DATA PROCESSING AGREEMENT

IN ADDITION TO THE SOFTWARE LICENSE AND SERVICES AGREEMENT, ALONG WITH ANY SUBSEQUENT AMENDMENTS OR ORDERS, (THE "AGREEMENT"), 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") PROVIDES ACCESS TO ITS SOFTWARE AND SERVICES SUBJECT TO THE TERMS AND CONDITIONS SET FORTH IN THIS DATA PROCESSING AGREEMENT (THE "DPA"). PLEASE READ THE TERMS OF THIS DPA CAREFULLY. AS USED IN THIS DPA, "YOU" OR "CUSTOMER" REFER TO YOU, THE PERSON OR ENTITY USING THE SOFTWARE OR RECEIVING THE SERVICES. BY USING THE SOFTWARE AND/OR THE SERVICES, YOU AGREE TO BE BOUND BY THE TERMS OF THIS DPA. IF YOU DO NOT AGREE TO THE TERMS OF THIS DPA, RETURN THE SOFTWARE TO JAMF FOR A REFUND.

THE "EFFECTIVE DATE" OF THIS DPA IS THE DATE YOU ACCEPT THIS DPA AS PROVIDED BELOW. AS USED IN THIS DPA, JAMF AND CUSTOMER ARE EACH A "PARTY", AND ARE TOGETHER THE "PARTIES".

1. **Subject Matter of this DPA.** This DPA supplements the Agreement for the provision of the Services between Customer and Jamf, when the Data Protection Laws and Regulations apply to Customer's use of the Services to process Customer 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. "**Customer Data**" means any Personal Data or Personal Information that is Processed by Jamf (or any Subprocessor) pursuant to Jamf's performance of the Agreement or provision of the Services to Customer.

    b. "**Data Protection Laws and Regulations**" 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 EU or EEA member states or the UK that supplement the GDPR or UK GDPR (respectively), and the California Consumer Privacy Act of 2018 ("**CCPA**").

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

    d. "**GDPR**" means EU General Data Protection Regulation 2016/679.

    e. "**Personal Data**" means any personal data (as defined in the GDPR) Processed by Jamf (or any Subprocessor) pursuant to Jamf's performance of the Agreement or provision of the Services to Customer.

    f. "**Personal Information**" means any personal information (as defined in the CCPA) Processed by Jamf (or any Subprocessor) pursuant to Jamf's performance of the Agreement or provision of the Services to Customer.

g. "**Processing**" means any operation or set of operations that is performed upon Customer Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure or destruction.

h. "**Restricted Transfer**" means a transfer of Personal Data by or to Customer (including an onward transfer of Personal Data between two establishments of Customer) in each case, where such transfer would be prohibited by Data Protection Laws and Regulations in the absence of the Standard Contractual Clauses.

i. "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise processed.

j. "**Services**" means, collectively, Hosted Services, Premium Cloud, JumpStart Services, Support and Maintenance, Premium Support, Premium Services, Training Services and/or other professional services. Services do not include custom development work.

k. "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of protection of Personal Data, which have been approved by the European Commission as adducing adequate safeguards for Restricted Transfers, or any successor clauses thereto or recognized by the European Commission pursuant to Article 46 of the GDPR, or by the relevant Secretary of State where the UK GDPR applies.

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.

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

a. Jamf will not retain, use, or disclose such Personal Information: (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 Information to any third party for monetary or other valuable consideration;

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

d. Jamf may disclose Personal Information 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 Information as necessary for Jamf to provide the Services to Customer; and

e. Jamf may combine Customer's Personal Information with Personal Information 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 Information.

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 Regulations and only upon Customer's documented instructions, except where Processing is otherwise permitted by Data Protection Laws and Regulations.

b. Transfers of Personal Data. The Standard Contractual Clauses (attached as Schedule 4) will apply to any Restricted Transfers of Personal Data between Customer (as data exporter) and Jamf (as data importer).

c. Details of Processing. The Personal Data shall be Processed by Jamf insofar as necessary for the performance of the Agreement, as provided for under this DPA, the Agreement or as otherwise agreed in writing between the Parties, and as further described in Schedule 1 (*Details of Processing*).

d. 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.

e. Categories of Data Subjects. The categories of Data Subjects whose Personal Data are Processed by Jamf 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 shall notify the Customer of any changes concerning the addition or replacement of other 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 shall 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 on the basis of the Agreement and this DPA. To the extent that a transfer of Personal Data between Jamf and a Subprocessor constitutes a Restricted Transfer, the Customer hereby authorizes Jamf to enter into the Standard Contractual Clauses 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 and Regulations, 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.

b. Data Subject Requests. Should a Data Subject contact Jamf with regard to correction or deletion of 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.

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 those 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 the 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 and Regulations by taking the security measures set out in Schedule 3 (*Security Measures*). Jamf shall 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. The measures shall also aim to prevent unnecessary collection and further Processing of Personal Data.

9. **Security Breach Management and Notification.** Jamf maintains security incident management policies and procedures and will notify Customer of a Security Breach of which Jamf becomes aware without undue delay and provide such further assistance as may be required by Data Protection Laws and Regulations. To the extent such Security 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 Security Breach. If a Security 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 Security 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 and Regulations, Jamf, upon written request by the Customer, shall provide reasonable assistance to the Customer in relation to that requirement. Customer is responsible for any costs arising from Jamf's assistance.

