END USER AGREEMENT
FOR GSA ORDERS

The purpose of this End User Agreement (the "*Agreement*") is to establish the terms and conditions under which End User may use services from Synack, Inc. ("*Synack*") purchased from a Reseller. This Agreement, including all Exhibits, constitutes the entire agreement between End User and Synack with regard to the services to be performed and/or products to be provided by Synack to End User and supersedes all prior agreements, understandings, statements, proposal and representations, whether written or oral, between the Parties. This Agreement is effective as of the effective date of the Order Form (the "*Effective Date*"). Synack and End User are each referred to herein as a "*Party*" and collectively as the "*Parties*." In consideration of the mutual promises and upon the terms and conditions herein, the Parties agree as follows:

The following Exhibits are incorporated as a part of this Agreement:

Exhibit A: General Terms and Conditions
Exhibit B: Information Security Addendum
Exhibit C: Data Processing Addendum

EXHIBIT A: GENERAL TERMS AND CONDITIONS

1. DEFINITIONS.

1.1 "*Confidential Information*" means, collectively, Confidential End User Information and Confidential Synack Information.

1.2 "*Confidential End User Information*" means non-public, confidential or proprietary information disclosed by End User to Synack, or to any employees, officers, directors, partners, shareholders, agents, attorneys, accountants or advisors (collectively, "*Representatives*") of Synack, whether disclosed orally or disclosed or accessed in written, electronic or other form or media, whether identified at the time of disclosure as confidential, or which would reasonably be understood, given the nature of the information or the circumstances surrounding its disclosure, to be confidential or proprietary. Confidential End User Information does not include System Data that has been aggregated and anonymized.

1.3 "*Confidential Synack Information*" means any non-public, confidential or proprietary information disclosed by Synack to End User, or to any of End User's Representatives, whether disclosed orally or disclosed or accessed in written, electronic or other form or media, whether identified at the time of disclosure as confidential, or which would reasonably be understood, given the nature of the information or the circumstances surrounding its disclosure, to be confidential or proprietary.

1.4 "*End User*" means the purchasing entity, which is authorized to order from a General Services Administration Schedule contract.

1.5 "*End User Account*" means the account used by End User to access the Synack Platform, as permitted by Synack in accordance with this Agreement.

1.6 "*End User Materials*" means any application, software, technology, or other product or service that is submitted by End User to Synack for testing in connection with the Synack Services, and any environment in which the foregoing exist, as well as any other software, technology, information, data, materials and intellectual property provided or made available by End User to Synack hereunder.

1.7 "*Data Processing Addendum*" means the Data Processing Addendum attached hereto as Exhibit C.

1.8 "*FedRAMP End User*" any End User using Synack's FedRAMP cloud environment as part of the Synack Services.

1.9 "*Information Security Addendum*" means the Information Security Addendum attached hereto as Exhibit B.

1.10 "*Order Form*" means the ordering document for the Synack Services between the Reseller and End User.

1.11 "*Reseller*" means the entity that is authorized to list and resell the Synack Services on a General Services Administration Schedule contract.

1.12 "*Rules of Engagement*" means the technical guidelines and restrictions mutually agreed upon in writing from time to time by End User and Synack regarding the Synack Services.

1.13 "*Subscription Period*" means the subscription period of the Synack Services purchased in an order document with a Reseller, including any renewal subscription period.

1.14 "*Synack Personnel*" means the Synack employees and contractors performing the Synack Services hereunder.

1.15 "*Synack Platform*" means the platform provided by Synack to End User in connection with the Synack Services which includes all software, interfaces, tools, utilities, and other technologies (and any related intellectual property) relating thereto.

1.16 "*Synack Services*" means all services provided by Synack to End User as set forth in on or more order documents with a Reseller, and any additional related support services as Synack may provide in its sole discretion.

1.17 "*System Data*" means information that is collected, derived, or otherwise generated in the course of providing the Synack Services.

1.18 "*Vulnerability*" means a weakness or mistake in a End User Material that (i) allows an attacker to gain access to a system or network or otherwise reduce a network or system's information security; and (ii) meets the terms provided in the End User's Rules of Engagement.

2. SYNACK SERVICES.

2.1 ***Synack Services.*** End User may order Synack Services from Synack through an Order Form with a Reseller. Synack shall provide End User the Services as specified in such Order Form. All changes to an Order Form must be approved by Synack.

2.2 ***Synack Platform.*** Synack will make the Synack Platform available to End User for use pursuant to this Agreement and the applicable Order Form during the Subscription Period specified in the applicable Order Form. End User will access the Synack Platform through the End User Account. End User will choose login credentials, including a password, for the End User Account. End User is responsible for all activities that occur through the End User Account or through use of the End User Account credentials. End User agrees to keep all End User Account credentials secure and will not provide this information to any third party. End User will notify Synack immediately of any loss or involuntary disclosure of its End User Account credentials, any unauthorized use of the End User Account, or any other breach of security.

3. END USER OBLIGATIONS.

3.1 ***Cooperation; End User Primary Contact.*** End User shall cooperate with Synack in all matters relating to Synack Services. End User shall appoint an End User employee to serve as the primary contact with respect to this Agreement and who will have the authority to act on behalf of End User with respect to matters pertaining to this Agreement.

3.2 ***End User Information and Materials.*** End User shall provide such End User Materials as Synack considers reasonably necessary in order to carry out the Synack Services in a timely manner and to ensure that Synack has adequate information to undertake the Synack Services. If End User provides Synack or Synack Personnel with access to any non-public End User Materials, End User shall cooperate with Synack in its efforts to make such End User Materials available through the Synack Platform and allow Synack Personnel to access the End User Materials.

3.3 ***End User Authorization.*** Subject to the terms and conditions of this Agreement, End User grants to Synack the right to use and access the End User Materials and to permit Synack Personnel to use and access the End User Materials for the purpose of performing and providing the Synack Services.

