人データを処理する場合にのみ適用されます。

2.2. お客様は、以下のことに同意するものとします。(a) Datasite が本契約に従って個人データを合法的に処理するために、お客様が、データ保護規則に基づいて必要なすべての関連する同意、またはその他の合法的な法的根拠（該当する場合）、許可および権利を確実に取得し、関連する通知をすべて提供したこと。(b) お客様は、適用されるデータ保護規則を遵守するものとし、その関連会社および招待ユーザーによる遵守に責任を負うこと。また、 (c) Datasite に対する処理の指示が、データ保護規則および第三者管理者（該当する場合）からのすべての指示と一致していること。

2.3. Datasite は、以下の内容に従って個人データを処理することに同意します。(a) 本補遺および本契約、(b) 本補遺の別紙 1 に記載されているお客様の書面による指示、および (c) データ保護規則に基づいて要求される場合、お客様から随時通知される内容。追加で要求された指示には、Datasite の事前の書面による同意が必要です。

2.4. フィードバック、使用データ、またはユーザーデータ（本項の目的でのみ総称して「データ」）が、特定または識別可能な人物に関連する限り、両当事者は、Datasite が、(a) 当該データに関して独立した「管理者」および/または「ビジネス」（データ保護規則で定義される）として行動し、かつ (b) 当該データをそのビジネス運営のためにのみ、適用されるすべてのデータ保護規則を遵守して処理することに合意するものとします。Datasite が独立した「管理者」および/または「ビジネス」（データ保護規則で定義される）として Datasite のビジネス運営のために合法的にデータを処理するために、お客様は、データ保護規則に基づいて必要なすべての同意、許可、権利を取得し、すべての関連通知を提供したことに同意するものとします。

2.5. Datasite が、ある指示がデータ保護規則に違反すると考える場合、不当に遅延することなくお客様に通知します。お客様が処理者として行動する場合、お客様は、その第三者管理者への必要とされる通知、支援または承認について責任を負うものとします。Datasite は、サービスプロバイダとして行動する場合、サービスの対価（米国データ保護法で定義される用語）として個人データを受け取らないことを認めます。

3. 本補遺の存続と終了

3.1. 本補遺は、発効日に発効し、本契約の期間中有効であるものとします。本補遺は、いずれかの SOW の終了

または失効により自動的に終了するものとします。

3.2. 本補遺の終了にかかわらず、Datasite は、引き続き機密保持の義務に拘束されるものとします。

4. 国際移転

すべての個人データは、米国、欧州経済領域（「EEA」）、またはオーストラリア内の第三者ホスティング施設に保管されます。お客様は、Datasite が、Datasite またはそのサブ処理者が事業を行う国に個人データを移転する可能性があることを認めるものとします。適用される国内当局によって発行された妥当性決定に基づいて移転される場合を除き、英国、EEA およびスイスからの個人データの移転はすべて、本補遺に組み込まれた SCCs（別紙 3）および IDTA（別紙 4）に基づいて行われるものとします。Datasite は、EEA、英国、スイスからの個人データの収集、使用、移転、保持、およびその他の処理に関して、欧州データ保護法を遵守するものとし、日本からの個人データに関しては日本の個人情報保護法を遵守するものとします。

5. 機密保持とセキュリティ

5.1. Datasite は、 (a) 個人データの機密を保持し、(b) 個人データを処理する従業員に、機密保持を約束させ、または適切な法的機密保持義務を負わせるものとします。

5.2. データ保護規則に従い、Datasite は、偶発的または違法な破壊、紛失、改ざん、不正な開示またはアクセスから個人データを保護するために、別紙 2 に記載するとおり適切な運用、技術および組織的措置を実施します。

5.3. お客様は、Datasite が導入した技術的および組織的措置が、適用されるデータ保護規則に基づくセキュリティ義務を含むお客様の要求を満たしているかどうかについて、独自の判断を下すことに単独で責任を負うものとします。お客様は、（最新技術、導入コスト、個人データ処理の性質、範囲、文脈および目的、ならびにデータ対象者に対するリスクを考慮した上で）Datasite が実施および維持するセキュリティ慣行およびポリシーが、個人データに関するリスクに適したレベルのセキュリティを提供することを認め、同意するものとします。

