Data Protection Requirements

**Purpose**: This Exhibit establishes minimum information security standards and related requirements for vendor identified in the relevant Agreement ("**Vendor**") in connection with its performance of services for We Work Management LLC or the applicable affiliate of We Work Management LLC identified in the Agreement ("**WeWork**") or to the extent it otherwise has access to Covered Data (defined below).

**Scope**: Vendor must handle, treat, and otherwise protect WeWork data in accordance with this Data Protection Exhibit, and any schedules and annexes attached hereto ("**Exhibit**"), and any contractual agreement between such WeWork and Vendor.

## 1. Definitions

a. "**Agreement**" means the Master Services Agreement or other service order, statement of work, authorization letter, or other written communication or electronic information entered into between Vendor and WeWork, or otherwise issued by WeWork and delivered to Vendor for the Services.

b. "**Applicable Law**" means all applicable government-issued laws, rules, regulations and guidance pertaining to privacy, data Processing, data protection, data security, encryption, or confidentiality; with respect to EU originating Personal Data that Vendor Processes, all references to "Applicable Law" shall be deemed to refer to Union or Member State law.

c. "**Controller**" shall have the same meaning as in the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), as may be amended from time to time.

d. "**Covered Data**" means in any form, format or media, whether provided by WeWork or otherwise accessed by Vendor in connection with its performance under the Agreement, all confidential information under the Agreement and Personal Data that Vendor Processes in connection with the Agreement.

e. "**Data Security Breach**" means, in connection with the Services, (i) the unauthorized and/or unlawful disclosure, access, acquisition, alteration, corruption, destruction, use or other Processing of or to Covered Data; or (ii) any other act or omission that compromises or may compromise the security, confidentiality, or integrity of Covered Data or the Systems.

f. "**Individual**" means any natural person from whom or about whom Personal Data is Processed in connection with the Services.

g. "**Personal Data**" means any information relating to an identified or identifiable natural person, including without limitation: a person's first and last name, home or other physical address, telephone number, fax number, email address or other online identifier, photographs, third-party issued identifier, biometric data, health information, credit card or other financial information, IP address and cookie information, and any other device-specific number or identifier.

h. "**Processing**" (including its cognate, "Process") means any operation or set of operations that is performed upon Covered Data, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction.

i. "**Services**" means those services, including without limitation Processing, that Vendor performs for or on behalf of Vendor pursuant to the Agreement.

j. "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2 to the Agreement, as may be amended pursuant to Section 10 of this Exhibit.

k. "**Systems**" means and all WeWork systems, software, facilities, or platforms that Vendor accesses in connection with its performance under the Agreement.

l. "**Vendor Parties**" means Vendor employees, subcontractors, and agents.

**2. <u>Privacy</u>**

a. Vendor, and the Vendor Parties, will Process Covered Data solely for the purpose of providing the Services to WeWork, and solely to the extent necessary to provide the Services to WeWork, in each case, in a manner in accordance with this Agreement and Applicable Law. Vendor acknowledges that a WeWork entity is the Controller of all Personal Data, and WeWork, on behalf of the applicable WeWork entity, will direct Vendor and the Vendor Parties in connection with the Processing of Personal Data. Vendor will only Process Personal Data in accordance with WeWork's documented instructions, unless Processing is required by Applicable Law to which Vendor is subject, in which case Vendor shall, to the extent permitted by Applicable Law, inform WeWork of that legal requirement before the relevant Processing of that Personal Data. WeWork reserves the right to submit further written instructions with regard to the processing of Personal Data from time to time after execution of the Agreement and for the duration of the term. Vendor shall immediately inform WeWork if Vendor is of the opinion that an instruction of WeWork regarding Processing Personal Data infringes the GDPR or other European Union or Member State data protection laws.

b. Vendor represents and warrants that Vendor Parties are subject to suitable confidentiality obligations in respect of the Covered Data.

