DATA PROCESSING AGREEMENT FOR JAMF CUSTOMERS

This Data Processing Agreement (the "**DPA**"), effective as of the date of the last signature below (the "**Effective Date**"), is made by and between JAMF Software, LLC, a Minnesota limited liability company, having a principal place of business at 100 Washington Ave. S., Suite 1100, Minneapolis, MN 55401-2155 USA, and its affiliates ("**Jamf**") and the organization identified below ("**Customer**"), each a "**Party**" and collectively the "**Parties**."

1. **Subject Matter of this DPA**. This DPA supplements either Jamf's Software License and Services Agreement or such other negotiated agreement (as applicable) between the Parties pursuant to which Jamf provides Software and/or Services to Customer, along with any subsequent amendments or orders (the "**Agreement**"). It is applicable when Data Protection Laws apply to Customer's use of the Services to Process Personal Data. In consideration of the mutual obligations hereto, the Parties agree that the terms of this DPA will form part of the Agreement, which shall remain in full force and effect except as modified below.

2. **Definitions.** The following defined terms are used in this DPA, together with other terms defined herein.

   a) "**Data Protection Laws**" means all applicable data protection, privacy, and cyber security laws, rules, and regulations of any country, including (where applicable and without limitation) the GDPR, the UK GDPR, the Swiss Data Protection Act, data protection laws of the European Union ("**EU**"), European Economic Area ("**EEA**") member states, or the United Kingdom ("**UK**") that supplement the GDPR or UK GDPR (respectively), and the California Consumer Privacy Act of 2018 ("**CCPA**").

   b) "**Data Subject**" means the individual to whom the Personal Data relates, which is Processed for the performance of the Agreement by Jamf.

   c) "**GDPR**" means the EU General Data Protection Regulation 2016/679.

   d) **"EEA Standard Contractual Clauses**" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data in countries not otherwise recognised as offering an adequate level of protection for Personal Data by the European Commission (as amended and updated from time to time) as set out in Schedule 4.

   e) "**ex-EEA Transfer**" means a processing activity whereby Personal Data which is Processed in accordance with the GDPR is transferred from the Customer to Jamf (or its premises) outside the EEA, and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

   f) "**ex-UK Transfer**" means a processing activity whereby Personal Data which is Processed in accordance with the UK Data Protection Laws is transferred from the Customer to Jamf (or its premises) outside the UK, and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR**.**

   g) "**Personal Data**" means any personal data (as defined in applicable Data Protection Laws) Processed by Jamf (or any Subprocessor) as part of Jamf's performance of the Agreement or provision of the Services to Customer.

   h) **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, transmitted, stored, or otherwise Processed.

   i) "**Processing**" or "**Process**" means any operation or set of operations that is performed upon Personal Data, whether by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure, or destruction.

   j) "**Secretary of State**" means the Secretary of State in the United Kingdom.

   k) "**Services**" means the same services that Jamf provides to Customer as defined in the Agreement.

   l) "**Subprocessor**" means any person or entity appointed by or on behalf of Jamf that Processes Personal Data.

m) "**UK GDPR**" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018. Where the UK GDPR applies to the Processing of Personal Data under this DPA, references in this DPA to the GDPR and to provisions of the GDPR shall be construed as references to the UK GDPR and to the corresponding provisions of the UK GDPR, and references to EU or Member State law shall be construed as references to UK law.

n) "**UK Addendum**" means the UK Addendum to the EEA Standard Contractual Clauses as set out in Schedule 5, as may be amended, replaced or superseded by the ICO from time to time (including when formally issued by the ICO under section 119A(1) Data Protection Act 2018).

3. **CCPA Processing of Personal Data**. In connection with Jamf's provision of Services to Customer, if the CCPA applies and Jamf receives any Personal Data from or on behalf of Customer, then:

a) Jamf will not retain, use, or disclose such Personal Data (i) for any purpose other than to perform the Services or (ii) outside of the direct business relationship between Customer and Jamf;

b) Jamf will not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate such Personal Data to any third party for monetary or other valuable consideration;

c) Jamf certifies that it understands the restrictions on Jamf's Processing such Personal Data as set forth in this Section and will comply with them;

d) Jamf may disclose Personal Data to Jamf's service providers in connection with such service providers providing services to Jamf and Jamf may permit such service providers to Process Personal Data as necessary for Jamf to provide the Services to Customer; and

e) Jamf may combine Customer's Personal Data with Personal Data received from other entities to the extent necessary to detect security incidents or protect against fraudulent or illegal activity, to the extent that Jamf acts as a "service provider" as defined in California Civil Code § 1798.140(v) with regard to all such Personal Data.

