Data Processing Agreement

1. Scope and Effective Date

1.1 This Data Processing Agreement, including its Schedules, ("**DPA**") applies to Supplier's Processing of Personal Data as part of Supplier's provision of the Services.

1.2 This DPA supplements the existing purchase agreement between the Parties (the "**Agreement**"). Except as expressly stated otherwise in this DPA, in the event of any conflict or inconsistency between the terms of the Agreement and the terms of this DPA, the relevant terms of the DPA will prevail to the extent of the conflict or inconsistency. In the event of any conflict or inconsistency between the terms of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail to the extent of the conflict or inconsistency.

This DPA shall commence on the Effective Date. The DPA is effective as long as Supplier Processes Personal Data under the Agreement.

2. Definitions

2.1 Capitalised terms have the meaning given to them in the Agreement unless otherwise defined in this DPA.

2.2 The following terms have the meanings set out below for this DPA:

"**Adequate Country**" means a country that has been declared to provide an adequate level of protection under Data Protection Laws;

"**Affiliate**" means any person, partnership, joint venture, corporation or other form of enterprise, domestic or foreign, including but not limited to subsidiaries, that directly or indirectly, control, are controlled by, or are under common control with a party;

"**CCPA**" means the California Consumer Privacy Act as amended by the California Privacy Rights Act, and any related regulations or guidance provided by the California Attorney General which modify the definitions in the DPA for Personal Data, Data Subject, Data Controller, and Data Processor;

"**Data Controller**", "**Data Processor**", "**Data Subject**", "**Processing**" (and "**Process**" and "**Processing**" shall be construed accordingly) and **"appropriate technical and organisational measures**" shall be interpreted in accordance with the GDPR;

"**Data Protection Laws**" means any applicable laws, regulations, or other binding obligations, each as updated from time to time, relating to privacy or data protection of personal data, including those of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, the United States and its states;

"**Effective Date**" means the date when the DPA has been signed;

"**Europe**" means the European Economic Area, Switzerland and the United Kingdom;

"**EU/Swiss Personal Data**" means Personal Data to which (i) Data Protection Laws of the European Union, or of a Member State of the European Union or European Economic Area, or (ii) the FADP, was applicable prior to its Processing by the Supplier;

"**FADP**" means the Swiss Federal Act on Data Protection;

"**GDPR**" means, in each case to the extent applicable to the processing activities: (i) Regulation (EU) 2016/679; and (ii) Regulation (EU) 2016/679 as applicable as part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended) as amended by any legislation;

"**Losses**" means all losses, liabilities, fines, charges, damages, actions, costs and expenses, professional fees (including legal fees actually incurred) and disbursements and costs of investigation, litigation, settlement, judgment, interest and penalties;

"**Personal Data**" means any information Processed by Supplier for the provision of the Services relating to an identified or identifiable Data Subject;

"**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data that Supplier Processes in the course of providing the Services;

"**Sensitive Personal Data**" means sensitive Personal Data as defined under the CCPA, special categories of Personal Data as described in Article 9 of the GDPR, and other similar categories of Personal Data that require a higher level of protection under Data Protection Laws;

"**Services**" means the products and/or services provided by Supplier to Arm pursuant to the Agreement;

"**Standard Contractual Clauses**" means:

(i) in respect of EU/Swiss Personal Data, the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation 2016/679 adopted by Commission implementation decision 2021/914 on 4 June 2021 (the "**EU Standard Contractual Clauses**"), currently found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en;

(ii) in case the FADP was applicable prior to its Processing by the Supplier the term "member state" in the EU Standard Contractual Clauses must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18 of the EU Standard Contractual Clauses; the EU Standard Contractual Clauses shall also protect the data of legal persons until the entry into force of the revised FADP; and

(iii) in respect of UK Personal Data, the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 (the "**UK Addendum**"), as updated or amended from time to time, currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf;

"**Sub-processors**" means Processors providing the Services, acting on behalf of Supplier;

"**Supplementary Measures**" means technical, organisational and contractual measures as described in EDPB Guideline adopted on 18th June 2021 ("Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data");

"**Third Country**" means a country that is neither a part of the European Economic Area nor an Adequate Country; and

"**UK personal data**" means the Personal Data to which Data Protection Laws of the United Kingdom were applicable prior to its Processing by the Supplier.

3. Roles of the Parties

3.1 The Parties agree to the following:

(a) Arm acts as a Data Controller; and

(b) Supplier acts as the Data Processor, in respect of Personal Data Processed by Supplier for the provision of the Services.