5.4. Datasite は、技術的および組織的なセキュリティ対策を、Datasite が判断する合理的な技術開発に合わせて更新します。

6. 協力・通知義務

6.1. 両当事者は、政府当局またはデータ対象者からの個人データの処理に関する照会、苦情およびクレームを迅速かつ効果的に処理するために相互に協力するものとします。

6.2. データ対象者が自身の個人データの権利を行使するために Datasite に直接申請する場合、Datasite は、データ保護規則で認められていれば、この要求を不当に遅滞することなくお客様に転送することにより、その要求に関してお客様を支援します。

6.3. 法令で禁止されている場合を除き、個人データが公的機関の管理、命令、調査の対象となった場合、Datasite は、(a) お客様に速やかに通知し、(b) 要求を満たすために厳密に必要かつ適切な範囲に限り、データ保護規則を遵守して個人データを開示するものとします。Datasite は、お客様の要求があれば、本補遺に基づく処理に関する情報を公的機関に提供し、データ保護規則の要求に従い、第 7 条に記載された範囲内で検査を許可するものとします。

6.4. Datasite は、お客様の個人データに影響を及ぼすと判断される個人データの侵害が発生した場合、お客様に不当に遅滞することなく通知します。Datasite は、データ保護規則の定めるところにより、お客様を合理的に支援するための情報を提供するものとします。

6.5. データ処理および個人データの性質を考慮し、データ保護規則に基づくデータ保護影響評価および事前協議をお客様が独自に実施できない範囲において、Datasite はお客様に対してこれらを行うための合理的な支援を提供するものとします。

7. お客様の監査権・検査権

お客様の要求があれば、合理的な通知、時間、場所、頻度、方法である限り、機密保持の要件に従って、Datasite は、本補遺および適用されるデータ保護規則に基づく Datasite の義務の遵守を証明するために必要な情報をお客様に提供するものとします。Datasite は、お客様またはお客様が指名した独立した第三者の監査人が実施する検査を含む監査を許可し、これに貢献するものとします。本条に基づくお客様の権利が、監査報告書、文書、または Datasite がその顧客に一般に提供するコンプライアンス情報によって合理的に満たされない限り、お客様はかかる監査に関連するすべての費用および手数料を負担するものとします。

8. サブ処理者の使用

8.1 お客様は、Datasite がサブ処理者を使用して個人データを処理することを承認し、一般的な権限を与えるものとします。Datasite の現在のサブ処理者一覧は、https://www.datasite.com/us/en/legal/sub-processors.html で確認できます。Datasite は、 (a) サブ処理者が個人データを処理するのは、Datasite が委託したサービスを提供するためのみであることを確認し、(b) サブ処理者に対して個人データに関する契約上の義務を本補遺に劣らない程度に課し、かつ (c) サブ処理者がかかる義務を遵守することに対して責任を持つものとします。

8.2 Datasite は、お客様が電子メールアドレスを提供することにより、新しいサブ処理者に関する通知を受け取ることができる仕組みを、サブ処理者のサイトで提供するものとします。Datasite が本補遺の対象となるサブ処理者を任命または交換する場合、新しいサブ処理者に個人情報の処理を許可する少なくとも 60 日前に、Datasite は(a) サブ処理者のサイトを更新し、(b) 登録された電子メールに通知を行い、(c) (a) および (b) の両方に関して、データ保護に関する合理的な根拠に基づいてかかる変更に反対する機会をお客様に提供するものとします。両当事者が解決できない場合、お客様は、唯一かつ排他的な救済措置として、SOW を終了する書面通知を Datasite に提供することができます。

9. 個人情報の返却・削除について

お客様の要求があった場合、または本補遺が終了した場合、適用されるデータ保護規則またはその他の法的義務により Datasite が個人データをより長く保持する義務を負わない限り、Datasite はすべての個人データおよびそのコピーを（SOW に従って）返却または破棄するものとします。お客様の要求があれば、Datasite はこれが行われたことを証明します。

10. 責任

データ保護規則の下でデータ対象者が利用できる権利または救済を害することなく、両当事者の責任およびその制限は、その関連会社が提起する請求を含めて、本契約に従うものとします。

お客様:	**Datasite:**
By:_____	By:_____
Name: _____	Name: _____
Title:_____	Title:_____
Date:_____	Date:_____