3.4 ***Synack Platform Restrictions***. In connection with End User's use of the Synack Platform, End User shall not:

(a) copy, reproduce, alter, modify, create derivative works from, rent, lease, loan, sell, distribute or publicly display the Synack Platform, Synack Services, any other material made available via the Synack Services, or any part of any of the foregoing, without the prior written consent of Synack;
(b) decompile, disassemble, translate or otherwise reverse engineer or attempt to derive the source code for the Synack Platform or the Synack Services or any portion thereof;
(c) attempt to obtain any information or content from the Synack Platform or Synack website using any robot, spider, scraper or other automated means for any purpose, except as otherwise expressly permitted in writing by Synack;
(d) transmit or upload any software viruses or any other computer codes, files, or programs that are designed or intended to disrupt, damage, limit, or interfere with the proper function of any software, hardware, or telecommunications equipment or to damage or obtain unauthorized access to any system, data, password, or other information of Synack or any third party;
(e) misrepresent or impersonate any person or entity, including any employee or representative of Synack;
(f) interfere or attempt to interfere with the proper working of the Synack Platform or Synack Services or any activities conducted on the Synack Platform or Synack Services;
(g) use the Synack Platform or the Synack Services in any manner that: (i) infringes any patent, trademark, trade secret, copyright, right of publicity, or other right of any other person or entity or violates any law or contract; (ii) is false, misleading or inaccurate; (iii) is unlawful, threatening, abusive, harmful, harassing, defamatory, libelous, deceptive, fraudulent, tortious, obscene, offensive, profane or invasive of another's privacy; (iv) makes any unsolicited communications or advertising not authorized by Synack, promotional materials or any other form of solicitation for any type of information; or (v) imposes, as determined in Synack's sole discretion, an unreasonable or disproportionately large load on Synack's IT infrastructure; or
(h) violate or otherwise not comply with any applicable local, state, national or international law or regulation.

4. INTELLECTUAL PROPERTY RIGHTS.

4.1 ***Synack Platform and Synack Services.*** Subject to the rights expressly granted to End User in this Agreement, any and all intellectual property rights in or related to the Synack Platform and Synack Services, including all related technology and services, are and shall remain, as between End User and Synack, the sole and exclusive property of Synack.

4.2 ***End User Materials.*** Subject to the rights expressly granted to Synack and Synack Personnel, any and all intellectual property rights in or related to the End User Materials are and shall remain, as between End User and Synack, the sole and exclusive property of End User.

4.3 ***System Data.*** Synack may use System Data (i) to analyze the performance of and enhance Synack products and services, and (ii) Synack may disclose such information and data in reports, presentations and other publications solely in an aggregated and anonymized manner such that it does not identify End User, any End User Material, or any individual, or enable any such information or data to be associated with End User, a End User Material, or any individual.

5. CONFIDENTIAL INFORMATION.

5.1 ***Obligations.*** Each Party (each, a "*Receiving Party*") will maintain in confidence all Confidential Information disclosed to it by the other Party (the "*Disclosing Party*"). Each Receiving Party agrees not to disclose such Confidential Information except as expressly authorized by this Agreement or unless the Disclosing Party provides the Receiving Party with written consent. Each Receiving Party agrees not to use the Disclosing Party's Confidential Information except as necessary to perform its obligations or exercise its rights under this Agreement. Each Receiving Party may disclose the Confidential Information of the Disclosing Party only to its employees, agents or subcontractors who need to know such Confidential Information for the purposes of this Agreement (including, in Synack's case, to Synack Personnel) who are under an obligation of confidentiality to the Receiving Party. The Receiving Party will promptly notify the Disclosing Party upon discovery of any unauthorized use or disclosure of the Disclosing Party's Confidential Information. At the end of the term of this Agreement, each Receiving Party will destroy any Confidential Information still in its possession, provided that backup copies may be retained for compliance purposes or in accordance with an ordinary course document retention policy of Receiving Party. All such copies remain subject to the confidentiality obligations of this Agreement.

5.2 ***Exceptions.*** The obligations of confidentiality contained in Section 5.1 will not apply to the extent that it can be established by the Receiving Party beyond a reasonable doubt that such Confidential Information:

(a) was already known to the Receiving Party, other than under an obligation of confidentiality, at the time of disclosure by the Disclosing Party;
(b) was generally available to the public or otherwise part of the public domain at the time of its disclosure by the Disclosing Party to the Receiving Party;
(c) became generally available to the public or otherwise part of the public domain after its disclosure to the Receiving Party and other than through any act or omission of the Receiving Party in breach of this Agreement;
(d) was disclosed to the Receiving Party, other than under an obligation of confidentiality, by a third party who had no obligation to the Disclosing Party not to disclose such information to others;
(e) was developed independently by the Receiving Party without any use of or reference to Confidential Information of the Disclosing Party; or
(f) was disclosed with the prior written consent of the Disclosing Party.

5.3 ***Required Disclosures.*** The foregoing confidentiality and nondisclosure obligations shall not prohibit the disclosure of Confidential Information, to the extent such disclosure is required by law or by regulation; provided, however, that, in such event, the Receiving Party provides the Disclosing Party with prompt notice of such disclosure so that the Disclosing Party has the opportunity if it so desires to seek a protective order or other appropriate remedy. Synack recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

5.4 ***Reserved****.*

6. DATA SECURITY AND PRIVACY

6.1 ***Information Security Requirements***. Synack shall maintain the information security standards set forth in Synack's Information Security Addendum during the Term.

6.2 ***End User Data.*** To the extent that Synack processes personal data in the course of providing the Synack Services to End User, End User agrees to Synack's Data Processing Addendum.

6.3 ***Data Privacy.*** End User represents and warrants that End User has obtained all necessary rights to permit Synack to collect and process the End User data described in Section 6.2, including, without limitation, data from endpoints, servers, cloud applications, and logs.

7. WARRANTIES.

7.1 ***Both Parties.*** Each Party represents and warrants to the other Party that:

(a) it is duly organized, validly existing and in good standing as a corporation or other entity as represented herein under the laws and regulations of its jurisdiction of incorporation, organization or chartering;
(b) it has the full right, power and authority to enter into this Agreement and to perform its obligations hereunder;
(c) the execution of this Agreement by its representative whose signature is set forth at the end hereof has been duly authorized by all necessary corporate action of the Party; and
(d) when executed and delivered by such Party, this Agreement will constitute the legal, valid and binding obligation of such Party, enforceable against such Party in accordance with its terms.

7.2 ***Synack Warranties.*** Synack shall perform the Synack Services in a timely and professional manner consistent with industry standards, and in conformance in all material respects with the requirements set forth in the applicable order document.

