15 December 2021

**KIGEN DATA PROCESSING ADDENDUM**

This Kigen Data Processing Addendum together with its Exhibits and Appendices ("**DPA**") sets out the Parties' agreement in relation to the Processing of Personal Data by Kigen for Customer in connection with the provision of Kigen M2M (Hosted) RSP Server services and/or data generation services (collectively, the "**Services**") pursuant to the Terms of Sale or any other written or electronic agreement between Kigen and Customer (the "**Service Agreement**").

Customer enters into this DPA and this DPA becomes binding upon execution of the Service Agreement, either upon signature of the Service Agreement by both Parties, or by Customer clicking "I accept" or by otherwise signifying its acceptance of the Service Agreement.

This DPA does not apply to any Processing of Personal Data which Kigen carries out as a Controller.

1.  **PARTIES TO THIS DPA**

1.1  This DPA is made between:

    the Customer as identified in the Service Agreement ("**Customer**"); and

    the Kigen entity that is party to the Service Agreement ("**Kigen**").

1.2  Customer and Kigen are hereunder jointly referred to as the "Parties", and each separately as a "Party".

2.  **DEFINITIONS**

2.1  For the purposes of this DPA, the following capitalised words are ascribed the following meanings:

    "**Agreement**" means the Service Agreement together with this DPA.

    "**Kigen Group**" means Kigen (UK) Limited, a company incorporated in England (UK), and its Subsidiaries from time to time.

    "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

    "**Customer Data**" means any data and information that are defined in the Service Agreement as "Device Data" or "Device Specific Data" and which are submitted by or for Customer to the Service.

    "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

    "**Data Subject Request**" has the meaning ascribed to it under Clause 5.2.

    "**Data Protection Legislation**" means all laws and regulations relating to the protection of personal data and privacy of individuals (all as amended, superseded or replaced from time to time), including without limitation the California Consumer Privacy Act, the GDPR, the European Directive 2002/58/EC (as amended by Directive 2009/136/EC), including any legislative and/or regulatory amendments or successors thereto, and any applicable implementing local legislation within the EEA, any other laws and regulations of the European Union, their member states and of the United Kingdom.

    "**Documented Instructions**" has the meaning ascribed to it under Clause 4.2.

    "**DPA**" has the meaning ascribed to it above.

    "**EEA**" means the European Economic Area.

**"European Data Protection Legislation"** means, as applicable, the GDPR, the UK GDPR and the Federal Data Protection Act of 19 June 1992 (Switzerland), each as amended, superseded or replaced from time to time.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), as amended, superseded or replaced from time to time.

"**Kigen Site**" means https://www.kigen.com, including without limitation all sub-domains thereof, and any successor or related site designated by Kigen.

"**Personal Data**" means any information relating to an identified or identifiable natural person included in Customer Data.

"**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 Kigen under the Agreement.

"**Processing**" means any operation or set of operations which is performed upon Personal 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, erasure or destruction.

"**Service**" means any and all services provided by Kigen under the Service Agreement.

**"Service Agreement"** has the meaning ascribed to it above.

"**Processor**" means the entity which Processes Personal Data on behalf of a Controller.

"**Relevant Transfer**" has the meaning ascribed to it under Clause 8.3.

"**Standard Contractual Clauses**" means the clauses included in Commission Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Sub-processor**" means a third party that Kigen or another Kigen Group entity engages for the Processing of Personal Data on behalf of Customer.

**"Subsidiary"** means any company the majority of whose voting shares is now or hereafter owned or controlled, directly or indirectly, by a party hereto. A company shall be a Subsidiary only for the period during which such control exists.

"**Supervisory Authority**" means an independent public authority charged with overseeing the compliance with Data Protection Legislation.

**"UK"** means the United Kingdom.

**"UK GDPR"** means the GDPR as incorporated into UK law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, as amended, superseded or replaced from time to time.

2.2 All capitalized terms not defined in this DPA shall have the meaning ascribed to them in the Service Agreement.

**3.     ROLES OF THE PARTIES**

3.1 Customer shall, in its use of the Service, Process Personal Data at all times in accordance with the requirements of the applicable Data Protection Legislation and any other laws and regulations applicable to Customer and in accordance with the Agreement.