別紙 1：処理される個人データと目的

個人データは、**以下の目的**のために転送され、処理されます。

- 企業間取引や社内業務のために、安全なオンラインリポジトリとデータ共有を実現します。

処理の対象および性質

- 本契約に記載されているように、Datasite は、データや文書の保存、管理、共同作業、配布のための安全なオンラインリポジトリツールを提供しています。

個人データのカテゴリ

個人データの種類は、お客様が独自の裁量で決定し管理するものであり、以下を含みますが、これに限定されません。

- 氏名、住所、会社の電子メールアドレス、会社の電話番号、報酬および手当、休日および年金情報、役職および機能、ならびにお客様管理者がウェブサイトにアップロードしたその他の種類の個人データ。

特別なカテゴリのデータ（該当する場合）

本契約の適用条件に従い、特別なカテゴリのデータの種類は、お客様が独自の裁量で決定し管理するものであり、以下を含みますがこれに限定されません。

- お客様から特に指定がない限り、なし。

データ対象者

個人データが関連するデータ対象者のカテゴリは、お客様が独自の裁量で決定し管理するものであり、以下を含みますが、これに限定されません。

- 現在、過去、および将来の所有者、従業員、代理人、顧客、アドバイザー、ビジネスパートナー、請負業者およびベンダーのデータ対象者に関するビジネス情報。

保持

- (a) お客様管理者がウェブサイト上の該当するプロジェクトを閉鎖した場合、または (b) お客様と Datasite の間の本契約が終了した場合、すべての個人データは永久に削除されます。

別紙 2

データの安全性を確保するための技術的・組織的な措置を含む、技術的・組織的な措置

	セキュリティ要件	Datasite が具体的にどのような情報セキュリティ対策を実施しているか
1.	*個人データの暗号化に関する措置*	個人データは、保存時および転送時に業界標準の暗号化技術を使用して暗号化されます。現在、保存時には AES 256 ビット暗号を使用し、転送時には Transport Layer Security (TLS) 1.2 プロトコルを使用していますが、Datasite が決定する合理的な技術開発に合わせて適宜更新されるものとします。
2.	*処理システムおよびサービスの継続的な機密性、完全性、可用性、および弾力性を確保するための措置*	Datasite は、ISO 27001, 27701, 27017, 27018 の認証を受け、SOC 2 Type II に準拠しており、お客様の個人データの完全性、可用性、機密性を保護するための適切な管理、物理、技術的セーフガードを維持、実施していることを保証します。
3.	*物理的または技術的な事故が発生した場合に、個人データへの可用性およびアクセスを適時に回復する能力を確保するための措置。*	Datasite では、各プラットフォームを冗長化し、システムの稼働状況のログを管理しています。また、冗長性により、システムの継続的なバックアップが可能です。Datasite は、災害復旧計画および事業継続計画を策定し、定期的に見直し、更新、テストを行っています。
4.	*処理の安全性を確保するために、技術的及び組織的な措置の有効性を定期的にテストし、評価するためのプロセス*	Datasite は、ウェブサイトで定期的なコードレビュー、脆弱性テスト、年 1 回の侵入テストを行っています。
5.	*ユーザーの識別と認証のための措置*	アクセスは、ロールベースのアクセスコントロールに従った Datasite のアクセス管理基準によって管理されます。個人データへのアクセスは、お客様の指示を満たすという唯一の目的のために厳密に必要な人員にのみ提供されます。アクセス管理基準では、（a）アクセス権は定期的に見直され、更新され、管理者によって承認されること、（b）アクセス権は従業員の退職後 24 時間以内に撤回されることが要求されています。その他の関連する管理としては、パスワードの要求、多要素認証、リムーバブルメディアの制限などがあり、これらは企業レベルで実施されています。
6.	*送信時のデータ保護措置*	個人データは、業界標準の暗号化技術（現在は TLS 1.2 プロトコル）を使用して暗号化されて転送されますが、この技術は Datasite が決定する合理的な技術開発に合わせて随時更新されます。
7.	*保管中のデータ保護措置*	個人データは、業界標準の暗号化技術（現在は AES 256 ビット暗号）を使用して暗号化されて保管されますが、この技術は、Datasite が決定する合理的な技術開発に合わせて随時更新されます。