7.3 ***End User Warranties*****.** End User represents and warrants that (a) it owns or has sufficient license or other legal rights to authorize the Synack Services with respect to all End User Materials and (b) the End User Materials do not infringe or otherwise misappropriate or violate (i) any third party intellectual property rights including, but not limited to, patents, trade secrets, trademarks, and copyrights or (ii) any other rights. End User shall immediately notify Synack in writing if End User becomes aware of any actual or suspected infringement,

misappropriation, or other violation of rights by the authorization provided by End User to Synack with respect to the Synack Services.

7.4 ***Disclaimer of Warranties.*** THE SYNACK SERVICES, THE SYNACK PLATFORM AND ANY CONTENT AND INFORMATION PRESENTED ON OR VIA THE SYNACK SERVICES OR THE SYNACK PLATFORM ARE PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, TIMELINESS, ACCURACY, COMPLETENESS, RELIABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR SAFETY. ANY ORAL OR WRITTEN INFORMATION OR ADVICE PROVIDED BY SYNACK OR ITS AUTHORIZED REPRESENTATIVES, OR BY SYNACK PERSONNEL, WILL NOT BE DEEMED TO CREATE ANY WARRANTY. WITHOUT LIMITING THE FOREGOING, NEITHER SYNACK NOR ITS LICENSORS WARRANT THAT ACCESS TO THE SYNACK SERVICES OR THE SYNACK PLATFORM WILL BE UNINTERRUPTED OR THAT THE SYNACK SERVICES OR THE SYNACK PLATFORM WILL BE ERROR-FREE.

8. INDEMNIFICATION.

8.1 ***Reserved.***

8.2 ***By Synack.***

(a) Synack shall have the right to intervene to defend, indemnify, and save harmless End User and its officers, directors, employees, agents and representatives ("*Indemnified End User Parties*") from and against any and all damages, liabilities, losses and other costs (including without limitation reasonable attorneys' fees) relating to any Claim against any Indemnified End User Party arising from or relating to any actual or alleged violation or infringement of any proprietary right of any third party, (including, but not limited to, any patent, copyright, trademark, trade secrets or any other intellectual property rights) by the Synack Services or Synack Platform. This Section 8.2(a) will not apply to any Claim in the event and to the extent that the Claim (i) arises out of or is related to (A) any modification of the Synack Services or Synack Platform other than by Synack, (B) any combination of the Synack Services or Synack Platform with other products, services or materials not authorized by Synack, or (C) End User's failure to use the replacement or modification provided by Synack pursuant to Section 8.2(b), or (ii) is subject to indemnification by End User pursuant to Section 8.1. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

(b) If Synack believes the Synack Services and/or Synack Platform infringe or may be alleged to infringe any third party proprietary right, then Synack may, in addition to its indemnification obligations set forth above, and at its sole option and expense: (i) procure for End User the right to use the allegedly infringing Synack Services or Synack Platform, as applicable, (ii) replace the Synack Services or Synack Platform, as applicable, with other non-infringing services or products, or (iii) modify the Synack Services or Synack Platform, as applicable, so that it does not infringe. If none of (i) through (iii) is commercially feasible, Synack may terminate this Agreement immediately upon written notice to End User. This Section 8.2 states the entire liability and obligations of Synack, and the exclusive remedy of End User, with respect to any actual or alleged infringement of any third-party proprietary rights in connection with this Agreement.

8.3 ***Indemnification Procedure.*** The indemnification obligations above in Sections 8.1 and 8.2 are contingent on the indemnified party (a) promptly notifying the indemnifying party of any Claim (provided that the indemnified party's failure to provide such prompt notice will not release the indemnifying party from its indemnification obligations except to the extent the indemnifying party is materially prejudiced thereby); (b) providing the indemnifying party with any reasonable information and assistance needed to defend or settle the Claim (provided the indemnifying party bears any out of pocket expenses incurred by the indemnified party in providing such assistance or information) and (c) allowing the indemnifying party the right to have sole control of the investigation, defense and settlement of the Claim, provided that the indemnifying party will not enter into any settlement of a Claim that: (i) imposes a monetary obligation on the indemnified party that is not covered by the indemnification; (ii) imposes a material, non-monetary obligation on the indemnified party, (iii) does not include an unconditional release of the indemnified party; or (iv) admits liability on the part of the indemnified party without the indemnified party's prior written consent, which will not be unreasonably withheld or delayed. The indemnified party shall have the option, at its expense, to participate in the defense or settlement of the Claim with counsel of its own choosing.

9. *LIMITATION OF LIABILITY*. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT FOR AMOUNTS PAYABLE BY A PARTY PURSUANT TO SECTION 8 (INDEMNIFICATION), (A) IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY, OR TO ANY THIRD PARTY CLAIMING THROUGH OR UNDER THE OTHER PARTY, FOR ANY LOST PROFITS, LOSS OF DATA, EQUIPMENT DOWNTIME OR FOR ANY OTHER INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY THEREOF, AND (B) IN NO EVENT WILL EITHER PARTY'S TOTAL CUMULATIVE LIABILITY UNDER OR ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, FROM ALL CAUSES OF ACTION OF ANY KIND, EXCEED THE TOTAL AMOUNT OF FEES PAID BY END USER FOR THE SYNACK SERVICES PROVIDED TO THE END USER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO THE CLAIM (DETERMINED AS OF THE DATE OF ANY FINAL JUDGMENT IN AN ACTION). THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR

ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

10. TERM AND TERMINATION.

10.1 ***Term*.** This Agreement shall continue in full force and effect until it is terminated in accordance with this Agreement.

10.2 ***Termination*.** When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Synack shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

10.3 ***Effect of Termination.***

(a) Except as otherwise expressly provided herein, upon any expiration or termination of this Agreement, all rights, licenses and obligations of the Parties shall immediately cease and terminate. Termination or expiration of this Agreement will not relieve or release either Party from any liability which, at the date of termination, has already accrued to the other Party.
(b) Upon any expiration or termination of this Agreement, each Party shall promptly return to the other Party all Confidential Information of the other Party in its possession or under its control, or, upon written request of the other Party, destroy all Confidential Information in its possession.
(c) Notwithstanding anything to the contrary in the foregoing, the provisions of this Section 10.3 and of Sections 1, 4-9, and 12.2-12.12 shall survive the termination or expiration of this Agreement in accordance with their terms.