c. Without limitation to the foregoing, Vendor represents and warrants that it and the Vendor Parties (1) will not, directly or indirectly, sell, rent, distribute, commercially exploit or transfer any Covered Data to any third party for any purpose whatsoever; (2) will not, directly or indirectly, collect, access, store, copy, modify, create derivative works of, disclose, or otherwise Process Covered Data except as specified in the Agreement or an applicable statement of work, work order, or similar instrument and, at all times, in accordance with this Exhibit; and (3) will preserve the integrity and accuracy of Personal Data.

d. Without limitation to any other obligation, Vendor will maintain the confidentiality of the Covered Data and will not disclose the Covered Data to third parties (including non-employee Vendor Parties) unless such disclosure is:

i. necessary to perform the Services for WeWork and Vendor has received WeWork's prior written approval (which will not be unreasonably withheld or delayed) provided that if such disclosure is necessary to perform the Services for WeWork and is to an agent or subcontractor which, prior to such disclosure, has agreed by written contract to be bound by obligations that are the same or equivalent to the obligations applicable to Covered Data as contained in this Agreement and as otherwise required by Applicable Law, and undergone a thorough assessment for compliance with these obligations conducted by Vendor and agreed to be assessed periodically by Vendor. Vendor shall make available to WeWork a current list of agents and subcontractors and shall inform WeWork of any intended changes concerning the addition or replacement of an agent or subcontractor; if WeWork objects to Vendor's change of agent or subcontractor, WeWork shall notify Vendor of its objections in writing within ten (10) business days of receipt of information about the change from Vendor and shall be entitled to terminate the Agreement with immediate effect and without cost in the event Vendor does not take into consideration WeWork's objections, and, prior to any such disclosure, Vendor enters into a written, valid and enforceable agreement with such third party that includes terms that are the same or equivalent to the obligations applicable to Covered Data as contained in this Agreement and as otherwise required by Applicable Law; or

ii. required by Applicable Law, in which case Vendor shall notify WeWork promptly in writing before complying with any such disclosure request unless, in relation to EU-originating Personal Data, Applicable Law prohibits such information on important grounds of public interest.

e. For disclosures that are permitted under Section(2)(d), Vendor will (i) use its best efforts to limit the nature and scope of the required disclosure, including by disclosing only the minimum amount of Covered Data necessary to perform the Services or to comply with Applicable Law, as applicable and (ii)

remain fully liable to WeWork for the performance of any such third party to which disclosures are permitted.

f. Vendor shall not transfer Personal Data from any jurisdiction to any other jurisdiction (the European Economic Area constituting a single jurisdiction for this purpose), without the prior written consent of WeWork and, if applicable, without putting in place an appropriate data transfer agreement or other mechanism appropriate to comply with Applicable Law. If requested by WeWork in order to enable WeWork to comply with any Applicable Law(s), Vendor will execute the Standard Contractual Clauses set out in Annex 2 to the Agreement, or any other version of a model contract deemed by the European Commission or applicable regulator to offer adequate data protection safeguards in relation to the transfer of Personal Data as WeWork deems reasonably necessary to comply with Applicable Law. Vendor may avoid execution of such data transfer agreements to the extent that it is permitted to transfer and receive WeWork Personal Data as a result of certification under the E.U.-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, "**Privacy Shield**"). Also, in the future, WeWork may elect to certify to Privacy Shield and cover data transfers under its own Privacy Shield certification; and, in such an event, Vendor further agrees: (i) to provide at least the same level of privacy protection as is required by the principles of the Privacy Shield, and to notify WeWork if it if can no longer provide such protection; and (ii) to permit WeWork to provide a summary or a representative copy of the relevant privacy provisions of this Agreement to the U.S. Department of Commerce ("**Commerce**") upon Commerce's request. Vendor shall provide WeWork with prompt written notification of any changes to its Privacy Shield certification status.

