DATA PROTECTION ANNEX

Version dated as of May 25, 2018

This Data Protection Annex ("**DPA**") forms part of Arm's Mbed Cloud Terms of Service and sets out how Arm processes Personal Data included in Account Data, Device Data and Device Specific Data.

1. PARTIES TO THIS DPA

a. The Customer as defined in the Mbed Cloud Terms of Service ("**Customer**"); and

b. Arm Limited ("**Arm**"), with registered office at 110 Fulbourn Road, Cambridge, CB1 9NJ, UK, company registration number 02557590.

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

This DPA supplements the Mbed Cloud Terms of Service which incorporate it.

2. DEFINITIONS

Unless otherwise defined in this DPA, terms used in this DPA, such as "Data Controller", "Data Processor", "Data Subject" and "Supervisory Authority", have the meanings as defined in the Data Protection Legislation (defined below). Additionally, the definitions from the Mbed Cloud Terms of Service apply to this DPA. In addition:

a. "**Data Protection Legislation**" means the EU Data Protection Directive 95/46/EC 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 the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and all applicable national implementing legislation and guidelines (including if the UK leaves the EU), in each case, as amended, revised or replaced from time to time.

b. "**Personal Data**" has the meaning given to such term in the Mbed Cloud Terms of Service.

c. "**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 on behalf of the Customer.

3. ROLES OF THE PARTIES AND CONFLICT RULES

Arm's obligations under Data Protection Legislation depend on Arm's role.

a. **Account Data:** Arm acts as a Data Controller when it processes Personal Data in Account Data for the purposes of managing Customer's Accounts. The processing of Personal Data in Account Data is done in accordance with the Privacy Policy and Section 8 of this DPA.
b. **Personal Data used in support:** Arm acts as a Data Controller when it processes Personal Data for purposes of providing support to Customer. The processing of Personal Data in this case is done in accordance with the Privacy Policy.
c. **Device Data and Device Specific Data:** Arm acts as a Data Processor where it processes Personal Data included in Device Data and Device Specific Data to provide the Services. In that case Customer or a Customer's End User may be a Data Controller or another Data Processor. The processing of Personal Data in this case is done in accordance with this DPA.
d. **Aggregated and Pseudonymized Device Specific Data for internal analytical purposes:** Arm acts as a Data Controller when it processes Device Specific Data for internal analytical purposes, in which case Arm is bound by the conditions of Clause 3.5 of the Mbed Cloud Terms of Service. The Parties agree that Arm may, as a Data Controller, use the data in aggregated or pseudonymized form for its own purposes as set out in in Clause 3.5.

Arm may process Personal Data as long as the Services are provided under the Agreement and after that if required by applicable law or contractual obligations or rights of Arm.

In the event of any discrepancy between this DPA and the Mbed Cloud Terms of Service, this DPA prevails.

4. ARM'S GENERAL OBLIGATIONS

Arm shall ensure that Arm's staff with access to Personal Data under this DPA has committed themselves to appropriate confidentiality obligations.

5. CUSTOMER'S INSTRUCTIONS AND OBLIGATIONS

Where Arm acts as a Data Processor, Arm shall process Personal Data in accordance with Customer's written instructions as established in this DPA.

Customer warrants and represents that Personal Data has been collected under a valid legal basis; that Customer is entitled to share the Personal Data with Arm where Arm provides the Service and where Arm acts as a Data Controller, that Data Subjects have been informed in an appropriate way about the processing of Personal Data, that Data Subjects have, where required, given valid consent under the GDPR and that this consent has not been revoked. Customers shall inform Arm without undue delay if a Data Subject has objected to the processing of Personal Data.

In cases where Arm's 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.

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.

6. PURPOSE OF PROCESSING OF PERSONAL DATA, DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA

Processing of Personal Data under the Mbed Cloud Terms of Service is for the purpose of providing the Services to Customer, including processing activities such as maintenance, audit, forensic and technical support and other equivalent processing activities. Arm processes Personal Data on the written instructions of Customer in accordance with Clause 5 of this DPA, unless prescribed otherwise by Data Protection Legislation applicable to Arm. In that case, Arm shall inform the Customer of that legal requirement, unless forbidden by law.

The categories of Data Subjects processed for the purposes of the Services include Customer's representatives, Customer's End Users and users associated with Customer's End Users' devices.

The following categories of Personal Data are processed under the Mbed Cloud Terms of Service:

a. Account and platform related data, such as account names, address data including telephone numbers, postal address;
b. data associated with the administration of the Account, and APIs, such as the name of the user, logs related to access of the Account, actions from administrators associated with Customer's Account (user name, email address, action details) and specific API keys and backups;
c. record of acceptance of terms, marketing preferences and any other preferences indicated;
d. device related data, such as device IDs, device models and operating systems; and
e. other technical data, such as certificate names and keys related to the Account.

7. OBLIGATION TO ASSIST, RECORDS OF PROCESSING

Arm shall, at Customer's written request and taking into account the information available to Arm, provide reasonable assistance to Customer in responding to requests for exercising the rights of Data Subjects where Customer does not have the required information. Arm shall, taking into account the information available to Arm, provide reasonable assistance to Customer in ensuring compliance with its obligations set out in Data Protection Legislation, relating to data security, Personal Data Breaches as set out in Clause 8 of this DPA, Data Protection Impact Assessments, and prior consulting obligations with the Supervisory Authority. Arm is entitled to charge Customer for costs and expenses that were incurred as a result of such assistance.