3.2 As between Customer and Kigen, Customer has sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Personal Data were acquired.

3.3 If Customer is not the Controller of the Personal Data, or is a Controller jointly with others, Customer represents and warrants to Kigen that any third party who is a Controller of the Personal Data agrees to the Processing by Kigen of the Personal Data pursuant to the Agreement and the Documented Instructions provided to Kigen pursuant to the Agreement.

3.4 Customer acts as a single point of contact and is responsible for obtaining any relevant authorizations, consents and permissions for the Processing of Personal Data in accordance with the Agreement. Where authorizations, consent, instructions or permissions are provided by Customer, these are provided not only on behalf of Customer but also on behalf of all relevant Controllers of the Personal Data. Where Kigen informs or gives notice to Customer, it is Customer's responsibility to forward such information and notices to any relevant Controller(s) (as applicable) without undue delay.

## 4. CUSTOMER'S INSTRUCTIONS AND CONFIDENTIALITY

4.1 The subject matter of Processing of Personal Data by Kigen in the performance of the Service pursuant to the Service Agreement, the duration, the nature and purpose of such Processing, the types of Personal Data Processed under the Service Agreement and relevant categories of Data Subjects are specified in Exhibit 2 to this DPA.

4.2 The Parties agree that this DPA and the Service Agreement and the instructions provided via configuration or other tools made available by Kigen under the Service Agreement (such as APIs or SDKs) constitute Customer's documented instructions regarding Kigen's Processing of Personal Data under the Agreement ("**Documented Instructions**"). The Documented Instructions shall comply with applicable Data Protection Legislation and any other laws and regulations applicable to Customer.

4.3 If, in Kigen's opinion, any Documented Instruction infringes European Data Protection Legislation or other provisions of data protection laws of the European Union or of one of its member states, Kigen will immediately inform Customer. For the avoidance of doubt, this Clause 4.3 does not imply any obligation binding on Kigen to conduct any legal review of any Documented Instruction and any communication or information provided by Kigen to Customer pursuant to this Clause 4.3 is not and shall not be deemed to be at any time as constituting legal advice.

4.4 Kigen shall process Personal Data in accordance with the Documented Instructions, unless otherwise required by law to which Kigen is subject. In such a case, Kigen shall inform Customer of such legal requirement before Processing, unless the law prohibits such information.

4.5 In cases where Customer is a Processor, not a Controller, in respect of the Personal Data, Customer shall ensure that the Documented Instructions provide the same or similar level of data protection as those required by the instructions of the relevant Controller(s).

4.6 Any instruction related to the Processing of Personal Data additional to the Documented Instructions require prior written agreement between the Parties, including agreement on any additional fees payable by Customer to Kigen for carrying out such instruction. Once agreed, any such additional instruction is deemed as a Documented Instruction under this DPA.

4.7 Where Standard Contractual Clauses apply between the Parties, the Documented Instructions are deemed to be the instructions by the Customer for the purpose of Clause 5(a) of the Standard Contractual Clauses.

4.8 Kigen shall not disclose Personal Data to any third party except as permitted under the Agreement or as necessary to comply with the law or a valid and binding order of a governmental body. If Kigen is required to disclose Personal Data to a governmental body, then Kigen will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Kigen is legally

prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Clause 4.8 varies or modifies the Standard Contractual Clauses.

4.9     Kigen shall ensure that persons it authorises to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

## 5.     OBLIGATIONS TO ASSIST

5.1     Kigen shall, taking into account the information available to Kigen and the nature of the Processing, provide reasonable assistance to Customer as required under applicable European Data Protection Legislation in ensuring compliance with Customer's obligations relating to data protection impact assessments and prior consulting obligations with the competent Supervisory Authority. Kigen may charge Customer for reasonable costs and expenses incurred as a result of such assistance.

5.2     Kigen provides assistance to Customer in relation to data security and personal data breaches according to Clause 6. Kigen may charge Customer for reasonable costs and expenses incurred as a result of any further assistance that Kigen may be required to provide in that respect under applicable Data Protection Legislation.