4. **Processing of Personal Data.**

a) Jamf's Processing of Personal Data. Jamf will Process Personal Data in accordance with the requirements of Data Protection Laws and only upon Customer's documented instructions, except where Processing is otherwise permitted by Data Protection Laws.

b) Transfers of EEA Personal Data. The EEA Standard Contractual Clauses (attached as Schedule 4) will apply to any ex-EEA Transfer of Personal Data between Customer (as data exporter) and Jamf (as data importer) with Annex 1 completed with information set out in Schedule 1, Annex II completed with information set out in Schedule 3, and Annex III completed with information in Schedule 2.

c) Transfers of UK Personal Data. The EEA Standard Contractual Clauses will apply to any ex-UK Transfer of Personal Data between Customer (as data exporter) and Jamf (as data importer) as amended by the UK Addendum (attached as Schedule 5) with the Part 1 tables completed as follows:

i) Table 1 shall be deemed completed with the information set out in Schedule 1;

ii) in Table 2, the first option shall be selected and the relevant version of the Approved EU SCCs (as defined in Schedule 5) referenced in that option shall be the EEA Standard Contractual Clauses referenced in Section 4 b) above;

iii) Table 3 shall be deemed completed as set out in Section 4 b) above; and

iv) Table 4 shall be deemed completed such that Jamf (as data importer) has the right to end the UK Addendum as set out in Section 19 of Part 2 of the UK Addendum.

d) Further Assurance. If Data Protection Law requires Customer to execute the EEA Standard Contractual Clauses (for ex-EEA Transfers) and/or UK Addendum (for ex-UK Transfers) applicable to a particular transfer of Personal Data to Jamf as a separate agreement, Jamf will, on request of the Customer, promptly execute such EEA Standard Contractual Clauses and/or UK addendum incorporating such amendments as may reasonably be required by Customer to reflect the applicable sections and Schedules of this DPA, the details of the transfer, and the requirements of the relevant Data Protection Law. If either (i) any of the means of legitimising transfers of Personal Data outside of the EEA or UK which are referred to in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Jamf may, by notice to Customer and with effect from the date set out in such notice, amend or put in place alternative arrangements for such transfers, as required by the relevant Data Protection Law.

e) Supplementary measures. For any ex-EEA or ex-UK Transfers, the following supplementary measures will apply:

i) Jamf represents and warrants that, at the time of the transfer, it has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the relevant Personal Data is being exported, for access to (or for copies of) Personal Data that has been transferred to Jamf pursuant to this Agreement ("**Government Agency Requests**");

ii) if, after the Effective Date of this DPA, Jamf receives any Government Agency Requests, it will (unless prohibited by law from doing so) inform the Customer in writing as soon as reasonably practicable and the Customer and Jamf will (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of such Government Agency Requests; and

iii) the Customer and Jamf will meet regularly to consider whether:

1) the protection afforded by the laws where Jamf is based to Data Subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA and/or the UK;

2) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Law; and

3) it is still appropriate for Personal Data to be transferred to Jamf, considering all relevant information available to the Parties, together with guidance provided by the supervisory authorities.

f) Details of Processing. Jamf will Process the Personal Data only as necessary for the performance of the Agreement, as provided for under this DPA or the Agreement, or as otherwise agreed in writing between the Parties, and as further described in Schedule 1 (*Details of Processing*).

g) Types of Personal Data. On behalf of the Customer, Jamf Processes the Personal Data that is necessary for the performance of the Agreement. This includes the types of Personal Data as set out in Schedule 1.

h) Categories of Data Subjects. The categories of Data Subjects whose Personal Data Jamf Processes on behalf of the Customer under this DPA are set out in Schedule 1.