g. Vendor will provide all assistance necessary for WeWork to meet its obligations in respect of Individuals' rights relating to Personal Data, including, as applicable, those set out in Chapter III of the GDPR; without limiting the foregoing, and to the extent required by Applicable Law, Vendor will grant access to, provide a copy of, cease and restrict Processing (with the exception of storage), update, revise, correct, or delete Personal Data as directed by WeWork or, upon WeWork's prior approval, by an Individual to whom the Personal Data relates. Without limiting the foregoing, Vendor agrees to assist WeWork in any way reasonably necessary to cooperate with and meet its obligations to regulatory authorities (and, where required, provide assistance to WeWork in performing a data protection impact assessment and/or prior consultation of regulatory authorities). Vendor shall notify WeWork in writing within five (5) calendar days of receipt of any enquiry, notice or complaint from any Individual relating to Personal Data about that Individual and shall further provide all reasonable assistance to Vendor in responding to all such communications.

**3. <u>Retention and Return of Covered Data.</u>**

a. Vendor will retain Covered Data only for as long as necessary to perform the Services, or as required by Applicable Law, and in all cases this Exhibit will continue to apply with respect to such Covered Data during all periods in which it is retained or accessible by Vendor.

b. Upon expiration or termination of the Agreement, or at any time upon WeWork's request, Vendor will as soon as reasonably practicable, but in no event, later than ten (10) days after such request, return or, if directed by WeWork, destroy all Personal Data, including without limitation all originals and copies in any medium, and any materials derived from or incorporating such Personal Data at any time. Upon request, Vendor will send WeWork a written certification acknowledging that all Personal Data have been returned or destroyed pursuant to the foregoing obligation. Notwithstanding the foregoing, in the event that it is infeasible to (as applicable) return or destroy Personal Data (or a subset thereof) on the date required pursuant to this Section (the "**Return Date**") or if Applicable Law prevents or precludes the return or destruction of any Personal Data by Vendor on the Return Date, Vendor shall notify WeWork in writing, in reasonable detail, of the reason for not returning or destroying such Personal Data on the Return Date. In such case, Vendor shall return or destroy the Personal Data (as applicable) as soon as possible after the Return Date, and, for the avoidance of doubt, the protections of this Exhibit shall apply to all Personal Data for as long as such Personal Data are retained by Vendor.

**4. <u>Cybersecurity and Data Breaches.</u>**

a. Vendor represents, warrants, and covenants that it has implemented and will maintain a written information security program that incorporates administrative, technical, and physical safeguards designed to ensure the security, confidentiality, integrity, and reliability of the Covered Data, Systems, and Services. Such safeguards should be commensurate with the type and amount of Covered Data Processed by Vendor, having regard to the state of art and industry standards, and should, at a minimum, protect Covered Data against reasonably anticipated threats or hazards, including from unauthorized access, loss, destruction, use, modification, or disclosure. Without limitation to the foregoing, Vendor agrees that the information security program it has implemented and maintains will:

   i. identify appropriately defined organizational roles related to security and incident response;

   ii. ensure compliance with Applicable Law and meet or exceed the requirements thereunder;

   iii. appropriately protect against the destruction, loss, disclosure, alteration or other accidental or unauthorized Processing of Personal Data in the possession of Vendor or a Vendor Party or to which Vendor or a Vendor Party may have access;

   iv. include appropriate controls with respect to the employment of and access given to Vendor Parties, including (as appropriate) background checks, security clearances that assign specific access privileges to individuals, and training regarding the handling of Personal Data;

   v. include an appropriate network security program that includes, without limitation, utilization of industry standard encryption technologies when appropriate and, in any case, with respect to Covered Data: (A) transmitted over public networks (i.e. the Internet) or transmitted wirelessly; (B) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD. ISN drives, back-up tapes); and (C) in any circumstances required under Applicable Law;

   vi. includes appropriate controls addressing (A) access identification and authentication, (B) maintenance and media disposal, (C) audit and accountability, (D) physical and environmental protection, (E) systems and communication security; and (F) incident response and planning; and

   vii. reasonably ensure the integrity and reliability of such facilities, systems, service, which shall include, to the extent appropriate: (A) critical asset identification, (B) configuration and change management for software systems, (C) physical and environmental protection, and (D) contingency planning/redundancy.