5.3     Kigen shall, to the extent legally permitted, promptly notify Customer if Kigen receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, object to Processing, or its right not to be subject to an automated individual decision making (each such request being a "**Data Subject Request**"). Taking into account the nature of the Processing, Kigen shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Legislation. To the extent Customer, in its use of the Service pursuant to the Service Agreement, does not have the ability to address a Data Subject Request, Kigen shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Kigen is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Legislation. To the extent legally permitted, Customer shall be responsible for any costs arising from Kigen's provision of such assistance.

## 6.     DATA SECURITY AND DATA BREACHES

6.1     Kigen has implemented and will maintain appropriate technical and organizational measures intended to protect Personal Data processed under the Agreement against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction ("**Security Measures**"). Kigen's Security Measures applicable to the Service provided under the Service Agreement are further described at Exhibit 2, Appendix 1 to this DPA.

6.2     Customer agrees that the Security Measures are appropriate for the Processing of Personal Data under the Agreement. Customer agrees that Kigen may modify at any time at its discretion the Security Measures, provided that Kigen does not decrease the overall security of the Service during the term of the Agreement and continues to comply with Clause 6.1 above. From time to time the most up to date description of the Security Measures will be made available on the Kigen Site or communicated to Customer in writing.

6.3     Kigen may offer for sale or otherwise make available optional security features and functionalities additional to the Security Measures. Customer is responsible for properly configuring the Service and determining whether to use any such optional feature or functionality if appropriate in consideration of the Personal Data being Processed with the Service and the Processing activities carried out under the Service Agreement.

6.4     In the event of a Personal Data Breach, Kigen shall notify Customer without undue delay after becoming aware of the Personal Data Breach. The notification shall contain information that Kigen is reasonably able to disclose to Customer, including the 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.

6.5    Kigen shall provide reasonable cooperation and assistance to Customer, at Customer's written request and at Customer's cost and expense, in relation to Personal Data Breach notifications to be made to a Supervisory Authority or to Data Subjects but only insofar as Customer is not able to provide such notification on the basis of the Personal Data Breach notification that Kigen has provided to Customer.

6.6    Kigen's obligation to report or respond to a Personal Data Breach under this Clause 6 is not and shall not be construed as an acknowledgement by Kigen of any fault or liability of Kigen with respect to the Personal Data Breach.

## 7    SUB-PROCESSORS

7.1    Kigen is entitled to use Sub-Processors for the purpose of providing the Service under the Agreement. Kigen provides information about its Sub-Processors on the Kigen Site or otherwise in writing to Customer. By entering into the Service Agreement, Customer accepts Kigen's use of Sub-Processors as they are listed on the Kigen Site at the time of agreeing to the Agreement, or as listed in the Service Agreement or otherwise communicated in writing to Customer at the time of entering into the Service Agreement. Kigen is entitled to reduce the number of Sub-Processors without separate notice.

7.2    When adding a new Sub-Processor: (i) Kigen shall update the list published on its website referred to under Clause 7.1 above at least 30 days before the new Sub-Processor Processes Personal Data under the Agreement. Such update is deemed to be a notice given to Customer about the proposed engagement of the new proposed Sub-Processor for the purpose of Clause 7.3 below; or (ii) where the list of Sub-processors was communicated to Customer pursuant to Clause 7.1 other than by its publication on Kigen's website, Kigen shall notify Customer in writing pursuant to the provisions on legal notices under the Service Agreement about the proposed engagement of the any new Sub-Processor at least 30 days before the new Sub-Processor Processes Personal Data under the Agreement.

7.3    Customer may object to Kigen's use of a new Sub-processor for Good Cause by notifying Kigen promptly in writing at privacy@Kigen.com within 14 days following notice of the new proposed Sub-Processor by Kigen. In the event Customer objects to a new Sub-Processor pursuant to this Clause 7.3, Kigen may make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening Customer. If Kigen is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the Agreement within the following thirty (30) days with respect only to that part of the Service which cannot be provided by Kigen without the use of the objected-to new Sub-Processor by providing written notice to Kigen. For the purpose of this Clause 7.3, "**Good Cause**" means a justified doubt as to whether the new proposed Sub-Processor can comply with the relevant contractual requirements described in this DPA.