5. **Subprocessors**

a) Approved Subprocessors. The Customer hereby authorizes the Processing of Personal Data by the Subprocessors listed in Schedule 2 (*Approved Sub-Processors*). Jamf will notify the Customer of any changes in Subprocessors, including the addition or replacement of Subprocessors, thereby giving the Customer the opportunity to object to such changes. If, within thirty (30) business days of receipt of this notice, the Customer has not objected to the intended change, the Customer is deemed to have authorized the intended change.

b) Contract with Subprocessor. Jamf will impose on all Subprocessors written data protection obligations that offer at least the same protection of Personal Data as the data protection obligations to which Jamf is bound in the Agreement and this DPA. To the extent that a transfer of Personal Data between Jamf and a Subprocessor constitutes an ex-EEA or ex-UK Transfer, the Customer hereby authorizes Jamf to enter the EEA Standard Contractual Clauses (for an ex-EEA Transfer) and/or the UK Addendum (for an ex-UK Transfer) with the Subprocessor for and on its behalf. Jamf will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors that cause Jamf to breach any of Jamf's obligations under this DPA.

6. **Rights of Data Subjects.**

a) Correction, Blocking, and Deletion. To the extent Customer does not have the ability to correct, amend, block, or delete Personal Data, as required by Data Protection Laws, Jamf will comply with any commercially reasonable request by Customer to facilitate such actions and provide such other assistance in relation to rights of Data Subjects to the extent Jamf is legally required to do so. Customer is responsible for any costs arising from Jamf's assistance to the extent any such assistance exceeds the scope of Jamf's obligations under Data Protection Laws and/or routine customer service.

b) Data Subject Requests. Should a Data Subject contact Jamf about correcting or deleting its Personal Data, Jamf will use commercially reasonable efforts to forward such requests to Customer. Jamf will not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. Jamf will provide Customer with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data. Customer is responsible for any costs arising from Jamf's assistance to the extent such assistance exceeds the scope of Jamf's obligations under Data Protection Laws and/or routine customer service.

7. **Jamf Personnel.**

a) Confidentiality. Jamf will ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Jamf will ensure that such confidentiality obligations survive the termination of the personnel engagement.

b) Reliability. Jamf will take commercially reasonable steps to ensure the reliability of any Jamf personnel engaged in the Processing of Personal Data.

c) Limitation of Access. Jamf will ensure that access to Personal Data is limited to personnel performing Services in accordance with the Agreement.

d) Privacy Officer. Jamf has appointed a privacy officer. The appointed person may be reached at privacy@Jamf.com.

8. **Security.** Jamf has implemented and will maintain technical and organizational measures to secure Personal Data against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data and will comply with Data Protection Laws by taking the security measures set out in Schedule 3 (*Security Measures*). Jamf will ensure an appropriate level of security, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects.

9. **Personal Data Breach Management and Notification.** Jamf maintains security incident management policies and procedures and will notify Customer of a Personal Data Breach of which Jamf becomes aware without undue delay and provide such further assistance as may be required by Data Protection Laws. To the extent such Personal Data Breach is caused by Jamf's violation of the requirements of this DPA, Jamf will make reasonable efforts to identify and remediate

the cause of such Personal Data Breach. If a Personal Data Breach is caused by Customer's violation of the requirements of this DPA, Customer will make reasonable efforts to identify and remediate the cause of such Personal Data Breach.

10. **Data Protection Impact Assessments.** Where the Customer is required to complete a data protection impact assessment or privacy impact assessment under Data Protection Laws, Jamf, upon written request by the Customer, will provide reasonable assistance to the Customer in relation to that requirement. Customer is responsible for any costs arising from Jamf's assistance to the extent such assistance exceeds the scope of Jamf's obligations under Data Protection Laws and/or routine customer service.