b. If Vendor Processes cardholder or other financial account data in connection with this Agreement, then it represents and warrants, and shall certify, that its information security program, and any Processing of such financial account data by Vendor or Vendor Parties, complies with the Payment Card Industry Data Security Standard ("PCI DSS"), ISO 22307, and ISO 27000.

c. Personal computers and mobile devices containing WeWork Confidential Information must be sanitized prior to recycling, resale, reassignment or disposal, or following such a computer or mobile device's loss or theft. If sanitization is not possible, the media must be destroyed. If Vendor issues a laptop computer or mobile device to any Vendor Party for temporary use, WeWork Covered Data stored on the device must be erased (or saved, if required, and appropriately maintained) before the computer is issued to any subsequent user.

d. If Vendor or Vendor Parties obtain or are granted access to any Systems, then such access, in all cases, will be subject to and in compliance with all then-current WeWork policies, including, not limited to all security, privacy, safety, environmental, information technology, legal, and business conduct policies. Any access to any such facilities, locations or other systems is strictly for the purpose of Vendor's performance of the Services hereunder.

e. Vendor hereby represents, warrants and covenants that it will use highest industry standards to scan and filter for harmful surreptitious code, such as viruses, spyware and worms ("**Viruses**"), and otherwise ensure that no forms of Viruses are introduced by any means into any Covered Data or Systems as a

result of WeWork's use of the Services. If a Virus is found to have been introduced into any System by the Services, Vendor shall promptly notify WeWork of the introduction and, at no additional charge to WeWork, assist WeWork in eradicating the Virus and eliminating its effects, and if the Virus causes an interruption of the Services, a loss of operational efficiency or loss of Covered Data or Systems, Vendor will take all necessary steps to repair any damage done by the Virus, including undertaking remediation efforts at no cost or loss to WeWork.

f. Vendor shall provide to WeWork written notice of any Data Security Breach promptly and in no event later than one (1) business day following the occurrence of such Data Security Breach. Such notice shall summarize in reasonable detail the impact of such Data Security Breach upon WeWork and Individuals, if any, whose Personal Data is affected by such Data Security Breach, the categories and approximate number of Individuals concerned and the categories and approximate number of Personal Data records concerned, and the corrective action to be taken by Vendor. In no case shall Vendor delay notification because of insufficient information but instead provide and supplement notifications as information becomes available.

g. In the event of any Data Security Breach, Vendor will undertake an investigation of such Data Security Breach and reasonably cooperate with WeWork in connection with such investigation, including by providing WeWork with a summary of the results of Vendor's investigation, and will take all necessary and appropriate corrective action, at the expense of Vendor, to prevent a recurrence of such Data Security Breach. Vendor will not make any public announcements relating to such Data Security Breach without WeWork's prior written approval, which shall not be unreasonably withheld. At WeWork's request, Vendor agrees to assist WeWork in, and bear responsibility for the costs of, all remediation efforts that are required by Applicable Law as a consequence of any Data Security Breach or that have been required by any governmental authority in similar circumstances, regardless of whether Applicable Law explicitly imposes such remediation obligations on Vendor or WeWork or both. Such remediation efforts may include without limitation (a) development and delivery of notices to Individuals whose Personal Data may have been affected; (b) establishment of a toll-free telephone number or numbers (or where not available, a dedicated telephone number or numbers) where affected Individuals may receive individual-specific assistance and information relating to the Data Security Breach; (c) provision of free credit reports, credit monitoring/repair and/or identity restoration/insurance for affected Individuals; (d) reimbursement for the costs of placing a freeze on a consumer credit file and likewise for the costs of unfreezing the same consumer credit file; (e) investigation and resolution of the causes and impacts of the Data Security Breach; and (f) such other measures that WeWork determines are reasonable and commensurate with the nature and level of severity of the Data Security Breach. Vendor shall be solely responsible for the costs and expenses of all remediation measures and all other actions undertaken pursuant to the foregoing, whether undertaken by Vendor or WeWork. Without limitation to the foregoing, Vendor shall promptly reimburse WeWork for all costs and expenses reasonably incurred by WeWork in connection with the Data Security Breach, including without limitation costs and expenses incurred in connection with remediation efforts or otherwise in connection with this Section.