7.4    If Customer does not object to the addition of a new Sub-Processor pursuant to Clause 7.3 or if, following any such objection, Customer does not terminate the Agreement pursuant to Clause 7.3, then Customer shall be deemed to have authorized Kigen to use the new Sub-Processor.

7.5    Kigen shall ensure that its Sub-Processors are subject to equivalent requirements regarding confidentiality and data protection as set out in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-Processors. Kigen remains responsible towards Customer for Kigen's Sub-Processors' acts and omissions pursuant to the Agreement.

7.6    Where Standard Contractual Clauses apply between the Parties, Customer acknowledges and expressly agrees that pursuant to Clause 5(h) of the Standard Contractual Clauses information about Kigen's Sub-Processors is given as described in this Clause 7 and that Kigen may engage new Sub-Processors as described in this Clause 7.

## 8    INTERNATIONAL TRANSFERS OF PERSONAL DATA SUBJECT TO EUROPEAN DATA PROTECTION LEGISLATION

8.1     Customer acknowledges that the provision of the Service may require international transfers of Personal Data, including without limitation transfers to countries not recognized by the European Commission, Switzerland or the UK as providing an adequate level of protection of personal data. Customer hereby agrees to any such transfers provided that Kigen complies with this Clause 8.

8.2     Subject to Clause 8.7 below, in respect of any transfer of Personal Data by Kigen under this DPA from the EEA, Switzerland  or the UK to countries which do not ensure an adequate level of data protection (within the meaning of the applicable European Data Protection Legislation) and to the extent such transfers are subject to European Data Protection Legislation, Kigen will use at its discretion a permitted transfer mechanism under European Data Protection Legislation, including without limitation, binding corporate rules (if available) or Standard Contractual Clauses.

8.3     As between Customer and Kigen, the Standard Contractual Clauses set out in Exhibit 1 apply only in respect of those international transfers of Personal Data Processed under the Agreement that are subject to European Data Protection Legislation, as long as such law recognizes the Standard Contractual Clauses as a lawful transfer mechanism of Personal Data and only to the extent to which Kigen does not elect to use another permitted transfer mechanism under applicable European Data Protection Legislation ("**Relevant Transfer**").

8.4     At Kigen's discretion where this option is available, Kigen may enter into Standard Contractual Clauses in the Customer's name and on the Customer's behalf with one or more Sub-Processor(s) in respect of Relevant Transfers. Customer hereby authorizes Kigen to sign and execute Standard Contractual Clauses with Sub-Processors in the Customer's name and on Customer's behalf. Where Kigen enters into Standard Contractual Clauses pursuant to this Clause 8.4, Kigen shall promptly inform Customer. The Parties agree that it is Customer's responsibility to ensure that Customer has the authority to grant Kigen the power of attorney necessary pursuant to this Clause 8.4 and Customer shall provide to Kigen written confirmation of it upon request.

8.5     Notwithstanding Clause 8.2 above, Customer agrees that Kigen may transfer Personal Data if required to do so by law to which Kigen is subject; in such a case, Kigen shall inform Customer of such legal requirement before transfer, unless that law prohibits such information.

8.6     In cases where Customer is not the Controller in respect of the Personal Data, then Customer is responsible for ensuring that its agreement with the Controller(s) allows for the use of all of the transfer mechanisms mentioned in this Clause 8. Customer warrants and represents that any relevant Controller has authorized Customer to agree to the transfers as described in this Clause 8.

8.7     Customer agrees to cooperate with Kigen in good faith, upon Kigen's request, to promptly have a new transfer mechanism in place in case any mechanism listed in Clause 8.2 is no longer applicable due to being modified or revoked by a competent court, the European Commission or other competent authority.

## 9.     AUDITS

9.1     Upon Customer's written request at reasonable intervals, Kigen will make available to Customer such information in Kigen's possession and control as Customer may reasonably request, with a view at demonstrating Kigen's compliance with the obligations of a Processor under the GDPR or the UK GDPR (as applicable) in relation to Kigen's processing of Personal Data under this DPA.