11. **Audits.** Jamf allows for, cooperates with, and contributes to audits, including inspections, conducted by Customer or an external auditor engaged by Customer. Audits may be conducted: (i) from time to time on reasonable notice, but no more than once annually; (ii) during normal business hours and so as not to unreasonably interfere with Jamf's performance of the Services under the Agreement or unreasonably interfere with Jamf's business; and (iii) during the term of this DPA. The notice requirement in this section 11(i) and the restrictions stated in 11(ii) will not apply to the extent the audit is initiated by a regulator. Jamf will provide to Customer, its auditors, and regulators reasonable assistance so they can perform an audit, including permitting them access to the following: the place, premises, and facilities from which the Services will be performed; the systems (including software, networks, firewalls, and servers) used to perform the Services; and data, records, manuals, and other information relating to the Services. Jamf will not be required to give auditors any access or information that may cause Jamf to compromise its own internal, legal, or regulatory compliance obligations, is subject to confidentiality obligations with its customers, vendors, or other third parties, or is commercially sensitive (such as trade secrets). If an audit results in Jamf being notified that it, or its Processing of Personal Data, does not comply with Data Protection Laws, the Parties will discuss that finding and, with respect to any such non-compliance, Jamf will take corrective actions to achieve compliance to the reasonable satisfaction of the auditor.

12. **Term**

    a) Duration. The term of this DPA is the same as the term of the Agreement. Regardless of the termination of this DPA, Jamf is obliged to comply with the provisions of this DPA as long as Personal Data are Processed by Jamf on behalf of Customer.

    b) Obligation to Delete or Return Personal Data. Upon termination or expiration of the Agreement and this DPA, and, at the choice of and upon Customer's written request, Jamf will, return the Personal Data and all copies thereof to the Customer and/or will securely destroy (delete) the Personal Data and all existing copies thereof in accordance with the Agreement, except to the extent continued storage is required under applicable laws and permitted under Data Protection Laws. In such case, Jamf will inform the Customer of such legal obligation, keep the Personal Data confidential, and only Process the Personal Data to the extent required by applicable laws.

13. **Limitation of Liability**. **NEITHER JAMF NOR ANY OF JAMF'S AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS, OR FAILURE TO STORE ANY PERSONAL DATA. IN ANY CASE, JAMF'S AND JAMF'S AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS DPA WILL NOT EXCEED THE AMOUNT CUSTOMER ACTUALLY PAYS JAMF UNDER THE AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE. THE EXCLUSIONS AND LIMITATIONS IN THIS SECTION 13 APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.**

14. **General Provisions.**

    a) Entire Agreement/Order of Precedence. This DPA constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior understandings regarding such subject matter, whether written or oral. To the extent a conflict exists between this DPA and the Agreement regarding the subject matter of this DPA, the terms of this DPA will govern. To the extent a conflict exists between this DPA and the EEA Standard Contractual Clauses (for an ex-EEA Transfer) or UK Addendum (for an ex-UK Transfer) regarding the subject matter of this DPA, the EEA Standard Contractual Clauses or UK Addendum will govern.

b) Amendment. No amendment or modification of this DPA will be binding unless in writing and signed by the Parties.

c) Waiver. Any waiver by a Party of a breach of any provision of this DPA will not operate as or be construed as a waiver of any further or subsequent breach.

d) Survival. Provisions of this DPA that by their nature are to be performed or enforced following any termination of this DPA will survive such termination.

e) Assignment. Jamf may assign this DPA to an affiliate or in connection with a merger of Jamf or the sale of substantially all Jamf's assets.

f) Binding Effect. This DPA will be binding upon and inure to the benefit of the Parties, their successors, and permitted assigns.

g) Unenforceability and Severability. If for any reason, a court of competent jurisdiction or duly appointed arbitrator finds any provision or portion of this DPA to be unenforceable, the remainder of this DPA will continue in full force and effect.

h) Translations. If this DPA is translated into languages other than English, the English version will control.

i) Headings. The headings are for convenience only and do not affect the interpretation of this DPA.

j) Counterparts. This DPA may be executed by electronic signature and in counterparts, which together constitute one binding agreement.

k) Third Party Rights. Except to the extent expressly provided by the EEA Standard Contractual Clauses or UK Addendum with respect to Data Subjects, this DPA does not give rise to any rights for third parties to enforce any term of this DPA.

15. **Authority of Signatories**. Each person signing this DPA represents and warrants that they are duly authorized and have legal capacity to execute it.

Jamf Software, LLC

Signature:

Name:

Title:

Date:

Jamf Internal Account Reference:

Customer

Signature:

Name:

Title:

Date:

Full Company Legal Name:

Type of Legal Entity:

Street Address:

State/Province:

Postal Code:

SCHEDULE 1
DETAILS OF PROCESSING

A. List of Parties

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: _____

Address: _____

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

_____

Activities relevant to the data transferred under these Clauses: use of Services provided by Jamf.