8.	*個人データが処理される場所の物理的な安全性を確保するための措置*	Datasite は、データストレージの要件について、クラウドサービスプロバイダーに依存しています。 Microsoft Azure のサーバーロケーションの物理的セキュリティプロトコルに関する情報は、https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-securit で入手可能です。すべてのデータセンターは、ISO 27001:2013 および SOC 2 Type 2 の認証を取得しています。Datasite の施設に関しては、すべてのオフィスでバッジアクセスが義務付けられており、クラウドに保存された録画カメラによる最新のビデオ監視を使用しています。
9.	*イベントロギングを確実に行うための措置*	Datasite は、SIEM ツール内で一元的に収集・正規化されたログと監視を実行します。ログは 180 日間保持され、アクセスは役割と責任に基づいて行われます。
10.	*デフォルトコンフィグレーションを含む、システムコンフィグレーションの確保のための措置*	Datasite は標準的なビルドプロセスを持ち、CIS のハードニング標準を適用しています。
11.	*社内の IT ならびに IT セキュリティガバナンスおよびマネジメントのための措置*	Datasite は、安定した安全な環境を実施・維持するために、Datasite の PIMS 委員会が管理する強固な情報セキュリティ管理システムを維持しています。
12.	*プロセスおよび製品の認証・保証のための措置*	Datasite は、2007 年以来、SOC II Type II 認証および ISO 27001 認証を維持しています 2021 年から ISO 27017 と 27018、2023 年から ISO 27701 の認証を維持しています。
13.	*データの最小化を確保するための措置*	収集および処理された個人データは、サービス契約、Datasite のポリシーおよびプライバシーに関する通知に従ってサービスを提供するために必要な場合を除き、保有または使用されることはありません。
14.	*データ品質確保のための措置*	Datasite は、すべてのシステムでマルウェア対策用クライアントを使用しています。ウェブサイトにアップロードされた個人データは、プラットフォーム内で行われる文書処理アクティビティの一環として、Datasite のアンチマルウェア・ソフトウェアによってスキャンされます。
15.	*限定的なデータ保持を確保するための措置*	個人データは、プロジェクト終了後 30 日またはサービス契約終了時に消去されます。
16.	*説明責任を果たすための措置*	記録されたすべての活動は追跡され、報告可能です。従業員は、毎年トレーニングを受け、Datasite の行動規範とポリシーを遵守していることを確認します。すべての従業員は、NDA に署名する必要があります。行動規範は、毎年全従業員によって確認されます。
17.	*データポータビリティおよび消去の確保のための措置*	お客様は、サービス契約に定義されたサーバーで個人データをホストしており、ご要望に応じて、Datasite がサーバーを維持する他の場所に転送することができます。個人データは、要求に応じて、暗号化された USB デバイスで顧客に返却することができます。個人データの削除は、プロジェクトの終了またはサービス契約の終了から 30 日以内に行います。

18.	*（サブ）処理者への移転の場合、管理者に支援を提供できるようにするために、（サブ）処理者が取るべき特定の技術的及び組織的措置についても記述すること。処理者からサブ処理者への移転の場合は、データ輸出業者についても記述すること。*	Datasite は、個人データの保存、処理、送信に必要なベンダーの最低セキュリティ基準を詳述するベンダーセキュリティ基準を維持します。この基準は、ベンダーとの関係の性質に基づき、各ベンダーの評価、適合性、リスク受容のために期待される管理の基本水準を提供するものです。各ベンダーは、Datasite がお客様に対して負う義務と同レベルの保護を保証する契約（DPA SCCs）に署名することが義務付けられています。

別紙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**

9 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.

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

10.1 **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.

10.2 **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.

10.3 **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.

10.4 **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).

10.5 **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.

10.6 **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.

10.7 **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.

10.8 **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.

(i) 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.