3.2 Arm shall be solely responsible for determining the purposes for which and the manner in which Personal Data are, or are to be, Processed.

4. Supplier's obligations

4.1 Where Supplier Processes Personal Data on behalf of Arm, Supplier shall, in respect of such Personal Data:

(a) act only on written instructions and directions from Arm and comply promptly with all such instructions and directions received from Arm from time to time;

(b) immediately notify Arm if, in Supplier's opinion, any instruction or direction from Arm infringes applicable Data Protection Law. Following such notification, Arm shall be entitled to suspend the Processing of Personal Data by Supplier, and to terminate any further Personal Data Processing and the Agreement;

(c) not Process Personal Data for any purpose other than for the provision of the Services and only to the extent reasonably necessary for the performance of the Agreement. Schedule 1 to this DPA sets out the nature, duration and purpose of the Processing, the types of Personal Data Supplier Processes and the categories of Data Subjects whose Personal Data are Processed;

(d) not disclose, publish or divulge Personal Data to any employee, director, agent, contractor or affiliate of Supplier or any third party except as necessary for the performance of the Services, to comply with applicable laws or with Arm's prior written consent;

(e) cooperate with Arm and provide such reasonable assistance as Arm requires to comply with Data Protection Laws, this DPA, including complying with any complaints made by Data Subjects or investigations or enquiries made by any supervisory authority or any other regulator relating to Arm's or Supplier's obligations under applicable Data Protection Laws; and

(f) comply with its obligations under the CCPA to the extent that the Processing of Personal Data under the Agreement is subject to the CCPA. In no event will Supplier sell any such data.

4.2 Supplier shall immediately and in writing inform Arm of:

(a) any request made by Data Subjects under Data Protection Laws;

(b) any request or complaint received from Arm's customers, consumers, employees or from any other individual;

(c) any question, complaint, investigation or other inquiry from a supervisory authority;

(d) any request from a regulator or other public authority of whatever jurisdiction requiring the disclosure of Personal Data Processed by Supplier on behalf of Arm;

and Supplier shall provide a copy of any such request within 2 (two) business days. Supplier agrees that it will only respond to such request as instructed by Arm or as otherwise required by applicable law. Supplier shall assist Arm to fulfil its obligations to respond to requests made by Data Subjects in accordance with Data Protection Laws.

4.3 Upon termination of the Agreement or upon request from Arm to securely delete or return Personal Data, Supplier shall comply with Arm's request to securely delete existing copies of such Personal Data unless Data Protection Laws require storage of the Personal Data, in which case Supplier shall protect the confidentiality of the Personal Data and shall not actively Process the Personal Data.

5. Security, Confidentiality and Breach Notification

5.1 Supplier agrees and warrants that it has implemented and maintains a comprehensive written information security program that complies with Data Protection Laws by applying all necessary and appropriate technical and organisational measures designed to:

(a) protect the security and confidentiality of Personal Data Processed by Supplier in providing the Services; and

(b) protect Personal Data against a Security Breach, having regard to the nature of the Personal Data which is to be protected.

As a minimum, the appropriate technical and organisational measures should include the requirements set out in Schedule 2.

5.2 To the extent that Supplier Processes Sensitive Personal Data, the security measures should include encryption of Sensitive Personal Data during transmission and storage. If encryption is not feasible, Supplier shall not store such data on any unencrypted devices unless compensating controls are implemented.

5.3 Supplier agrees to notify Arm by emailing privacy@arm.com of any technical, operational, organisational or other change having a material impact on the security, confidentiality or protection of Personal Data, no less than 10 (ten) working days prior to implementing any such change. Supplier agrees to submit its information security program to an audit as provided by section 8 of this DPA.

5.4 Supplier shall ensure that any Supplier personnel with access to Personal Data are bound by confidentiality obligations in respect of access, use or Processing of such Personal Data, and take reasonable steps to ensure the reliability and competence of Supplier's personnel who have access to the Personal Data. Without limiting the foregoing, Supplier undertakes to provide training as necessary from time to time to Supplier's personnel with respect to Supplier's obligations in this DPA and to ensure that Supplier's personnel are aware of and comply with such obligations.