11. PRODUCT SPECIFIC TERMS.

11.1 ***FedRAMP.*** Non-federal End Users who purchase FedRAMP Synack Services will be required to enter into a FedRAMP addendum to be provided by Synack prior to the commencement of such use. FedRAMP End Users must notify and receive prior approval from Synack for third party functions, ports, protocols, and services intended for organizational use. The only integrations the FedRAMP End User may use in Synack's FedRAMP cloud environment are those integrations provided by Synack. Further, these integrations may only integrate with environments which are hosted by FedRAMP authorized cloud providers or self-hosted by the FedRAMP End User which adhere to the NIST SP 800-53 compliance standards. FedRAMP End Users must notify Synack prior to making any changes that will cause any previously approved integrations to no longer adhere to the NIST SP 800-53 compliance standards.

11.2 ***Synack Credits.*** To the extent End User has purchased Synack Credits from a Reseller, such Synack Credits will be promptly credited to the End User Account and will be redeemable for the Synack Services described in the catalog published within the Synack Platform or such other site as indicated by Synack (the "*Synack Catalog*"). The Synack Services and the number of Synack Credits required to redeem Synack Services set forth in the Synack Catalog may change at any time. Synack Credits may only be redeemed for the Synack Services listed in the Synack Catalog. Synack Credits have no cash value, are non-transferable and non-refundable. All Synack Credits are valid only during the Subscription Period defined in the applicable order document in which they were purchased (or, if undefined, one (1) year from the date of purchase). Synack Credits will expire upon the earlier of the end of the applicable Subscription Period or the termination of the Agreement unless used prior to such expiration or termination.

12. GENERAL.

12.1 ***Publicity.*** Synack shall have the right to use and display End User's name on Synack's website and in other advertising and marketing materials and to otherwise disclose that End User is a client of Synack to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

12.2 ***Governing Law*.** The validity, construction and interpretation of this Agreement, and the rights and duties of the Parties, shall be governed by and construed in accordance with the Federal laws of the U.S.A., without giving effect to the conflict of law provisions thereof, and excluding any application of the United Nations Convention on Contracts for the International Sale of Goods.

12.3 ***Waiver and Amendment*.** No waiver, amendment or modification of any provision hereof or of any right or remedy hereunder shall be effective unless made in writing and signed by the Party against whom such waiver, amendment or modification is sought to be enforced, and this Agreement may only be amended by a writing signed by both Parties. No failure by any Party to exercise, and no delay by any Party in exercising, any right, power or remedy with respect to the obligations secured hereby shall operate as a waiver of any such right, power or remedy.

12.4 ***Assignment*.** End User shall not assign this Agreement or any of its rights or obligations under this Agreement without the prior written consent of Synack. This Agreement shall be binding upon and inure to the benefit of the successors and the permitted assigns of the respective Parties hereto.

12.5 ***Force Majeure*.** In accordance with GSAR Clause 552.212-4(f), neither Party shall be liable under this Agreement by reason of any failure or delay in the performance of its obligations under this Agreement on account of, riots, insurrections, fires, floods, storms, explosions, acts of nature, acts of terrorism, war, governmental action, labor conditions, earthquakes, or any other cause that is beyond the reasonable control of such Party.

12.6 ***Notices*.** All notices required by or permitted under this Agreement shall be in writing and shall be deemed given as of the day personally delivered or electronic mail (provided that delivery to the recipient is confirmed), or sent by express courier, each such delivery method delivered, sent or addressed to the address set forth below the signature line, or at such other address as properly designated in writing from time to time.

12.7 ***Severability.*** If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, void, or unenforceable, such provision shall be enforced to the maximum extent possible and the remaining provisions of this Agreement shall continue in full force and effect to the maximum extent permissible without being impaired or invalidated in any way.

12.8 ***Counterparts.*** This Agreement may be executed simultaneously in two or more counterparts, each of which shall be considered an original, but all of which together shall constitute one and the same instrument.

12.9 ***Third Party Beneficiaries.*** Except as otherwise expressly provided in this Agreement, nothing in this Agreement shall confer any rights upon any person other than the Parties, and each such Party's respective successors and permitted assigns.

12.10 ***Independent Contractors***. The relationship between the Parties is and shall be that of independent contractors. It is expressly agreed that nothing in this Agreement shall be construed to create or imply a partnership, joint venture, fiduciary or agency relationship, or contract of employment. Neither Party shall have the authority to make any statement, representation or commitment of any kind, or to take any action, that shall be binding on the other Party.

12.11 ***Headings*****.** The headings used in this Agreement are for convenience only and shall not be considered part of the Agreement.

12.12 ***Entire Agreement*****.** This Agreement along with all Exhibits constitute the entire understanding and agreement of the Parties hereto with respect to the subject matter hereof and supersedes all prior agreements or understandings, written or oral, between the Parties hereto with respect to the subject matter hereof. This Agreement shall supersede any separate confidentiality or nondisclosure agreement signed by the Parties with respect to the performance of the Synack Services hereunder.

EXHIBIT B: INFORMATION SECURITY ADDENDUM

This Information Security Addendum (this "*Addendum*") forms part of the End User Agreement by and between Synack, Inc., a Delaware corporation ("*Synack*") and the counterparty thereof ("*Customer*"), dated as of the Effective Date (the "*Agreement*"). Capitalized terms used but not defined in this Addendum have the meanings ascribed in the Agreement.

1. PURPOSE. This Addendum describes the minimum information security standards that Synack shall maintain in connection with the Confidential Customer Information, including information regarding the Customer Materials and any personal data disclosed or made available to Synack by Customer (collectively, the "*Customer Data*"). Requirements in this Addendum are in addition to any requirements in the Agreement and the Data Processing Addendum, if applicable.

2. SECURITY MEASURES.

2.1 ***Access control to premises and facilities***. Synack shall maintain appropriate security measures to prevent unauthorized physical access to premises and facilities holding the Customer Data, including:

(a) Locked doors;
(b) Access control system using electronic access, biometric access or physical key;
(c) Alarm system;
(d) Video surveillance; and
(e) Logging of facility exits and entries.