Signature and date: _____

Role (controller/processor): Controller
Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: JAMF Software, LLC

Address: 100 Washington Avenue South, Suite 1100, Minneapolis, MN 55401 USA

Contact person's name, position, and contact details: Justin Francis, Vice President, Enterprise Risk & Compliance; privacy@jamf.com; +1 612-605-6625

Activities relevant to the data transferred under these Clauses: Jamf's provision of Services under the Agreement.

Signature and date: _____

Role (controller/processor): Processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is transferred: employees of Customer (and students of Customer if Customer is an education customer).

Categories of Personal Data transferred: Names, IP addresses, telephone numbers, computer names, job titles and functions, and email addresses.

Sensitive data/special categories transferred (if any): none.

Frequency of transfer: the frequency of the transfer of Personal Data is directly related to the nature of processing.

Nature of the Processing: Process Personal Data if Customer enters Personal Data into Customer's instance of the Hosted Services provided by Jamf pursuant to the Agreement. Jamf utilizes subprocessors for infrastructure to provide the Hosted Services in which Personal Data is stored.

Purpose(s) of the data transfer and further processing: the purpose of data transfers is for Customer to utilize Jamf's Services.

The period for which Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: Personal Data is retained in accordance with the Agreement and this DPA.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the Processing: Jamf utilizes the approved Subprocessors set forth in and as further described in Schedule 2. The duration of the Processing is equivalent to the length of time Customer utilizes Jamf's Services under the Agreement.

C. Competent Supervisory Authority (identify the competent supervisory authority/ies in accordance with Clause 13 of Schedule 4 to the DPA (EEA Standard Contractual Clauses)): The competent supervisory authority is identified in Clause 13 of the EEA Standard Contractual Clauses and shall be either 13 (a) (i), (ii), or (iii), whichever is applicable to Customer (data exporter).

SCHEDULE 2
APPROVED SUBPROCESSORS

Jamf's subprocessor list can be found at https://www.jamf.com/jamf-subprocessors/.

SCHEDULE 3
SECURITY MEASURES

Processing of Personal Data takes place on data processing systems for which technical and organizational measures for protecting such data have been implemented. In this context, Jamf assures Customer that it will take all reasonable measures required to ensure such Processing is done in accordance with applicable Data Protection Laws. Considering the state of technological development and the cost of implementing such measures, Jamf will ensure a level of security appropriate to the harm that might result from unauthorized or unlawful Processing or accidental loss, destruction, or damage, considering the nature of the Personal Data to be protected.

Jamf will implement the following measures:

1. **Information Security Policies and Measures**

   a) Policies. Jamf's information security policies will be documented and approved by Jamf's senior management.

   b) Review of the Policies. Jamf's information security policies will be reviewed by Jamf at least annually, or promptly after material changes are made to the policies to confirm applicability and effectiveness. Jamf will not make changes to the policies that would materially degrade Jamf's security obligations.

   c) Information Security Reviews. Jamf will independently review its approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) at planned intervals or when significant changes occur.

   d) Disaster Recovery. During the term of the Agreement, Jamf will maintain a disaster recovery (DR) or high availability (HA) solution and related plan that is consistent with industry standards for the Services Jamf provides to Customer. Jamf will test the DR or HA solution and related plan at least once annually. In addition, the solution and related plan will ensure:

      i) that installed systems used to provide Services will be restored in case of interruption;

      ii) Jamf's ability to restore the availability and access to Customer Content in a timely manner in the event of a physical or technical incident; and

      iii) the ongoing confidentiality, integrity, availability, and resilience of systems Jamf uses to provide Services.

   e) Testing. Jamf will maintain a process for regularly testing the effectiveness of its technical and organizational measures for ensuring the security of the processing of Customer Content.

2. **Information Security Framework**

   a) Security Accountability. Jamf will assign one or more security officers who will be responsible for coordinating and monitoring all information security functions, policies, and procedures.

   b) Security Roles and Responsibility. Jamf personnel, contractors and agents who are involved in providing Services will be subject to confidentiality agreements with Jamf.

   c) Risk Management. Jamf will perform appropriate information security risk assessments as part of an ongoing risk governance program with the following objectives (i) recognize risk, (ii) assess the impact of risk, and (iii) where risk reduction or mitigation strategies are identified and implemented, effectively manage the risk with recognition that the threat landscape constantly changes.