5.5 In the event of a suspected Security Breach, Supplier shall, at Supplier's own expense:

(a) immediately take action to investigate any suspected Security Breach, and to identify, prevent and mitigate the effects of the suspected Security Breach and to remedy the Security Breach;

(b) notify Arm by emailing privacy@arm.com within 48 hours of becoming aware of the Security Breach, and without undue delay provide Arm with a detailed description of the Security Breach including:

(i) the likely impact of the Security Breach;

(ii) the categories and approximate number of Data Subjects affected and their country of residence and the categories and approximate number of records affected;

(iii) the risk posed by the Security Breach to individuals;

(iv) the measures taken or proposed to be taken by Supplier to address the Security Breach and to mitigate its adverse effects;

and provide timely updates to this information and any other information Arm may reasonably request relating to the Security Breach; and

(c) not release or publish any filing, communication, notice, press release or report concerning the Security Breach without Arm's prior written approval (except where required to do so by applicable law). Supplier acknowledges and agrees that a violation of this clause, or the occurrence of any Security Breach, may cause immediate and irreparable harm to Arm for which monetary damages may not constitute an adequate remedy.

6. Sub-processing

Arm agrees that Supplier may engage third-party Sub-processors for the purposes of Processing Personal Data under the DPA under the conditions listed in sections 6.2. and 6.3 below.

6.1 Supplier must provide Arm with an initial list of Sub-processors at the Effective Date.

6.2 After the initial notification of current Sub-processors, Supplier can at any time appoint a new Sub-processor provided that:

(a) Supplier includes in any contract with such Sub-processor provisions in favour of Arm which are equivalent to those in this DPA and as are required by applicable Data Protection Laws and

(b) Arm is given 15 (fifteen) business days' prior notice by emailing privacy@arm.com and

(c) Arm does not object to such changes within that timeframe. If Arm objects to the appointment of a new Sub-processor within such period, Supplier shall use reasonable efforts to make available to Arm a change in the Services or recommend a change to Arm's configuration or use of the Services, in each case to avoid the Processing of Arm Personal Data by the objected-to Sub-processor for Arm's consideration and approval. If Supplier is unable to make available such change within a reasonable period of time, which shall not exceed 10 (ten) business days or Arm does not approve any such changes proposed by Supplier, Arm may, by providing written notice to Supplier, terminate the Service or part thereof which cannot be provided by Supplier without the use of the objected-to Sub-processor. In such case, termination will result in no further liability between the Parties, except as otherwise provided in the Agreement.

6.3 For the avoidance of doubt, where a Sub-processor fails to fulfil its obligations under any sub-processing agreement or any applicable Data Protection Laws, Supplier will remain fully liable to Arm for the fulfilment of Supplier's obligations under this DPA.

7. International data transfers

7.1 Supplier shall not Process (i) EU/Swiss Personal Data outside the European Economic Area (EEA)/Switzerland or (ii) UK Personal Data outside the UK unless Supplier:

(a) Processes Personal Data in an Adequate Country or

(b) has obtained the prior explicit written permission from Arm and follows the additional requirements listed in this section.

7.2 To the extent that Supplier has obtained the prior explicit written permission from Arm and Supplier is Processing Personal Data outside of the EEA/Switzerland or UK (as applicable) or an Adequate Country, the Parties shall be deemed to have executed the EU Standard Contractual Clauses (in respect of EU/Swiss Personal Data) and the UK Addendum (as appended to the EU Standard Contractual Clauses, in respect of UK Personal Data) to this DPA. For the purposes of this DPA, when the Parties execute these Standard Contractual Clauses, they acknowledge that:

(a) MODULE TWO (controller to processor) is the relevant module of the EU Standard Contractual Clauses;

(b) Supplier is acting as Arm’s Processor. Arm is the “data exporter” and Supplier is the “data importer” according to Clause 1 of the EU Standard Contractual Clauses;

(c) in clause 7, the Parties choose to include the “docking clause”;

(d) in clause 9, the Parties choose Option 2: “General written authorization”;

(e) in clause 9, the Parties choose 15 working days as the specific time period;

(f) in clause 11, the Parties do not choose the optional complaint mechanism;

(g) in clause 17, the Parties choose the laws of Ireland;

(h) in clause 18, the Parties choose the courts of Ireland for resolving disputes;

(i) Schedule 1 to this DPA shall supplement “Annex I” of the EU Standard Contractual Clauses;

(j) Schedule 2 to this DPA shall supplement “Annex II” of the EU Standard Contractual Clauses; and

(k) The initial list of Sub-processors in section 6.1 in this DPA shall supplement “Annex III” of the EU Standard Contractual Clauses.