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) shall not apply to the extent the audit is initiated by a regulator. Jamf shall provide to Customer and its auditors and regulators reasonable assistance as they require for the purpose of performing an audit, including 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 shall 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, is not in compliance with Data Protection Laws and Regulations, the Parties shall discuss such finding and, with respect to any such non-compliance, Jamf shall take corrective actions to achieve compliance to the reasonable satisfaction of 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 shall, return the Personal Data and all copies thereof to the Customer and/or shall securely destroy (delete) such 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 and Regulations. In such case, Jamf shall inform the Customer of such legal obligation, shall keep the Personal Data confidential and shall only Process the Personal Data to the extent required by the applicable laws.

13. **Miscellaneous**. 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. This DPA will be binding upon and inure to the benefit of the Parties, their successors and permitted assigns. Jamf may assign this DPA to an affiliate or in connection with a merger of Jamf or the sale of substantially all of Jamf's assets. If this DPA is translated into languages other than English, the English version will control. 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. No amendment or modification of this DPA will be binding unless in writing and signed by the Parties. 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. Provisions of this DPA that by their nature are to be performed or enforced following any termination of this DPA shall survive such termination.

14. **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 CUSTOMER 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 15 APPLY ONLY TO THE

MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

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

SCHEDULE 1

DETAILS OF PROCESSING

Nature of the Processing

Process Personal Data if and when Customer enters Personal Data into Customer's instance of the Hosted Services provided by Jamf pursuant to the Agreement. Jamf utilizes AWS for infrastructure to provide the Hosted Services in which Personal Data is stored, if Customer enters Personal Data into the Hosted Services.

Types of Personal Data that may be Processed

Names, IP addresses, telephone numbers, computer names, job titles and functions and email addresses.

Categories of Data Subjects

Employees and/or students of Customer.

SCHEDULE 2

APPROVED SUB-PROCESSORS

Amazon Web Services, Inc. ("**AWS**")

SCHEDULE 3

SECURITY MEASURES

Processing of Customer 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 and Regulations. 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 Customer Data to be protected.

Jamf will implement measures designed to:

a. Deny unauthorized persons access to data-processing equipment used for processing Customer Data (equipment access control);

b. Prevent the unauthorized reading, copying, modification or removal of data media (data media control);
c. Prevent the unauthorized input of Customer Data and the unauthorized inspection, modification or deletion of stored Customer Data (storage control);
d. Prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);
e. Ensure that persons authorized to use an automated data-processing system only have access to the Customer Data covered by their access authorization (data access control);
f. Ensure that it is possible to verify and establish the extent to which an individual's Customer Data has been or may be transmitted or made available using data communication equipment (communication control);
g. Ensure that it is subsequently possible to verify and establish which Customer Data has been put into automated data-processing systems and when and by whom the input was made (input control);
h. Prevent the unauthorized reading, copying, modification or deletion of Customer Data during transfers of those data or during transportation of data media (transport control);
i. Ensure that installed systems may, in case of interruption, be restored (recovery);
j. Ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored Customer Data cannot be corrupted by means of a malfunctioning of the system (integrity);
k. Ensure that no person will be appointed by Jamf to process Customer Data unless that person:
    i. Has a need to access Customer Data for the purpose of performing the obligations under the Agreement;
    ii. Has been authorized by Jamf;
    iii. 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 said Processing; and
    iv. Is aware that it is prohibited to make copies of any Customer Data transmitted by Customer to Jamf, provided, however, that Jamf may retain copies of Customer Data provided to it under the Agreement in its servers for backup and archive purposes until the completion of the Agreement.
l. Ensure the pseudonymisation and encryption of Customer Data;
m. Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
n. Ensure the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident;
o. Ensure a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

SCHEDULE 4

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (These can be located in their original text on the European Commission website here: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

For purposes of this Schedule 4:

any reference to "data exporter" means Customer

and

any reference to "data importer" means Jamf.

each a "**party**"; together "**the parties**".

The parties have agreed on the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

a. *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
b. *'the data exporter'* means the controller who transfers the personal data;
c. *'the data importer'*> means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
d. *'the subprocessor'*> means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
e. *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
f. *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and

obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
e. that it will ensure compliance with the security measures;
f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
g. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
i. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
j. that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
d. that it will promptly notify the data exporter about:
   i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
   ii. any accidental or unauthorised access, and
   iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
e. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
f. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
h. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
i. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
j. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
    a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
    b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data controller is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data controller is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to SCHEDULE 4 Standard Contractual Clauses

This Appendix 1 forms part of the Clauses.

Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself. Activities relevant to the transfer include the performance of Services by data importer for Customer.

Data importer

The data importer is Jamf. Activities relevant to the transfer include the performance of Services for Customer.

Data subjects

Employees and/or students of Customer.

Categories of data

Names, IP addresses, telephone numbers, computer names, job titles and functions, email addresses, usernames, building names, room and location.

Special categories of data

The personal data transferred may concern the following special categories of data:

None.

Processing operations

The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Customer and Jamf: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under applicable law, (c) consulting, professional, storage, hosting and other services delivered to customers, including services offered by means of the products and solutions described by Jamf, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements.

Appendix 2 to SCHEDULE 4 Standard Contractual Clauses

Appendix 2 to Attachment D, the Standard Contractual Clauses, is the Security Measures located at *Schedule 3 of this DPA.*

BY CLICKING THE "AGREE" BUTTON, YOU AGREE TO BE BOUND BY THE TERMS OF THIS DPA. IF YOU DO NOT AGREE TO THE TERMS OF THIS DPA, RETURN THE SOFTWARE TO JAMF FOR A REFUND. NOTWITHSTANDING THE FOREGOING, YOUR USE OF THE SOFTWARE AND/OR SERVICES INDICATES ACCEPTANCE OF THE TERMS OF THIS DPA.

Jamf School Customer DPA v08242020