3. **Human Resource Security**

a) Security Training. Jamf will provide appropriate security awareness, education, and training to all Jamf personnel and contractors with access to the Software and Services provided to Customer.

b) Background Screening. Jamf will ensure that background checks have been performed on Jamf personnel who are part of teams managing Jamf's hosting infrastructure. Additionally, background checks will be performed on Jamf personnel or agents assigned to provide Services at Customer's premises. Jamf will perform background checks in accordance with applicable law and Jamf's background screening policies and procedures. Only individuals who have passed background checks will be allowed by Jamf to provide Services at Customer's premises or be part of Jamf's teams managing Jamf's hosted infrastructure.

4. **Asset Management**

a) Asset Inventory.

i) Jamf will maintain an asset inventory of all media and equipment where Customer Content is stored. Jamf will restrict access to such media and equipment to authorized personnel of Jamf. Jamf will prevent the unauthorized reading, copying modification or removal of data media.

ii) Jamf will classify Customer Content so that it is properly identified and will appropriately restrict access to Customer Content. Specifically, Jamf will ensure that no person appointed by Jamf to process Customer Content, will process Customer Content unless that person:

1) has a need to access Customer Content for the purpose of performing Jamf's obligations under the Agreement;

2) has been authorized by Jamf in a manner consistent with Jamf's information security policies;

3) has been fully instructed by Jamf in the procedures relevant to the performance of the obligations of Jamf under the Agreement, in particular the limited purpose of processing Customer Content; and

4) is aware that they are prohibited from copying any Customer Content transmitted by Customer to Jamf, provided, however, that Jamf may retain copies of Customer Content provided to it under the Agreement in its servers for backup and archive purposes until completion of the Agreement.

iii) Jamf will further maintain measures to ensure that persons appointed by Jamf to process Customer Content will prevent the unauthorized input of Customer Content and the unauthorized inspection, modification, or deletion of stored Customer Content.

iv) Jamf will maintain an appropriate approval process whereby approval is provided to personnel, contractors, and agents prior to storing Customer Content on portable devices or remotely accessing Customer Content. All approvals will be subject to measures designed to prevent the unauthorized reading, copying, modification or deletion of Customer Content during transfers of such content or during transportation of data media. If remote access is approved and granted, Jamf personnel, agents, and contractors will use multi-factor authentication. Multi-factor authentication may include techniques such as the use of cryptographic certificates, one-time- password (OTP) tokens, or biometrics.

b) Security of Software Components. Jamf agrees to appropriately inventory all Software components (including open-source software) used with Jamf's Software and Services. Jamf will assess whether any such software components have any security defects and/or vulnerabilities that could lead to unauthorized disclosure of Customer Content. Jamf will perform such assessment prior to delivery of, or providing Customer access to, Jamf's Software and Services and on an on-going basis thereafter during the term of the Agreement. Jamf agrees to remediate any security defect or vulnerability it detects in a timely manner.

5. **Access Control**

a) Policy.

i) Jamf will maintain an appropriate access control policy that is designed to restrict access to Customer Content and Jamf assets to authorized personnel, agents, and contractors. To ensure clarity, all references to user accounts and passwords in this section relate only to Jamf's users, user accounts, and passwords. This Section 5 does not apply to Customer's access to and use of the Software and Services, Customer user accounts, or Customer passwords.

b) Authorization.

i) Jamf will maintain user account creation and deletion procedures for granting and revoking access to all assets, Customer Content, and all Jamf internal applications while providing Software and Services under the Agreement. Jamf will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.

ii) Jamf will maintain and update records of employees and contractors who are authorized to access systems that are involved in providing Software and Services to the Customer and review such records at least quarterly. Administrative and technical support personnel, agents, or contractors will only be permitted to have access to such data when required; provided, such personnel, agents, or contractors comply with applicable Jamf technical and organizational measures.

iii) Jamf will ensure the uniqueness of user accounts and passwords for everyone. Individual user accounts will not be shared.

iv) Jamf will remove access rights of personnel and contractors to assets that store Customer Content upon termination of their employment, contract, or agreement within 24 hours, or adjust access upon change of personnel role.