h. Vendor shall prohibit download and use of file sharing and other software that can open security vulnerabilities to areas that hold Covered Data.

i. **Passwords.**

   i. Vendor must manage account passwords and require minimum password standards in accordance with industry best practices and standards, as may be deemed acceptable by WeWork.
   ii. Vendor will implement and maintain a documented process for the secure distribution of user accounts and passwords.
   iii. Vendor will manage all passwords in such a manner as to immediately change or terminate passwords or other credentials that authorize access to WeWork Confidential Information whenever a person is no longer authorized to access such information, whether due to change in role, termination of relationship with Supplier or otherwise.
   iv. Vendor will encrypt all passwords, passphrases, and PINs using solutions that are certified against industry best practices and standards, and verify that the encryption keys and any keying material are not stored with any associated data.

v. Vendor will replace and renew all cryptographic keys and certificates within twenty-four (24) hours if any part of the Certificate Authority signing hierarchy is compromised, expired or otherwise revoked. Any such occurrence shall be considered a Data Security Breach.

**5. Additional Obligations.**

a. Vendor shall comply with Applicable Law with respect to the Processing of Covered Data.

b. Vendor shall notify WeWork promptly of the receipt of any communication, complaint, enforcement action, or other inquiry from or by any legal or regulatory authority relating to the Processing by Vendor of Personal Data, and Vendor shall further provide all reasonable assistance to WeWork in responding to all such inquiries that relate to the Processing of Personal Data.

c. Vendor shall ensure that Vendor Parties with access to Covered Data are advised of and comply with (i) Vendor's written information security program; (ii) provisions relating to the privacy and security of Covered Data; and (iii) all Applicable Laws. Vendor shall be responsible for any breach of the obligations set forth in this Agreement and for all acts or omissions of its employees, agents, and subcontractors in the same manner as for its own acts or omissions (whether or not such employees, agents, or subcontractors have acted within the scope of employment or agency) and any violation of any Applicable Law by any Vendor Party.

**6. Inspection and Audit Rights.**

a. Vendor shall provide WeWork with all necessary materials, documents, assessments and other information to enable WeWork to confirm that Vendor has complied with its obligations under this Agreement (e.g., SSAE 16, SOC I, II, and II, SysTrust, Web Trust, or perimeter certifications or other third-party assessments, test results, audits or reviews) ("**Risk Assessments**"); provided, however, that Vendor is not required to provide any materials that would cause it to violate its pre-existing and written policies or data security standards. Vendor shall promptly correct or adopt an appropriate plan to correct any material risks or threats or nonconformance (to this Agreement, industry practices and/or Applicable Law) identified through a Risk Assessment.