2.2 ***Access control to systems***. Synack shall maintain appropriate measures to prevent unauthorized access to its information technology systems, including:

(a) Unique login identifiers assigned to each user;
(b) Prohibition of shared non-machine accounts in all circumstances;
(c) Required password procedures (including minimum length and complexity and forced changes of password);
(d) Prohibition of guest users or anonymous accounts;
(e) Central management of system access;
(f) Tracking of access change requests;
(g) Privilege access restrictions (whereby access is subject to existing access rights and approval from management);
(h) Quarterly access checks to ensure access levels are appropriate for the roles each user performs;
(i) Monitoring of all access control changes to accounts and groups (including creation, modification, and deletion);
(j) Network access control for all information technology systems (requiring hosts to be preauthorized and authenticated to the network and ensuring hosts are running the minimum set of information security controls prior to being granted access);
(k) Required multi-factor authentication through a VPN tunnel from a pre-authorized machine for remote access to internal corporate network and consoles; and
(l) Full suite of firewall controls that monitors inbound and outbound traffic against a pre-established set of permissible traffic flows.

2.3 ***Access control to data***. Synack shall maintain appropriate security measures to prevent authorized users from accessing data beyond their authorized access rights and to prevent the unauthorized input, reading, copying, removal, modification or disclosure of data. These measures include the following:

(a) Principle of least privilege applied to all access request decisions;
(b) Access rights defined according to duties, with appropriate levels of access allocated according to the "need to know" principle;
(c) Differentiated access rights through Role Based Access Controls (RBAC);
(d) Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment;
(e) Host-based device management and data loss prevention software on all hosts (monitoring for the movement of sensitive data to and from the host), which is required to join the network through network access control; and
(f) Row level access controls on all databases containing sensitive information to restrict access of data objects to specific users.

2.4 ***Disclosure control***. Synack shall maintain appropriate security measures to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures include:

(a) Compulsory use of a wholly-owned and managed private network for all data transfers within the corporate group;
(b) Full-disk encryption required on all end-user devices to protect against data incidents through theft or loss, including Device Management and Data Loss Prevention controls with the ability to remotely wipe the device of data (required to join the network through network access control);
(c) Audit trail creation for all data access and transfers across all information systems, including but not limited to date and time of event, type of action performed, and name of files accessed; and
(d) Encryption of all sensitive data to protect against theft or loss of database files in transit and at rest.

2.5 ***Input control***. Synack shall maintain appropriate security measures to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom. These measures include:

(a) Creating an audit trail for all user actions across all information systems, including but not limited to date and time of event, type of action performed, and process used;

(b) Ensuring that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment; and
(c) Ensuring that it is possible to verify and establish which personal data have been entered into automated data processing systems and when and by whom the data have been entered.

2.6 ***Job control***. Synack shall maintain appropriate security measures to ensure that Customer Data is processed strictly in compliance with Customer's instructions, including unambiguous wording of contractual instructions and monitoring of contract performance.

2.7 ***Availability control***. Synack shall maintain appropriate security measures to ensure that data are protected against destruction or loss of data through accidental or malicious intent, including:

(a) Ensuring that installed systems may be restored in the event of an interruption;
(b) Ensuring that systems are functioning and faults are reported;
(c) Ensuring stored personal data cannot be corrupted by means of a malfunctioning of the system;
(d) Uninterruptible power supply (UPS) of critical information systems;
(e) Automation backup functions of user and system level data across information systems and off-site storage;
(f) Business Continuity and Disaster Recovery Plans and Procedures;
(g) Prohibition of portable or removable media and enforcement through device management policy; and
(h) Anti-malware and Intrusion Detection/Prevention solutions with advanced persistent threat detection capabilities, which perform real-time behavior analysis of machine and network behavior.

2.8 ***Segregation control***. Synack shall maintain appropriate security measures to allow data collected for different purposes to be processed separately, including:

(a) Restriction of access to data stored for different purposes according to staff roles and responsibilities;
(b) Segregation of business information system functions; and
(c) Segregation of testing and production information system environments.

2.9 ***Audit***. Synack shall maintain appropriate security measures to ensure proper functioning of controls, including:

(a) Audits and certifications each year to the ISO 27001:2013 standard in multiple locations throughout the world;
(b) Allowing audits multiple times throughout the year by external clients as part of their own internal risk management processes; and
(c) Audits multiple times each year through internal risk management processes by internal audit teams for application security, vulnerability assessments, and network security.

3. MESSAGING SYSTEM. Customer may from time to time use Synack's messaging system to communicate with Synack Personnel through the Synack Platform. Synack reserves the right to monitor, intercept and review, without further notice, messages sent or received using the message system. Synack may also store copies of such data and communications for a period of time after they are created, and may delete such copies from time to time without notice. Customer acknowledges and agrees that the identity of any Synack Personnel will not be disclosed or otherwise made available to Customer by Synack or through the Synack Platform, and that Synack has no obligation to disclose the identity of any Synack Personnel to Customer.

4. MISCELLANEOUS.

4.1 ***Effectiveness***. This Addendum will be effective from the date on which it is appended to the Agreement and shall remain in effect throughout the term of the Agreement. In the event of the expiration or termination of the Agreement or this Addendum, Synack's obligations described in Section 2 of this Addendum will survive for so long as Synack holds, stores or otherwise processes Customer Data.

4.2 ***Integration***. This Addendum forms part of the Agreement and shall be governed by and subject to the terms therein, including, without limitation, provisions regarding limitation of liability, governing law, and notices.

EXHIBIT C: DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "*Addendum*") forms part of the End User Agreement by and between Synack, Inc., a Delaware corporation ("*Synack*") and the counterparty thereof ("*Customer*"), dated as of the Effective Date (the "*Agreement*"). This Addendum, together with all addendums, annexes, amendments, and attachments hereto, reflects the Parties' agreement with regard to Synack's Processing of Customer Personal Data in connection with providing Synack Services described in the Agreement. In the event of a conflict, the terms and conditions of this Addendum will prevail.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

WHEREAS, Synack may process Customer Personal Data (as defined below) on behalf of Customer in connection with the Synack Services provided under the Agreement, and

WHEREAS, Synack and Customer seek to implement a data processing agreement that defines each party's rights and obligations with respect to the processing of Customer Personal Data in compliance with the Privacy and Security Laws (as defined below).