15.1 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

A. 当事者一覧

データ輸出者:

名称：SOW で定義されるお客様（ただし、本書にて別途定められている場合を除く）

住所：

担当者の氏名、肩書及び連絡先：

本条項に基づいて移転されるデータに関連する活動：データ輸出者は、データ輸出者およびデータ輸入者の間のサービス契約（以下、「サービス契約」）に従って、データおよびドキュメント （以下、「コンテンツ」）を保存、管理、コラボレーション、および配布するために、SaaS ベースの電子的に安全なオンライン・リポジトリ・ツール（以下、「ウェブサイト」） を使用する（以下、「サービス」）。データ輸入者は、EU、米国、およびオーストラリア内の第三者サーバーにコンテンツを保存して、データ輸出者にウェブサイトを提供し、コンテンツをホストする。コンテンツは、その内容について評価されていないが、個人データを含む場合がある。ウェブサイトのコンテンツはこれらのサーバーに保存されたままになるが、別紙1に記載されるサービスを提供する目的でデータ輸入者の担当者がアクセスする可能性がある。

役割：管理者

データ輸入者：

名称：Datasite LLC（米国デラウェア州にて有限責任会社として登録）およびその範囲内の関連会社

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

担当者の氏名、肩書及び連絡先： Patricia Elias, Director, Secretary and Data Protection Officer, patricia.elias@datasite.com, 651 632 4042

本条項に基づいて移転されるデータに関連する活動：

データ輸入者は、EU、米国、またはオーストラリア内の第三者サーバーでデータ輸出者のコンテンツをホストするために、データ輸出者にウェブサイトを提供する。コンテンツは、その内容については評価されていないが、個人データを含む場合がある。コンテンツはこれらのサーバーに保存されたままになるが、別紙 1に記載されるサービスを提供する目的でデータ輸入者の担当者がアクセスする場合がある。

役割：処理者

B. 移転の詳細

データ処理に関する補遺別紙1を参照のこと。

C. 管轄当局

- ***Germany Federal Commissioner for Data Protection and Freedom of Information（データ保護と情報の自由のためのドイツ連邦コミッショナー）***

Annex 2

データのセキュリティを確保するための技術的および組織的措置を含む技術的および組織的措置

データ処理に関する補遺別紙2を参照のこと。

別紙4

欧州委員会標準契約条項に付加する国際データ移転に関する補遺

本補遺は、制限付き移転を行う当事者のための情報コミッショナーによって発行されました。 情報コミッショナーは、法的拘束力のある契約として締結された場合、制限付き移転に適切な保護手段を提供するものとみなします。

パート1：表
表1: 当事者及び署名
SOW で定義されるお客様（ただし、本書にて別途定められている場合を除く）

本補遺が添付されているデータ処理契約 (以下、「DPA」) の締結は、この英国の補遺の締結とみなされる。

以下、「**輸出者**」。

Datasite LLC（米国デラウェア州にて有限責任会社として登録）およびその範囲内の関連会社

主要な連絡先： Patricia Elias, Director, Secretary and Data Protection Officer, patricia.elias@datasite.com, 651 632 4042
本補遺が添付されているDPAの締結は、この英国の補遺の締結とみなされる。

以下、「**輸入者**」。

表2：選択されたSCCs、モジュール、条項

EU SCCs の補遺：

Controller to Processor (Module 2) standard contractual clauses for the transfer of Personal Data to Processors（処理者への個人データの移転に関する、管理者から処理者（モジュール2）への標準契約条項）（2016 年 4 月 27 日付欧州議会および理事会の EU規則2016/679に基づいて第三国に設立され、2021 年 6 月 4 日付欧州委員会の委員会実施決定2021/914により採択され、随時更新、修正、置換、または置き換えられるもの）（以下、「EU SCCs」）

日付：本契約の発効日

リファレンス：特になし

表3: 別紙情報

「別紙情報」とは、承認された EU SCCs（当事者を除く）の別紙に記載されているとおり、選択されたモジュールに対して提供する必要がある情報を意味し、本別紙については以下のとおり。

Annex 1A: 当事者一覧：承認された EU SCCs のAnnex 1, Part Aを参照のこと。

Annex 1B: 移転の詳細：承認された EU SCCs のAnnex 1, Part Bを参照のこと。

Annex II: データ処理に関する補遺の別紙2を参照のこと。

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

表4: 承認された補遺が変更された場合、本補遺が終了するか否か

承認された補遺が変更された場合、本補遺が終了するか否か：

第19条（輸入者および輸出者）に規定されているように、両当事者は、本補遺を終了することができる。

パート2：必須条項

必須条項：

パート 2：承認された補遺の必須条項（ICO によって発行され、2022 年 2 月 2 日にデータ保護法 2018 の s119A に従って議会に提出されたテンプレート補遺 B.1.0）（当該必須条項のもとで改訂されたもの）