DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of Arm's Pelion Device Management Terms of Service and sets out how Arm processes Personal Data included in Device Data and Device Specific Data, as required by Data Protection Legislation.

1. PARTIES TO THIS DPA

This DPA is made between the Customer and Arm as both are defined in the Pelion Device Management Terms of Service.

Customer and Arm are hereinafter jointly referred to as the "**Parties**" and each separately as a "**Party**".

2. DEFINITIONS

Unless otherwise defined in this DPA or elsewhere in the Agreement, terms such as "Data Controller", "Data Processor", "Data Subject", and "Supervisory Authority" have the meanings given to such terms in Data Protection Legislation (defined below). In addition:

2.1 "**Data Protection Legislation**" means the General Data Protection Regulation (EU) 2016/679 and the Electronic Communications Data Protection Directive 2002/58/EC, in each case, as amended, revised or replaced from time to time (in particular, by operation of the Directive 2009/136/EC), and all applicable national implementing legislation and guidelines (including if the UK leaves the EU);

2.2 "**Personal Data**" has the meaning given to such term in the Pelion Device Management Terms of Service; and

2.3 "**Personal Data Breach**" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Arm under the Agreement.

3. DETAILS OF DATA PROCESSING

3.1 Subject matter: Arm's provision of the Service to Customer.

3.2 Purpose: as necessary for the provision of the Service to Customer in accordance with the Agreement.

3.3 Nature of processing: computing, storage and such other services as described in the Agreement from time to time.

3.4 Types of personal data: Device Data and Device Specific Data.

3.5 Categories of Data Subjects: Customer End Users or other individuals whose personal data (as defined in GDPR) has been provided to Arm via the Service.

4. CUSTOMER INSTRUCTIONS, LEGAL BASIS AND CONFIDENTIALITY

4.1 Arm shall process Personal Data in accordance with Customer's written instructions as established in this Agreement where Arm acts as a Data Processor, unless otherwise required by EU or EU member state law to which Arm is subject; in such a case, Arm shall inform Customer of such legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 In cases where Customer is also a Data Processor, not a Data Controller, Customer shall ensure that the instructions agreed upon in this DPA provide the same or similar level of data protection as those required by the instructions of the Data Controller. Customer shall inform Arm without undue delay of any additional instructions.

4.3 The Parties agree that this DPA represents Customer's and, as the case may be, the Data Controller's, complete written instructions to Arm. Additional instructions require prior written agreement between the Parties.

4.4 Customer warrants and represents that the Personal Data has been collected under a valid legal basis; that Customer is entitled to share the Personal Data with Arm; that Data Subjects have been informed in an appropriate way about the processing of Personal Data under this DPA, including the use of subprocessors and transfers described herein; that Data Subjects have, where required, given valid consent under Data Protection Legislation or other law applicable to Customer, and that this consent has not been revoked. Customer shall inform Arm without undue delay if a Data Subject has objected to the processing of Personal Data. Customer shall ensure that it has obtained any other authorization required under applicable law for the processing of Personal Data under this DPA, including the use of subprocessors and transfers described herein.

4.5 Arm shall take reasonable steps to ensure that Arm persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. ARM'S OBLIGATION TO ASSIST

5.1 Arm shall, taking into account the information available to Arm and the nature of the processing, provide reasonable assistance to Customer in ensuring compliance with Customer's obligations set out in Data Protection Legislation relating to data security, personal data breaches, data protection impact assessments, and prior consulting obligations with a Supervisory Authority. Arm may charge Customer for costs and expenses incurred as a result of such assistance.

5.2 Arm shall, taking into account the nature of the processing, provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising Data Subject rights set out in Chapter III of the GDPR.

6. DATA SECURITY AND DATA BREACHES

6.1 Arm has implemented and will maintain appropriate technical and organizational measures intended to protect Device Data and Device Specific Data processed under the Agreement against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction. Arm's security measures are further described in Schedule 1 (Security Measures). Customer agrees that the technical and organizational measures set out in Schedule 1 are appropriate for the processing of Personal Data under the Agreement.

6.2 In the event of a Personal Data Breach, Arm shall notify Customer without undue delay after becoming aware of the Personal Data Breach and shall take reasonable steps to mitigate any damage resulting from such Personal Data Breach. The notification shall contain information that Arm is reasonably able to disclose to Customer, including following information (which may be provided in phases if it is not possible to provide the information at the same time):

a. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of data records concerned;
b. the name and contact details of contact point where more information can be obtained;
c. a description of the likely consequences of the Personal Data Breach; and
d. a description of the measures taken or proposed to be taken to address the Personal Data Breach.

6.3 Where Customer is subject to Data Protection Legislation, Arm shall cooperate with and assist Customer, at Customer's written request and at Customer's cost and expense, in relation to the Personal Data Breach notifications made to a Supervisory Authority or to Data Subjects, as required under the Data Protection Legislation, but only insofar as Customer is not able to provide such assistance based on the Personal Data Breach notification that Arm has provided to Customer.

6.4 If Customer is not the Data Controller of the Personal Data, then Customer is responsible for informing the Data Controller of any Personal Data Breach notification from Arm.