NOW, THEREFORE, in consideration of the mutual covenants and agreements in this Addendum and the Agreement, and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Synack agree as follows:

1. DEFINITIONS. The following terms, including any derivatives thereof, will have the meanings set forth below:

1.1 "*Customer Personal Data*" means any Personal Data that is Processed by Synack or its subcontractors on behalf of Customer as part of Customer's use of the Synack Services.

1.2 "*Data Subject*" means an individual who is the subject of Personal Data.

1.3 "*Personal Data*" means information Synack processes for Customer that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Synack's possession or control or that Synack is likely to have access to, or (b) the relevant Privacy and Security Laws otherwise define as protected personal information.

1.4 "*Privacy and Security Laws*" means all applicable federal, state, and foreign laws and regulations relating to the processing, protection, or privacy of the Personal Data under the Agreement, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, (a) the California Online Privacy Protection Act (CalOPPA) (Cal. Bus. & Prof. Code § 22577), the California Data Protection Act (Cal. Civ. Code § 1798.80-84), and California Breach Notification Laws (Cal. Civ. Code §§ 1798.29, 1798.82), (b) the UK Data Protection Act 2018 ("*DPA*"), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (collectively, the "*UK GDPR*"), (c) the EU General Data Protection Regulation 2016/679 (the "*EU GDPR*") and the Privacy and Electronic Communications Directive 2002/58/EC, and (d) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of Personal Data, in each case only to the extent applicable to the activities or obligations under or pursuant to the Agreement and as amended, consolidated, re-enacted or replaced from time to time.

1.5 "*Process*" means any activity that involves the use of Personal Data or that the relevant Privacy and Security Laws may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

1.6 "*Security Incident*" means any actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access to, or malicious infection of Customer Personal Data transferred, stored, or otherwise Processed by Synack or any of its subcontractors or third parties that Process Customer Personal Data on Synack's behalf.

1.7 "*Synack Personnel*" will have the same meaning provided under the Agreement.

1.8 "*Synack Services*" will have the same meaning provided under the Agreement.

2. PROCESSING OF CUSTOMER PERSONAL DATA.

2.1 Synack will only Process Customer Personal Data for purposes of providing the Synack Services, which constitutes a business purpose under CCPA, and only in accordance with Customer's instructions unless otherwise required under the Privacy and Security Laws, in which case Synack will use commercially reasonable efforts to inform Customer of that legal requirement prior to Processing such Customer Personal Data (unless that law prohibits such information on important grounds of public interest). The subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Customer Personal Data and categories of the data subjects is described in more detail in Annex 1. Synack is prohibited from retaining, using, or disclosing Customer Personal Data except for the purpose of providing the Synack Services or as otherwise instructed by Customer.

2.2 Synack will reasonably assist Customer with meeting Customer's compliance obligations under the Privacy and Security Laws, taking into account the nature of the Synack's Processing and the information available to Synack. Subject to subsection 2.4 below, if Synack receives a request or demand from a Data Subject or third party for information regarding Customer Personal Data, Synack will promptly provide a copy of that request to Customer. Synack will cooperate with Customer to enable it to respond to the request, including providing Customer with any information or erasure of information to satisfy the request within a commercially reasonable period and in compliance with the Privacy and Security Laws.

2.3 Upon instruction from Customer and upon termination of the Agreement (or Customer's request, if earlier in time), Synack will either return all Customer Personal Data in a commercially acceptable format to Customer or securely destroy all Customer Personal Data, unless retention is required by law. At Customer's request, Synack will provide a signed certification that Customer Personal Data has been destroyed. If required to retain Customer Personal Data by law, Synack will securely store the data and continue to safeguard such data in accordance with this Addendum.

2.4 Synack will not sell or disclose Customer Personal Data to any third parties except as permitted by this Addendum or the Agreement, unless required by law, in which case Synack will (to the extent permitted by law) notify Customer in writing and liaise with Customer before complying with such disclosure request.

2.5 Subject to the terms herein, Synack will limit access to Customer Personal Data only to Synack Personnel, subcontractors, and other third parties who require access as part of the Synack Services.

2.6 Synack will ensure that its employees who access Customer Personal Data: (a) are informed of the Personal Data's confidential nature and use restrictions; (b) have undertaken training on the Privacy and Security Laws relating to handling Personal Data and how it applies to their particular duties; and (c) are aware both of Synack's duties and of their personal duties and obligations under the Privacy and Security Laws.

2.7 Synack agrees to treat all Customer Personal Data as strictly confidential and will ensure that all Synack Personnel, subcontractors, or other third parties with access to Customer Personal Data are bound by confidentiality obligations.

3. SUBPROCESSORS.

3.1 Customer agrees that Synack may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Sub-processors currently engaged by Synack and authorized by Customer are listed in Annex III of the Appendix of the SCCs attached hereto and will be updated from time to time according to the process described in more detail in such Annex.

3.2 Synack shall: (a) enter into a written agreement with each Sub-processor containing data protection obligations are substantially similar to the data protection obligations contained in this Addendum; and (b) remain responsible for such Sub-processor's compliance with the obligations of this Addendum and for any acts or omissions of such Sub-processor that cause Synack to breach any of its obligations under this Addendum.

4. AUDIT.

4.1 Synack shall make available to Customer upon Customer's written request information necessary to demonstrate compliance with this Addendum.

4.2 Synack shall permit, when Customer has reasonable cause to believe Synack is in non-compliance with its obligations under this Addendum, Customer or a mutually agreed-upon third party (the "*Auditor*") to perform an audit in relation to Synack's Processing of Customer Personal Data in compliance with this Addendum. Synack acknowledges that the Auditor may enter its premises for the purposes of conducting this audit, subject to Government security requirements,provided that Customer gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Synack's operations. Customer will not exercise its audit rights more than once in any twelve (12) calendar month period and shall bear all costs associated with the audits.