c) Authentication.

i) Jamf will use industry standard capabilities to identify and authenticate personnel, agents, and contractors who attempt to access information systems and assets.

ii) Jamf will maintain industry standard practices to deactivate passwords that have been corrupted or disclosed.

iii) Jamf will monitor for repeated access attempts to information systems and assets.

iv) Jamf will maintain industry standard password protection practices that are designed to maintain the confidentiality and integrity of passwords generated, assigned, distributed, and stored in any form.

v) Jamf will use multi-factor authentication for all administrative access, including domain and cloud portal administrative access. Multi-factor authentication may include techniques such as the use of cryptographic certificates, one-time-password (OTP) tokens or biometrics.

d) Data-processing Equipment.

i) Jamf will deny unauthorized persons access to systems and equipment used for processing Customer Content ("**Data-Processing Equipment**").

ii) Jamf will prevent the use of automated Data-Processing Equipment by unauthorized persons using data communication equipment.

iii) Jamf will ensure that persons authorized to use an automated Data-Processing Equipment only have access to the Customer Content covered by their access authorization.

iv) Jamf will ensure that it is subsequently possible to verify and establish which Customer Content has been put into automated Data-Processing Equipment when it was added and by whom the input was made.

6. **Cryptography**

a) Jamf will maintain policies and standards regarding the use of cryptographic controls that are implemented to protect Customer Content. Such protections will include the pseudonymization and encryption of Personal Data, as further detailed below in Section 9. Jamf will implement industry standard key management policies and practices designed to protect encryption keys for their entire lifetime.

7. **Physical and Environmental Security**

a) Physical Access to Facilities. Jamf will limit access to facilities where systems that are involved in providing the Services are located to identified personnel, agents, and contractors.

b) Protection from Disruptions. Jamf will use reasonable efforts, and, to the best of Jamf's ability and to the extent within Jamf's control, protect equipment from power failures and other disruptions caused by failures in supporting utilities.

c) Secure Disposal or Reuse of Equipment. Jamf will verify that all Customer Content has been deleted or securely overwritten from equipment containing storage media using industry standard processes prior to disposal or re-use.

8. **Operations Security**

a) Operations Policy. Jamf will maintain appropriate operational and security operating procedures and such procedures will be made available to all Jamf personnel who require them.

b) Protections from Malware. Jamf will maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks.

c) Configuration Management. Jamf will have policies that govern the installation of software and utilities by personnel.

d) Change Management. Jamf will maintain and implement procedures to ensure that only approved and secure versions of the code, configurations, systems, and applications will be deployed in the production environment(s).

e) Encryption of Data. Encryption solutions will be deployed with no less than 256-bit Advanced Encryption Standard (AES) encryption.

f) Systems. Jamf will ensure that the functions of the systems utilized to provide Services perform, that the appearance of faults in the functions is reported, and that stored Customer Content cannot be corrupted by means of a malfunctioning of such systems.

9. **Communications Security**

a) Information Transfer.

i) With respect to Jamf's Hosted Services, Customer Content is encrypted in-transit to the Hosted Services and maintained in encrypted storage. Jamf will use industry standard encryption to encrypt Customer Content.

ii) Jamf will restrict access through encryption to Customer Content stored on media that is physically transported from Jamf facilities.

iii) Jamf will ensure that it is possible to verify and establish the extent to which Customer Content has been or may be transmitted or made available using data communication equipment.

b) Security of Network Services.

i) Jamf will ensure that industry standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced.

c) Intrusion Detection.

i) Jamf will deploy intrusion detection or intrusion prevention systems for all systems used to provide Services to Customer to provide continuous surveillance for intercepting and responding to security events as they are identified and update the signature database as soon as new releases become available for commercial distribution.

d) Firewalls.

i) Jamf will have appropriate firewalls in place which will only allow documented and approved ports and services to be used. All other ports will be in a deny all mode.