7. SUBPROCESSORS

7.1 Arm is entitled to use subprocessors for the purpose of providing the Service under the Agreement. Arm provides information about its subprocessors on the Pelion Device Management Site. By entering into this DPA, Customer accepts Arm's use of subprocessors as they are listed on the Pelion Device Management Site at the time of agreeing to this DPA. Arm is entitled to reduce the number of subprocessors without separate notice.

7.2 When adding new subprocessors, Arm shall update the Pelion Device Management Site at least 14 days before a new subprocessor processes Personal Data under the Agreement. If Customer objects to the addition of such subprocessor, then Customer shall have the right to terminate the Agreement by written notice before the effective date of the change. If Customer does not object to the addition, then Customer shall be deemed to have authorized Arm to use the new subprocessor.

7.3 Arm shall use its commercially reasonable efforts to ensure that its subprocessors are subject to equivalent requirements regarding confidentiality and data protection, as set out in this DPA. Arm remains responsible for its subprocessors' compliance with the obligations of this DPA in respect of processing of Personal Data included in Device Data and Device Specific Data to the extent that any such subprocessor performs the same data processing activities as those performed by Arm under the Agreement.

7.4 In cases where Customer is not the Data Controller in respect of the Personal Data, then Customer is responsible for informing the Data Controller about Arm's subprocessors, the process for adding subprocessors and newly added subprocessors. Customer warrants and represents that the Data Controller has authorized Customer to agree to the changes to Arm's subprocessors as described in this Clause 7.

8. TRANSFERS OF PERSONAL DATA

8.1 Customer acknowledges that the provision of the Service may require the transfer of Personal Data outside the EEA from time to time, to countries not recognized by the European Commission as providing an adequate level of protection of personal data (as defined in the GDPR). Customer hereby agrees to such transfers provided that: (i) a valid export mechanism for Personal Data is used, such as the standard contractual clauses issued by the European Commission by decision 2010/87/EU, or a current Privacy Shield certification is in place; or (ii) the transfer is otherwise in compliance with Data Protection Legislation.

8.2 Customer hereby agrees to the following transfers of Personal Data: (i) transfers among Arm group companies for the purpose of providing the Service, (ii) transfers to Amazon Web Services based in the United States and Japan for the purposes of hosting Device Data and Device Specific Data; and (iii) and (iii) transfers to subprocessors listed on the Pelion Device Management Site as of the date of this DPA.

8.3 Customer agrees that Arm may transfer Personal Data outside of the EEA if required to do so by EU or EU member state law to which Arm is subject; in such a case, Arm shall inform Customer of such legal requirement before transfer, unless that law prohibits such information on important grounds of public interest.

8.4 In cases where Customer is not the Data Controller in respect of the Personal Data, then Customer is responsible for informing the Data Controller of the transfers set out in this Clause 8. Customer warrants and represents that the Data Controller has authorized Customer to agree to the transfers as described in this Clause 8.

9. AUDITING

9.1 Arm will, in accordance with Data Protection Legislation, make available to Customer such information in Arm's possession or control as Customer may reasonably request by submitting a written request to Arm, with a view to demonstrating Arm's compliance with the obligations of data processors under Data Protection Legislation in relation to its processing of Personal Data.

9.2 Customer may exercise its right of audit under Data Protection Legislation by submitting a written request to Arm for an audit report, in which case Arm shall provide an audit report prepared by a third party which is not older than 18 months, in satisfaction of such request, so that Customer can reasonably verify Arm's compliance with its obligations under Data Protection Legislation in relation to its processing of Personal Data under the Agreement.

9.3 Any information or audit report shared in accordance with this Clause 9 shall at all times be deemed as Arm's Confidential Information.

9.4 If Customer is not the Data Controller with regard to the Personal Data, and the Data Controller would like to audit Arm, then Customer shall deliver such request to Arm without delay.

10. LIMITATION OF LIABILITY

The limitations and exclusions in Clause 11 (Limitations of Liability) of the Pelion Device Management Terms of Service apply to the liability of the Parties under or in connection with this DPA.

11. TERM AND TERMINATION, RETURN OR DELETION OF DATA

11.1 This DPA shall continue in force until the termination of the Agreement.

11.2 Upon termination of the Agreement or upon Customer's written request, Arm shall where possible either delete or return the Personal Data processed hereunder to Customer, or to a third party designated by Customer in writing. If not instructed otherwise in writing by Customer, Arm shall have the right to delete Personal Data processed hereunder within 30 days of termination of the Agreement. If Customer requests that Personal Data be returned to Customer or to a third party, then Customer will pay Arm reasonable costs and expenses arising out of such request.

12. CONFLICT RULES

In the event of any discrepancy between this DPA and the Pelion Device Management Terms of Service, this DPA prevails.