5. SECURITY MEASURES.

5.1 Synack shall adhere to the technical and organizational measures in Exhibit B to the Agreement (Information Security Standards) as the minimum standards during the term of the Agreement. Synack is free to replace the measures described in Exhibit B by others as long as the minimum standards are still met or exceeded. In exceptional cases, individual measures may be waived by the parties to an Agreement as long as (a) the level of data protection concretely required for the specific data Processing is not compromised, (b) it is necessary for the implementation of the specific data Processing and (c) Customer has agreed to such a deviation in advance in writing.

5.2 In the event Synack discovers or becomes aware of a Security Incident relating to Customer Personal Data, Synack will: (a) notify Customer without undue delay, but in any case, no later than forty-eight (48) hours of becoming aware of the Security Incident; (b) investigate the Security Incident; (c) keep Customer apprised of Synack's investigation; and (d) provide reasonable assistance in relation to any required notifications to regulators or Data Subjects.

6. DATA TRANSFERS.

6.1 Synack shall not transfer or authorize the transfer of Customer Personal Data from a country within the European Economic Area, Switzerland or the UK to a country outside the European Economic Area, Switzerland or the UK except: (a) to a third country recognized by the European Commission or the relevant competent authorities of Switzerland or the UK, as applicable, as providing an adequate level of protection for personal data in accordance with the Privacy and Security Laws, (b) in compliance with Section 6.2 of this Addendum, or (c) otherwise in accordance with the Privacy and Security Laws.

6.2 Synack and Customer each agree that, for Customer Personal Data transferred from Customer to Synack, whether directly or via an onward transfer: (a) where such Customer Personal Data Processing is subject to the EU GDPR, the Standard Contractual Clauses ("*SCC*"), attached to this Addendum as Attachment 1 will apply, (b) where such Customer Personal Data Processing is subject to the UK GDPR, the UK International Data Transfer Addendum to the SCCs, attached as Addendum A to Attachment 1 shall apply, and (c) where such Customer Personal Data Processing is subject to the data protection laws of Switzerland, the Swiss Addendum to the SCCs, attached as Addendum B to Attachment 1 shall apply.

7. WARRANTY AND REMEDIES.

7.1 Synack will at all times comply with the United States Federal Privacy and Security Laws. Synack represents and warrants that nothing in the Privacy and Security Laws prevents it from performing the Synack Services or its obligations as described in this Addendum or the Agreement.

7.2 Customer will at all times comply with the Privacy and Security Laws, including obtaining all required consents and giving all required notices to enable Synack to Process the Customer Personal Data in accordance with the Agreement and this Addendum. Customer represents and warrants that nothing in the Privacy and Security Laws prevents Synack from performing the Synack Services or Synack's obligations as described in this Addendum or the Agreement, including fulfilling the Customer instructions regarding Customer Personal Data.

7.3 Synack represents and warrants that the information Synack provided to Customer in assessing its security measures, including Exhibit B to the Agreement, and any additional assessment questionnaires, is complete and accurate.

7.4 Reserved.

7.5 Notwithstanding anything to the contrary in this Addendum or in the Agreement, the liability of either Party for any breach of this Addendum shall be subject to the limitations of liability provisions set forth in the Agreement.

8. MISCELLANEOUS.

8.1 This Addendum will be effective from the last date set forth below and shall remain in effect throughout the term of the Agreement. In the event of the expiration or termination of the Agreement or this Addendum, Synack's obligations described in Section 2 of this Addendum (Processing of Customer Personal Data) will survive for so long as Synack holds, stores or otherwise Processes Customer Personal Data.

8.2 All notices sent pursuant to this Addendum shall comply with the notice section set forth in the Agreement.

8.3 Except as required by the Privacy and Security Laws, any dispute relating to this Addendum shall be governed by and interpreted in accordance with the law of the country and subject to the jurisdiction referred to in the Agreement.

ATTACHMENT 1 TO DATA PROCESSING ADDENDUM:

STANDARD CONTRACTUAL CLAUSES

MODULE 2: CONTROLLER TO PROCESSOR TRANSFER

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 Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "*entity/ies*") transferring the personal data, as listed in Annex I.A. (hereinafter each "*data exporter*"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "*Clauses*").

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

---

[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 of 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 […].

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:

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

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - 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 Annex I.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 the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.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 Annex I.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 Annex I.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 the 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

[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.

(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

(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 thirty (30) days 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.

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

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 residence 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.

(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 I.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];

[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

(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. 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

(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.

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.

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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland (without reference to conflicts of law principles).

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 the jurisdiction specified in Clause 17 above.

(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.

ADDENDUM A TO THE STANDARD CONTRACTUAL CLAUSES:

UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES FOR TRANSFERS OUT OF UK TO THIRD COUNTRIES

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.

Part 1: Tables

Table 1: Parties

Start date	Effective Date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Appendix, Annex I	See Appendix, Annex I
Key Contact	See Appendix, Annex I	See Appendix, Annex I
Signature (if required for the purposes of Section 2)	See Appendix, Annex I	See Appendix, Annex I

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date Reference (if any): Attachment I to the Data Processing Addendum

Table 3: Appendix Information

"**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:

Annex 1A: List of Parties: See Appendix, Annex I
Annex 1B: Description of Transfer: See Appendix, Annex I
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Appendix, Annex I
Annex III: List of Sub processors (Modules 2 and 3 only): See Appendix, Annex III

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

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.

ADDENDUM B TO THE STANDARD CONTRACTUAL CLAUSES:

SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES FOR TRANSFERS OUT OF SWITZERLAND TO THIRD COUNTRIES

(a) This Addendum amends the Standard Contractual Clauses to the extent necessary so they operate for transfers made by the data exporter to the data importer, to the extent that the Swiss DPA applies to the data exporter's processing when making that transfer. "**Swiss DPA**" shall mean the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced.

(b) The Standard Contractual Clauses shall be amended with the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

(iii) references to Regulation (EU) 2018/1725 shall be removed;

(iv) references to "EU", "Union" and "Member State" shall be replaced with references to "Switzerland";

(v) Clause 13(a) and Part C of Annex II are not used and the "competent supervisory authority" shall be the Swiss Federal Data Protection Information Commissioner ;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);

(vii) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

(viii) to the extent the Swiss DPA applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts".