Arm shall maintain records of processing activities under its responsibility, to the extent necessary to demonstrate compliance with Arm's obligations set out in this DPA and in the Data Protection Legislation. Customer and any other entity that is legally entitled to inspect such records is obliged to treat all such information as Confidential Information at all times.

8. DATA SECURITY AND DATA BREACHES

Arm has implemented and will maintain and follow appropriate technical and organizational measures intended to protect all data (including Device Data, Device Specific Data, and Account Data) against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction. Arm's security measures are further described in Appendix 1 (Security Measures).

The Customer agrees that those technical and organizational measures are appropriate for the processing of Personal Data.

In the event of a Personal Data Breach, Arm shall notify Customer without undue delay after becoming aware of the Personal Data Breach and take reasonable steps to mitigate any damage resulting from such Personal Data Breach. The notification shall contain information Arm is reasonably able to disclose to Customer, including following information:

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 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.

The information may be provided in phases if it is not possible to provide the information at the same time.

Arm shall cooperate with and assist the Customer, at the Customer's written request and the Customer's cost and expense, in relation to the Personal Data Breach notifications made to Supervisory Authority as required under the Data Protection Legislation.

If the Customer is not the Data Controller with regard to the Personal Data, the Customer is responsible for informing such Data Controller about Arm's notifications regarding Personal Data Breaches. Arm shall cooperate and assist the Data Controller at the Data Controller's written request and the Data Controller's cost and expense, in relation to the Personal Data Breach notifications made to Supervisory Authority, but only insofar as the Customer is not able to provide such assistance based on the Personal Data Breach notification Arm has provided to the Customer.

9. SUBPROCESSORS

Arm is entitled to use subprocessors for the purposes of providing the Services under the Agreement. Arm provides information about its subprocessors on the Mbed Site. By entering into this DPA, Customer accepts Arm's use of subprocessors as they are listed on the Mbed Site at the time of agreeing to this DPA.

Arm is entitled to reduce the number of subprocessors without separate notice.

When adding new subprocessors, Arm shall update its Mbed Site at least 14 days before a new subprocessor processes Personal Data under the Agreement. If Customer objects, 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, this indicates Customer's authorization for Arm to use the new subprocessor.

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 sub-processor performs the same data processing activities performed by Arm under the Agreement.

If Customer is not the Data Controller with regard to the Personal Data, Customer is responsible for informing such Data Controller about Arm's subprocessors, the process of 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 9.

10. TRANSFERS OF PERSONAL DATA

a. Customer hereby agrees to transfers of Personal Data by Arm to countries outside of the European Economic Area ("EEA") provided that: (i) a valid export mechanism for Personal Data, such as the standard contractual clauses issued by the European Commission by the decision 2010/87/EU for international transfers of Personal Data or Privacy Shield, have been executed and, in the case of the Privacy Shield, the certification is current at time of data transfer; or (ii) the transfer is otherwise in compliance with Data Protection Legislation.
b. Customer hereby agrees to the following transfers of Personal Data (i) transfers among Arm group companies for the purpose of providing the Services, and (ii) transfers to Amazon Web Services based in the United States for the purposes of hosting Device Data and Device Specific Data.
c. Customer agrees that Arm may transfer Personal Data outside of the EEA if required to do so by law applicable to Arm. In that case, Arm will inform the Customer of that legal requirement before processing, unless prohibited from doing so by law.

11. AUDITING

At Customer's written request, Arm shall provide Customer with an audit report, which is not older than 12 months so that Customer can reasonably verify Arm's compliance with its obligations under this DPA. If Customer is not the Data Controller with regard to the Personal Data, and such Data Controller would like to audit Arm, Customer shall deliver such request to Arm without delay.

The audit report generated in accordance with this Clause 11 shall at all times be deemed as Arm's Confidential Information.

12. LIMITATION OF LIABILITY

The provisions of Section 11 (Limitations of Liability) of the Mbed Cloud Terms of Service apply to the liability of the Parties under or in connection with this DPA.

13. TERM AND TERMINATION

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

Appendix 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, Device Specific Data and Account 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 the Customer Data that could result in substantial harm or inconvenience to the person that is the subject of the 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 dedicated border gateway security device, 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:
1. HTTP with SSL 128-bit or 256-bit encryption (HTTPS); and
2. secure access to the Services.

c. Access and Use Monitoring. Arm will monitor Arm's user access to and use of the Services for 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:
1. Reliance on accredited and certified cloud providers to assure, inter alia, secure physical resources
2. A strong dedicated border gateway (a.k.a., 'firewall') through which all traffic is routed, and which can deal with encrypted traffic
3. 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.
4. 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.
5. Proper logging of both successful and failed attempts, along with the alters to the Arm Security Operation Center.
6. Secure administrative remote access to the service network, such as by using Jump-boxes along with secure authentication.
7. 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 Services 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 Services' 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 Mbed Cloud. They are used for secure storage, for token generation, for authentication and AKE algorithms. Mbed Cloud 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:

1. 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.
2. Keys that are used for different authentication purposes within Mbed Cloud are stored by a centralized Kubernetes component.
3. Private keys that are used by different hosts to authentication (only) themselves maybe be stored by the hosts, with proper file-system permissions.