13. AMENDMENTS

From time to time, an amendment to this DPA may be necessary, for example after a decision made by a Supervisory Authority or court or a change in Data Protection Legislation that would have an impact on this DPA. Where, in Arm's opinion, an amendment to this DPA is required for Arm to remain compliant with Data Protection Legislation, then Arm shall have the right, at its sole discretion, to amend this DPA by giving Customer notice of such amendment (each such notification, an "**Amendment Notice**"). Upon receipt of the Amendment Notice, Customer may either:

13.1 accept the amended DPA, in which case no further action is needed, Customer is deemed to have accepted the change, and the DPA is so amended as of the date 30 days after the Amendment Notice; or

13.2 reject the amended DPA and thereby terminate the Agreement, in which case Customer shall give written notice to Arm of such rejection and termination (each such notification, a "**Termination Notice**") within 30 days of the Amendment Notice, and such termination shall take effect no later than 10 days from the date of the Termination Notice.

Schedule 1
Security Measures

1. **General Description of Arm's Security Measures**

Arm's security measures are designed to:

a. ensure the security, integrity and confidentiality of Device Data and Device Specific Data ("**Customer Data**");
b. protect against anticipated threats or hazards to the security or integrity of Customer Data; and
c. protect against unauthorized access to or use of Customer Data that could result in substantial harm or inconvenience to the person that is the subject of Customer Data.

2. **General Procedures**

a. Data Storage. Customer Data is always protected using cryptographic means whenever the interfaces to it cannot be properly enumerated and protected, such as when being transmitted over a network. When the data resides in a secure location, such as on servers that are adequately controlled, it is protected using logical means as are known in the art, such as: database access lists, and file system permissions. When using cryptography, only established and/or NIST-approved algorithms and modes of operation are being used; for example, symmetric encryption is done using AES-128 or AES-256, and transport encryption is carried out using TLS and DTLS. Customer Data that is stored on Internet-facing hosts is protected by a border gateway, which enforces a strict rule-set on incoming traffic. Anomalous activities, such as activities which can be indicative or an emerging attack, are logged and signaled to the Arm Security Operation Center for analysis and remediation.
b. Data Transfers. Arm uses HTTPS standards to protect data integrity during transfers. In addition, subject to Clause 2.a above, Arm will maintain at least the following security measures: HTTP with SSL 128-bit or 256-bit encryption (HTTPS); and secure access to the Service.
c. Access and Use Monitoring. Arm will monitor Arm's user access to and use of the Service for v security, performance evaluation, and system utilization purposes.

3. Security reviews of the operations environment

The operations environment is repeatedly reviewed both in terms of design and in terms of actual execution. The latter is accomplished using penetration tests that are carried out by Arm as well as by external service providers. The outcomes of those reviews can be shared with Customers in certain situations and under certain conditions (such as: exposing just as long as the exposure of the outcome to one customer cannot potentially jeopardize the security posture of another customer).

Arm has experience in supporting external audits by third parties on behalf of customers. In such situations, some of the internal security review material can be shared with the external auditor, to facilitate a more thorough review for lesser costs.

4. Network security

Network security is a wide security domain that is addressed at multiple levels, some of which are:

a. Reliance on accredited and certified cloud providers to assure, inter alia, secure physical resources
b. A strong dedicated border gateway (a.k.a., 'firewall').
c. Patch management and vulnerability management: the former deals with knowing when components that the overall system relies on need to be updated and carrying out such updates; the latter refers to the lifecycle of discovered vulnerabilities from their discovery to their remediation, along with the associated risk management.
d. Secure authentication supporting multiple robustness levels, according to the privilege of the account to which the user authenticates. Authentication security ranges from that of using simple passwords, thorough that of using two-factor authentication with software binding or call-back, all the way to authentication that is secured by two-factors that utilize hardware binding.
e. Proper logging of both successful and failed attempts, along with the alters to the Arm Security Operation Center.
f. Secure administrative remote access to the service network, such as secure authentication.
g. Proper utilization of Hardware Security Modules (HSM) for key long-term assets, and reliable multiple backups of those.

5. **Backup and Business Continuity**

Arm maintains a business continuity program, including a recovery plan, sufficient to ensure Arm can continue to function through an operational interruption and continue to provide Service to Customer.

The program provides a framework and methodology, including a business impact analysis and risk assessment process, necessary to identify and prioritize critical business functions. In the event Arm experiences an event requiring recovery of systems, information or services, the recovery plan will be executed promptly. Arm continuously enhances the Service's security and availability of its multi–tenant enterprise class cloud infrastructure. Arm maintains means of being able to recover copies of Customers Data and tests those regularly.

6. **Key Management**

Encryption keys are used all around the hosted software application used to provide the Service. They are used for secure storage, for token generation, for authentication and AKE algorithms. The hosted software application used to provide the Service does not utilize a single centralized key-store, for both architecture and security reasons. Different keys are stored by different means in accordance with their availability and security requirements.

See below for a few examples for keys in the system and their storage:

a. The highest-grade keys are the keys used in the internal Certification Authority. Those keys are implicitly trusted by all components, are expensive to ever replace, and are thus stored in HSMs.
b. Keys that are used for different authentication purposes within the hosted software application used to provide the Service are stored by a centralized Kubernetes component.
c. Private keys that are used by different hosts to authentication (only) themselves may be stored by the hosts, with proper file-system permissions.