b. Vendor acknowledges and agrees that WeWork shall have the right, at any time during the term of the Agreement, including any renewal thereof, to audit Vendor's privacy and security practices or (at WeWork's discretion) to request that Vendor engage a third party at Vendor's sole cost and expense, such third party to be mutually agreed upon by WeWork and Vendor (such agreement not to be unreasonably withheld), to conduct an independent audit of Vendor's privacy and security practices, and Vendor will comply with such request. To the extent that any audit conducted pursuant to this Agreement identifies alleged risks or threats and/or nonconformance to Applicable Law or generally accepted trade practice in the industry or other breach of the Exhibit (each a "**Security Issue**"), Vendor shall, within ten (10) days of receipt of such written notification, either correct such Security Issues or provide WeWork with a plan acceptable to WeWork for remediating the Security Issues. If (i) the Security Issues are not corrected, or (ii) if an acceptable plan for correcting them is not agreed to during such period, or (iii) if an acceptable plan is not executed according to its schedule, WeWork may, by giving Vendor written notice thereof, immediately terminate the Agreement in whole or in part and demand from Vendor a pro rata refund of the fees paid or payable under such Agreement, which Vendor shall deliver to WeWork within thirty (30) days.

**7. Disaster Recovery and Backup**

a. Vendor will maintain the capability to resume provision of the Services from an alternative location, and via an alternative data communications route if necessary ("**DR Services**"), in the event of a problem, crisis or other incident which results in the inability of Vendor to provide the Services or that will result in significant damage or loss to WeWork in relation to the Services or Covered Data ("**Disaster**"). Vendor will provide DR Services in the event of a Disaster regardless of whether such Disaster qualifies as a force majeure event. As a result of DR Services, Vendor will restore full access and use of the Services no later than twenty four (24) hours after the occurrence of a Disaster.

b. As part of the Services, Vendor will (i) develop, submit to WeWork for approval and, upon WeWork approval, implement and manage Disaster recovery plans for the infrastructure utilized in performing the Services; (ii) within one hundred twenty (120) days of the date of the Agreement, and at least once every quarter year during the term of the Agreement, including any renewal thereof, update and test the operability of the Disaster recovery plans in effect at that time; (iii) upon WeWork's request, certify to WeWork that the Disaster recovery plans are fully operational; and (iv) upon discovery, immediately notify WeWork of any Disaster affecting the provision or receipt of the Services, and in such event or on receipt of notice of a Disaster from WeWork implement the Disaster recovery plan and provide the DR Services.

**8.** **Insurance.** Without limitation to any other obligation in the Agreement, Vendor will obtain and maintain at its sole expense insurance coverage of the types and in the amounts customary for a business that provides similar services ("**Required Insurance Coverages**"), which shall include without limitation: (A) general liability coverage including contractual liability, products/completed operations, and personal/advertising injury coverage for no less than $5 million per occurrence and $5 million in the aggregate (or, if applicable, the greater amounts specified in the Agreement); (B) E&O coverage applicable to all services for no less than $20 million per claim or per wrongful act and in the annual aggregate (or, if applicable, the greater amounts specified in the Agreement); (C) Network Security Liability coverage that covers Data Security Breaches for no less than $20 million per occurrence or claim (or, if applicable, the greater amounts specified in the Agreement); and (D) Employee Dishonesty and Computer Fraud coverage for loss arising out of or in connection with fraudulent or dishonest acts committed by Vendor Parties, including damage to or destruction of property, funds, and/or electronic data. no less than $20 million per occurrence (or, if applicable, the greater amounts specified in the Agreement).

a. The Required Insurance Coverages will be worldwide and not limited by the location in which any error, omission, act or loss occurred. Vendor will ensure that there is no lapse or interruption of the Required Insurance Coverages. Insurance coverages written on a claims-made form shall be maintained in effect from the effective date of the Agreement until at least three calendar years after its termination or expiration and provide for reporting periods that extend for at least sixty (60) days after the expiration of the policy period. The retroactive date for all claims-made coverages must be no later than the effective date of the Agreement.

b. All insurance shall be procured with carriers having an A.M. Best rating of A- VII or better. All policies (other than workers' compensation) shall name WeWork as an additional insured for liability arising from Vendor's actual or alleged acts, errors or omissions and other occurrences, and each policy that provides first-party coverage will name WeWork as a loss payee. Such policies also shall provide cross-liability coverage, severability of interests, and a waiver of subrogation against WeWork. Vendor's insurance coverage shall be primary to and noncontributory with any valid insurance issued or affording coverage to WeWork. Vendor's insurance coverage will not limit Vendor's liability to WeWork under the Agreement or this Exhibit.

c. Vendor will provide WeWork certificates of insurance evidencing the Required Insurance Coverages before the effective date of this Order Form and upon each renewal or material change to the policies. Upon request, Vendor will provide WeWork copies of policies comprising the Required Insurance Coverages or a schedule listing the Required Insurance Coverages.