(l) To the extent that Arm transfers Personal Data from the United Kingdom to Supplier, the UK Addendum is hereby incorporated by reference. References to the GDPR will be deemed to be references to the UK GDPR and the UK Data Protection Act 2018; references to “supervisory authorities” will be deemed to be references to the UK Information Commissioner and references

to “Member State(s)” or the EU will be deemed to be references to the UK. With respect to information required in the UK Addendum:

(i) In Table 1, Schedule 1 of this DPA shall serve to provide the required information;

(ii) In Table 2, the Parties select the Approved EU Standard Contractual Clauses;

(iii) In Table 3, the information shall be as set forth in Schedule 1 of this DPA; and

(iv) In Table 4, the exporter may end the UK Addendum as set out in section 19 of the UK Addendum.

7.3 To the extent that Supplier is sharing Personal Data with a Sub-processor outside Europe, Supplier shall enter into the appropriate Standard Contractual Clauses with this Sub-processor and make those Standard Contractual Clauses available to Arm. Where necessary, the Parties shall implement additional safeguards to supplement the Standard Contractual Clauses. Such Supplementary Measures shall be documented between the Parties in Schedule 2. The Parties shall commit to implement and update applicable additional safeguards during the term of this Appendix in accordance with guidance provided by Supervisory Authorities under Data Protection Laws. In addition, use of the Standard Contractual Clauses is subject to following conditions:

(a) The Supplier shall, without delay, inform Arm of any inability to comply with Standard Contractual Clauses, including but not limited to local requirements that would require it to provide Personal Data to public authorities in a Third Country;

(b) The Supplier shall inform Arm about the total number of law enforcement requests received during a calendar year. This obligation can be fulfilled by making available a law enforcement access report;

(c) Arm is entitled to suspend the transfer of Personal Data and/or to terminate the relevant agreement with immediate effect in case the Supplier is in breach of this DPA or unable to comply with this DPA;

(d) To the extent required under or necessitated by Data Protection Laws and/or guidance issued by data protection regulatory authorities in relevant jurisdictions, Supplier shall conduct a risk assessment of any such international transfer to determine if the level of protection provided under the laws of the recipient country are adequate to protect Arm in advance of engaging in any such transfer (“**Transfer Assessment**”). Depending on the outcome of any such Transfer Assessment, Supplier shall implement additional measures as necessary to ensure the protection of Arm Personal Data, which may include, without limitation, additional contractual protections and security measures. Upon Arm’s reasonable request, Supplier shall provide Arm with a copy of such Transfer Assessment and/or provide Arm with information to enable Arm to complete its own such assessments; and

(e) In addition to what is stated in the EU Standard Contractual Clauses and the UK Addendum, under certain conditions, Arm may, at its sole discretion, require Supplier to cease Processing Personal Data for the provision of the Services or co-operate with it and facilitate the use of additional technical, organisational and contractual measures. Those conditions are:

(i) an Adequate Country is held no longer to provide an adequate level of protection under Data Protection Laws; or

(ii) a security measure is held to be invalid; or

(iii) a supervisory authority requires transfers to an Adequate Country to be suspended.

7.4 Supplier shall cooperate with Arm in good faith in case the Standard Contractual Clauses or the UK Addendum are modified, revoked, or held in a court of competent jurisdiction to be invalid to:

(a) promptly terminate the transfer of Personal Data or

(b) to pursue a suitable alternative transfer mechanism that can lawfully support the transfer of Personal Data.

8. Audit

8.1 Supplier shall:

(a) make available to Arm all information necessary to demonstrate Supplier's compliance with this DPA; and

(b) provide such co-operation as Arm considers to be necessary to enable Arm to audit and verify Supplier's and Supplier's Sub-processors compliance with this DPA from time to time during the term of the Agreement and for 12 (twelve) months thereafter, which will include providing access to the premises, resources, and personnel of Supplier and Supplier's Sub-processors use in connection with the provision of the Services. Such co-operation may include but shall not be limited to helping Arm to carry out risk assessments of Supplier's data processing operations, in particular providing information about, and permitting Arm to inspect, those operations.

9. Indemnity

9.1 Supplier shall not cause or permit to be done anything within its knowledge or control which may cause (or otherwise result in) Arm to be in breach of Data Protection Laws.

9.2 Supplier shall fully indemnify Arm from and against any and all Losses suffered or incurred by Arm arising from or in connection with breach by Supplier of any of its obligations under this DPA.