10. **System Acquisition, Development and Maintenance**

a) Workstation Encryption. Jamf will require hard disk encryption of at least 256-bit Advanced Encryption Standard (AES) on all workstations and/or laptops used by personnel, contractors, and agents where such personnel are accessing or processing Customer Content.

b) Application Hardening.

i) Jamf will maintain and implement secure application development policies, procedures and standards that are aligned to Industry Standard practices such as the SANS Top 25 Security Development Techniques or the OWASP Top Ten project.

ii) All personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Services and receive appropriate training regarding Jamf's secure application development practices.

c) System Hardening.

i) Jamf will establish and ensure the use of standard secure configurations of operating systems. Images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening includes removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, applying patches, closing open and unused network ports, and implementing intrusion detection systems and/or intrusion prevention systems. These images should be validated on a regular basis to update their security configuration as appropriate.

ii) Jamf will perform periodic (at least quarterly) access reviews for system administrators for all supporting systems requiring access control.

iii) Jamf will implement patching tools and processes for both applications and operating system software. When outdated systems can no longer be patched, Jamf will update to the latest version of application software. Jamf will remove outdated, unsupported, and unused software from the system.

iv) Jamf will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

d) Infrastructure Vulnerability Scanning. Jamf will scan its internal environment (e.g., servers, network devices, etc.) related to the Services monthly and external environment related to the Services on a weekly basis. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed no later than 30 days after discovery.

e) Application Vulnerability Assessment. Jamf will perform an application security vulnerability assessment prior to any new public release. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery.

f) Penetration Tests and Security Evaluations of Websites. Jamf will perform a comprehensive penetration test and security evaluation of all systems and websites involved in providing Services on a recurring basis no less frequent than once annually. Additionally, Jamf will have an industry-recognized independent third party perform an annual test. Jamf will have a defined process to address any findings but will ensure that any high-risk vulnerabilities are addressed within 30 days of discovery. Upon Customer's written request, but no more than once per year, Jamf will provide an assertion statement to validate the completion of the independent third-party penetration test and attest to the fact that Jamf maintains a process to address findings.

11. **Jamf Relationships**

a) If Jamf must use a third-party application or service to provide the Services, Jamf's contract with that third-party vendor must clearly outline security requirements for the third-party vendor consistent with the security requirements of this Information Security Schedule. In addition, service level agreements with the third party must be clearly defined.

b) Any third-party gaining access to Jamf systems must be covered by a signed agreement containing confidentiality and security provisions consistent with the confidentiality and security requirements of the Agreement and this Information Security Schedule.

c) Jamf will perform quality control and security management oversight of outsourced software development.

SCHEDULE 4
EEA Standard Contractual Clauses

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 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.

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 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Reserved

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 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 (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:

(a) 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;

(b) 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;

(c) 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

(d) 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 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. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual 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.

(c) 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.

(d) 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)

(i) Where the data exporter is established in an EU Member State 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.

(ii) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679 the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(iii) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679 the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 ([2]);

(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.

(b) 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.

(c) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(d) 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.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the

data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

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 Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. List of Parties

See Schedule 1 to the DPA.

B. Description of Transfer

See Schedule 1 to the DPA.

C. Competent Supervisory Authority

See Schedule 1 to the DPA.

ANNEX II

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

See Schedule 3 to the DPA.

ANNEX III

LIST OF SUB-PROCESSORS

See Schedule 2 to the DPA.

Schedule 5
UK Addendum

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses
Version B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards (as defined in Table 4, Section 3 below) for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Effective Date of the DPA to which this Schedule 5 is attached.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Section A to Schedule 1 (Details of Processing) of the DPA.	See Section A to Schedule 1 (Details of Processing of the DPA.
Key Contact	See Section A to Schedule 1 (Details of Processing) of the DPA.	See Section A to Schedule 1 (Details of Processing) of the DPA
Signature (if required for the purposes of Section 2)	Deemed signed via signature on the DPA and Schedule 1 of the DPA.	Deemed signed via signature on the DPA and Schedule 1 of the DPA.

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 and as referenced in Section 4 b) of the DPA.

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 Section A of Schedule 1 to the DPA (Details of Processing)
Annex 1B: Description of Transfer: Section B of Schedule 1 to the DPA (Details of Processing)

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 3 to the DPA (Security Measures)

Annex III: List of Sub processors (Modules 2 and 3 only): See Schedule 2 to the DPA (Approved Subprocessors)

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 19: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers (governed by this Addendum), the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed to alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "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";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(a) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or

b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.