9.2     Customer agrees to exercise any right it might have under applicable Data Protection Legislation to conduct an audit or an inspection (including without limitation any right to audit Sub-Processors) by submitting a written request to Kigen for an audit report, in which case Kigen shall provide an audit report prepared by a respected third party which is not older than 12 months, in satisfaction of such request, so that Customer can reasonably verify Kigen's compliance with its obligations in relation to its Processing of Personal Data under this DPA.

9.3     Where the Standard Contractual Clauses apply between the Parties, the Parties agree that audits pursuant to Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses may be carried out as follows:

(a) in accordance with Clauses 9.1 and 9.2 above of this DPA; and/or

(b) Customer may contact Kigen to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Kigen for any time expended for any such on-site audit at Kigen's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Kigen shall mutually agree upon the scope, timing, and duration of the audit in addition to the reasonable reimbursement rate for which Customer shall be responsible. Customer shall promptly notify Kigen with information regarding any non-compliance discovered during the course of an audit.

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

## 10. LIMITATION OF LIABILITY

Each Party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations and exclusions of liability set out in the Service Agreement, and any reference thereunder to the liability of a Party means the aggregate liability of that Party under the Agreement.

## 11. TERM OF THE DPA AND CONSEQUENCES OF TERMINATION

11.1 This DPA shall continue in force until expiration or termination of the Service Agreement. Clauses 2, 3, 4.8, 10, 11 and 12 shall survive termination of this DPA.

11.2 Kigen shall, at Customer's choice, return or delete (or otherwise render permanently inaccessible) all Personal Data in its possession within 30 days (and within 120 days in respect of Personal Data stored in its back-ups) from termination or expiration of the Service Agreement ("**Post-Termination Period**"), unless otherwise required by law. Where Customer elects to have Personal Data returned to it pursuant to this Clause 11.2, Kigen may fulfill its obligation under this Clause 11.2 by granting Customer, at Customer's cost, access to Personal Data stored in the Service during a 30-day period following termination or expiration of the Service Agreement (or any other period as it may be agreed by the Parties in writing) ("**Extended Post-termination Period**") so as to allow Customer to extract a copy of the Personal Data. Where Personal Data are not deleted by Customer, Kigen shall delete (or otherwise render permanently inaccessible) Personal Data in its possession within the end of the Post-Termination Period or within 30 days (and within 120 days in respect of Personal Data stored in its back-ups) from the expiration of the Extended Termination Period, unless otherwise required by law.

11.3 Where the Standard Contractual Clauses apply, the Parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Kigen to Customer only upon Customer's written request.

## 12. CONFLICT RULES

12.1 In the event of any conflict between this DPA and the Service Agreement, this DPA prevails.

12.2 Where the Standard Contractual Clauses at Exhibit 1 apply, in the event of any conflict between Exhibit 1 and any other provision of this DPA, Schedule 1 prevails.

## 13. AMENDMENTS TO THIS DPA

13.1 Kigen is permitted to modify this DPA from time to time by posting a revised version on the Kigen Site or by otherwise notifying Customer according to the provisions on legal notices under the Service Agreement (each such notification, an "**Amendment Notice**"). Changes are effective 30 days following posting or as otherwise specified in the Amendment Notice ("**Amendment Effective Date**") unless Customer objects to such amendments before the Amendment Effective Date pursuant to Clause 13.2 below. Where Customer does not object in accordance with Clause 13.2 below, Customer is deemed to have agreed on

the notified amendments and this DPA is amended accordingly with effect from the Amendment Effective Date.

13.2    Save as provided under Clause 6.2, Customer may object to changes to this DPA notified by Kigen pursuant to Clause 13.1 by written notice to Kigen sent to privacy@Kigen.com ("**Objection Notice**"). The Objection Notice must detail the reasons for Customer's objection. The Parties will negotiate in good faith the proposed amendment to this DPA during the period of 30 days following receipt by Kigen of the Objection Notice ("**Negotiation Period**"). The Parties may agree in writing to extend the Negotiation Period. Where the Parties do not agree on changes to this DPA before expiration of the Negotiation Period, either Party may terminate the Agreement by serving the other Party 10-day prior written notice within 30 days from the end of the Negotiation Period. Where the Agreement is not terminated pursuant to this Clause 13.2, Customer is deemed to have agreed on the amendments originally notified via the Amendment Notice and this DPA is amended accordingly with effect from 30 days after the end of the Negotiation Period.