**9.** **Indemnification and Limitation of Liability.**

a. Vendor will indemnify, defend, and hold harmless WeWork, its affiliates, and each of their respective officers, directors, employees, and agents (collectively, the "WeWork Indemnitees") from and against any and all costs, charges, damages, expenses, fees (including without limitation reasonable attorney's fees) and losses (including without limitation fees and costs incurred in recovering the same) incurred by any WeWork Indemnitee that arises from Vendor's negligence, gross negligence or willful misconduct, or a breach by Vendor or any of its employees, subcontractors, or agents of this Exhibit.

b. Vendor's indemnification obligations under this Exhibit shall be in addition to any indemnification and other obligations Vendor may have under the Agreement. The rights and remedies of WeWork under this Exhibit shall not be subject to any limitation of actions, arbitration, or any other limiting provisions set forth in the Agreement, including conditions of force majeure. Without limiting the generality of the

foregoing, and notwithstanding anything herein nor in the Agreement to the contrary, (i) there shall be no limitations on Vendor's liability arising under this Exhibit, and (ii) WeWork shall not be precluded from immediately pursuing any rights or remedies it may have under or relating to this Exhibit.

c. Vendor undertakes and warrants:

i. where Vendor becomes aware that it will or may face a claim under Article 82 of the GDPR in relation to Processing of Personal Data for or on behalf of WeWork the Vendor shall

1. promptly inform WeWork of the claim or potential claim and provide all material detail concerning the claim and the progress of the claim insofar as is known to Vendor, and

2. provide WeWork with all material detail concerning the underlying circumstances that gave rise to the claim or potential claim. Irrespective of its rights under Article 82(5) of the GDPR, Vendor shall defend any such claim prudently.

ii. where WeWork faces an actual or potential claim under Article 82 of the GDPR concerning Processing by Vendor of Personal Data for or on behalf of WeWork, Vendor shall provide all materials and information requested by WeWork that are relevant to the defense of such claim and the underlying circumstances concerning the claim.

10. **Changes in Applicable Law**.

a. Upon fifteen (15) days' written notice to Vendor, WeWork may from time to time make amendments to:

i. This Exhibit, which WeWork reasonably considers to be necessary to address the requirements of Applicable Law; and

ii. The Standard Contractual Clauses as they apply to cross-border transfers of Covered Data which are subject to Applicable Law, which such changes are required as a result of any change in, or decision of a competent authority under, Applicable Law to allow cross-border transfers of Covered Data to be made (or continue to be made) without breach of Applicable Law.

b. Upon delivery of the notice contemplated by Section 10(a) of this Exhibit, WeWork and Vendor Parties shall promptly cooperate (and Vendor shall ensure that any applicable Vendor Parties cooperate) and negotiate in good faith with a view to agreeing and implementing changes necessary to comply with Applicable Law.

11. **Survival**. The terms of this Exhibit shall survive the expiration or termination of the Agreement.

12. **Severance**. Should any provision of this Exhibit be held invalid or unenforceable, then the remainder of this Exhibit shall remain valid and in full force and effect. The invalid or unenforceable provisions shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

13. **Governance and Order of Precedence**. To the extent not inconsistent herewith, the applicable provisions of the Agreement (including without limitation confidentiality, termination, enforcement, and interpretation) shall apply to this Exhibit. In the event of a conflict between this Exhibit and the Agreement, the terms of this Exhibit shall control and govern.