Schedule 1

Description of Data Processing Activities

A) List of Parties	**EXPORTER**: *The contact information, signature and date provided above are incorporated herein by reference.* Activities relevant to the data transferred under these Clauses: *Services described in the Agreement.* Role (controller/processor): ***Controller*** **IMPORTER**: *The contact information, signature and date provided above are incorporated herein by reference.* Activities relevant to the data transferred under these Clauses: *Providing Services as described in the Agreement.* Role (controller/processor): ***Processor***
B) Description of transfer	Categories of data subjects whose personal data is transferred *As needed for Supplier to perform the Services, which may include:* • *Employees and applicants* • *Customers and end users* • *Suppliers, agents, consultants, and contractors* Categories of personal data transferred *As needed for Supplier to perform the Services, which may include personal data related directly or indirectly to the categories of data subjects listed above:* • *Direct identifiers such as name, date of birth, and home address* • *Communications data such as home telephone number, mobile telephone number, email address, postal mail, personal vehicle number plate, driver's license number* • *Family and other personal circumstances information such as age, date of birth, marital status, spouse or partner, and number and names of children* • *Education, licenses/certifications held* • *Employment information such as employer, work address, work email and phone, job title and function, salary, manager, employment ID, system usernames and passwords, performance information, and CV data* • *Financial, goods or services purchased, device identifiers, online profiles, and IP address* Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

	Visa information, passport, religion (Ireland only), national identification number, ethnicity data (outside EU) The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis). *Continuously throughout the term of the Agreement.* Nature of the processing *Storing, recording, using, sharing, transmitting, analysing, collecting, transferring and making available personal data.* Purpose(s) of the data transfer and further processing *Provide the Services in accordance with the Agreement.* The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period *Retained for the duration of the Services and deleted in compliance with the Agreement, the DPA, or applicable law.* For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing *Transfers on a continuous basis as needed to perform the Services.*
C) Competent Supervisory Authority	*The Supervisory Authority of Ireland.*
D) Purpose of the Processing in general	*To provide the Services in accordance with the Agreement.*
E) Duration of the Processing	*Continuously throughout the term of the Agreement.*

Schedule 2

Security Measures

This Schedule 2 sets out the description of types of technical and organisational security measures to be implemented and maintained by the Data Importer in accordance with sections 4 and 5 of this DPA, and shall include the following:

1. Access control to premises and facilities

1.1 Unauthorized access (in the physical sense) must be prevented.

1.2 Technical and organizational measures to control access to premises and facilities, particularly to check authorization, such as: access control system ID reader, magnetic card, chip card; (issue of) keys; door locking (electric door openers etc.); security staff and janitors; surveillance facilities alarm system, and video/CCTV monitor.

2. Access control to systems

2.1 Unauthorized access to IT systems must be prevented.

2.2 Technical (ID/password security) and organizational (user master data) measures for user identification and authentication, such as: password procedures (including special characters, minimum length, change of password, two-factor authentication); automatic blocking (e.g., password or timeout); creation of one master record per user; and encryption of data media.

3. Access control to data

3.1 Activities in IT systems not covered by the allocated access rights must be prevented.

3.2 Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses, such as: differentiated access rights (profiles, roles, transactions, and objects); reports; use of professional and secure storage solutions; and logging of access and (attempted) misuse.

4. Disclosure control

4.1 Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

4.2 Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking, such as: encryption/tunnelling (VPN); electronic signature; logging; and transport security.

5. Input control

5.1 Full documentation of data management and maintenance must be maintained.

5.2 Measures for subsequent checking whether data have been entered, changed, or removed (deleted), and by whom, such as logging and reporting systems.

6. Job control

6.1 Commissioned data processing must be carried out according to directions.

6.2 Measures (technical/organizational) to segregate the responsibilities between the principal and the agent, such as: unambiguous wording of the contract; formal commissioning (request form); criteria for selecting the agent; and monitoring of contract performance.

7. Availability control

7.1 The data must be protected against accidental destruction or loss.

7.2 Measures to assure data security (physical/logical), such as: backup procedures; mirroring of hard disks, e.g., RAID technology; uninterruptible power supply (UPS); remote storage; anti-virus/firewall systems; and disaster recovery plan.

8. Segregation control

8.1 Data collected for different purposes must also be processed separately.

8.2 Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes, such as: “internal client” concept/limitation of use, and segregation of functions (production/test).