APPENDIX

Annex I

A. LIST OF PARTIES

Data exporter(s):

Company Name	*End User*
Company Address	*End User Address set forth in Order Form.*
Contact Person Name	*End User Address contact set forth in Order Form.*
Contact Person Position	*End User Address contact set forth in Order Form.*
Contact Person Address	*End User Address contact set forth in Order Form.*
Activities relevant to the data transferred	Receipt of cybersecurity vulnerability testing services
Role (controller / processor)	Controller

Data importer(s):

Company Name	Synack, Inc.
Company Address	Synack, Inc. 303 Twin Dolphin Drive, 6th Floor Redwood City, CA 94065 USA
Contact Person Name	Stephen Soper
Contact Person Position	General Counsel
Contact Person Address	Synack, Inc. 303 Twin Dolphin Drive, 6th Floor Redwood City, CA 94065 USA legal@synack.com
Activities relevant to the data transferred	Provision of cybersecurity vulnerability testing services
Role (controller / processor)	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- Individuals signing onto Synack's user platform on behalf of Client; and
- Any personal data processed during the course of cybersecurity vulnerability testing.

Categories of personal data transferred:

- Basic account information of individuals signing onto Synack's user platform on behalf of Client (username, password, email) and user activity while on Synack's user platform; and
- Any personal data processed during the course of cybersecurity vulnerability testing

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

Not applicable.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

For user activity of individuals signing onto Synack's platform, the data is transferred on a continuous basis when the individual uses the Synack platform. All other transfers of data occur on a one-off basis.

Nature of the processing:

For Synack platform user account information and platform user activities: collection, use, analysis, storage.

Any additional personal data processed during the course of cybersecurity vulnerability testing will be incidental in nature.

Purpose(s) of the data transfer and further processing:

Provide and improve cybersecurity vulnerability testing services pursuant to a Services Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Account details of individuals signing onto Synack's platform will be retained as long as the Client maintains an account on the platform or otherwise in accordance with the Services Agreement or applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Personal data processed by sub-processors is processed for the purposes and duration of the relevant Synack services agreement or ordering document. For more information on the nature and subject matter of the processing, see Annex I.B.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: Republic of Ireland

APPENDIX

Annex II

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

Description of the technical and organizational security measures implemented by the Data Importer can be found in the Information Security Addendum ("ISA"). Where applicable, the ISA will serve as Annex II to the Standard Contractual Clauses.

The following table provides additional information for referencing certain technical and organizational security measures in the ISA.

Measures of pseudonymisation and encryption of personal data	See Section 2.4 (Disclosure Control) of the ISA
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	See Section 2.7 (Availability Control) of the ISA
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	See Section 2.7 (Availability Control) of the ISA
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	See Section 2.9 (Audit) of the ISA
Measures for user identification and authorisation	See Sections 2.2 (Access Control to Systems) and 2.3 (Access Control to Data) of the ISA
Measures for the protection of data during transmission	See Section 2.4 (Disclosure Control) of the ISA
Measures for the protection of data during storage	See Sections 2.7 (Availability Control) and 2.8 (Segregation Control) of the ISA
Measures for ensuring physical security of locations at which personal data are processed	See Section 2.1 (Access Control to Premises and Facilities) of the ISA
Measures for ensuring events logging	See Sections 2.1 (Access control to premises and facilities), 2.4 (Disclosure Control) and 2.5 (Input Control) of the ISA
Measures for ensuring system configuration, including default configuration	See Section 2.9 (Audit) of the ISA
Measures for internal IT and IT security governance and management	See Sections 2.2 (Access Control to Systems) and 2.3 (Access Control to Data) of the ISA

Measures for certification/assurance of processes and products	See Section 2.9 (Audit) of the ISA
Measures for ensuring data minimisation	See Section 2.6 (Job Control) of the ISA
Measures for ensuring data quality	See Section 2.6 (Job Control) of the ISA
Measures for ensuring limited data retention	See Section 2.6 (Job Control) of the ISA
Measures for ensuring accountability	See Sections 2.6 (Job Control) and 2.9 (Audit) of the ISA
Measures for allowing data portability and ensuring erasure	See Section 2.7 (Availability Control) of the ISA
Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	When Synack engages a sub-processor under Section 3 (Subprocessors) of this Addendum, Synack and the sub-processor enter into an agreement with data protection obligations substantially similar to those contained in this Addendum.

APPENDIX

Annex III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Subprocessor Name	Description of Processing	Synack Services	Corporate Location
Amazon Web Services, Inc.	Data hosting provider	Commercial Only	USA
Appcues, Inc.	Onboarding	Commercial Only	USA
Atlassian, Inc.	Collaboration	Commercial Only	USA
DUO Security (Cisco Systems, Inc.)	Two factor authentication	Commercial and FedRAMP	USA
Gainsight	Customer Success / Business Insight	Commercial Only	USA
Google Cloud Platform	Data hosting provider / Infrastructure Monitoring	Commercial and FedRAMP	USA
Microsoft Azure (Microsoft Corporation)	Data hosting provider / Infrastructure Monitoring	Commercial and FedRAMP	USA
Microsoft Defender Advanced Threat Protection	Endpoint Detection and Response	Commercial and FedRAMP	USA
NowSecure, Inc.	On-Device Mobile Testing (Mobile testing only)	Commercial Only	USA
Palo Alto Networks, Inc.	Secure Remote Access (Prisma Access) and Cloud Workload Protection / Cloud Security Posture Management (Prisma Cloud)	Commercial and FedRAMP	USA
Red Maple Technologies Limited	Scanning (Attack Surface Discovery & Digital Reconnaissance only)	Commercial Only	United Kingdom
Salesforce, Inc.	Customer Onboarding	Commercial and FedRAMP	USA
Sendgrid (Twilio Inc.)	Email delivery	Commercial Only	USA
SpyCloud Inc.	Breach detection	Commercial Only	USA
Zendesk, Inc.	Support Ticketing System	Commercial and FedRAMP	USA

Synack Third-Party Subprocessors may be updated from time to time at the following location: https://www.synack.com/data-processing-addendum/#subprocessorlist. Any changes to Synack Third Party Subprocessors will be posted to the foregoing site and Customer shall have ten (10) business days to object to the appointment in writing. If Customer does not object within ten (10) business days, the appointment will be deemed to be approved pursuant to Section 3.1 of the Data Processing Addendum. If the Customer does object, Synack and Customer will cooperate in good faith to resolve the objection.