13.3    Save as provided under Clause 13, any change to this DPA shall be in writing and signed by the authorized representatives of the Parties.

# EXHIBIT 1

# STANDARD CONTRACTUAL CLAUSES (PROCESSOR TO CONTROLLER)
## (Transfers from the EEA to third countries)

# SECTION I

### *Clause 1*

### Purpose and scope

(a)  The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b)  The Parties:
   (i)    the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
   (ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')
   have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c)  These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)  The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

### *Clause 2*

### Effect and invariability of the Clauses

(a)  These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)  These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### *Clause 3*

### Third-party beneficiaries

(a)  Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i)    Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii)   Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.l(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.l(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
(iii)  Clause 9-Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
(iv)  Clause 12-Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
(v)   Clause 13;
(vi)  Clause 5.l(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18-Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

### *Clause 4*

### Interpretation

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

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

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

### *Clause 5*

### Hierarchy

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

*Clause 6*

**Description of the transfer(s)**

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

*Clause 7*

**Docking clause**

(a)   An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b)   Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)   The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

# SECTION II - OBLIGATIONS OF THE PARTIES

*Clause 8*

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a)   The data exporter shall process the personal data only on documented instructions  from the data importer acting as its controller.

(b)   The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c)   The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d)   After the end of the provision of the processing services, the data exporter shall, at the choice of the

data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

### 8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (this includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

### *Clause 9*

### **Use of sub-processors**

[Not applicable for processor to controller transfers – see Kigen Data Processing Addendum]

### *Clause 10*

### **Data subject rights**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

*Clause 11*

**Redress**

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

*Clause 12*

**Liability**

(a)    Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)    Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c)    Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d)    The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e)    The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

*Clause 13*

**Supervision**

[Not applicable for Processor to Controller transfers]

## SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*Clause 14*

**Local laws and practices affecting compliance with the Clauses**

[Not applicable for Processor to Controller transfers as Kigen (the EU processor) does not combine personal data received from third country-controller with personal data collected by Kigen in the EU)]

## Clause 15

### Obligations of the data importer in case of access by public authorities

[Not applicable for Processor to Controller transfers as Kigen (the EU processor) does not combine personal data received from third country-controller with personal data collected by Kigen in the EU)]

# SECTION IV - FINAL PROVISIONS

## Clause 16

### Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated.

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   (ii) the data importer is in substantial or persistent breach of these Clauses; or
   (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

## *Clause 17*

### Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

## *Clause 18*

### Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Ireland.

# ANNEX I TO EXHIBIT 1

### A.  LIST OF PARTIES

**Data exporter:**

**Name:** Kigen (UK) Limited (or any other Kigen entity identified in the DPA)

**Address:** Merlin Place, Milton Road, Cambridge, CB4 0DP (or the address of any other Kigen entity identified in the Service Agreement)

**Contact person's name, position and contact details**:  John Page, Legal Counsel, Kigen (UK) Limited, legal@kigen.com

**Activities relevant to the data transferred under these Clauses**: Processing and export of Personal Data in the performance of Services under the Service Agreement

**Signature and date**: Signatory of the Service Agreement

**Role**: Processor

**Data importer:**

**Name**: Customer, as identified in the DPA

**Address**: Customer address, as identified in the Service Agreement

**Contact person's name, position and contact details**:  See Notices clause of Services Agreement.

**Activities relevant to the data transferred under these Clauses**: Importing Personal Data from Kigen's performance of Services under the Service Agreement.

**Signature and date**: Signatory of the Service Agreement

**Role**: Controller

### B.  DESCRIPTION OF TRANSFER

| | |
|---|---|
| Subject matter and duration of the Processing: | Provision of the Services to Customer; Kigen Processes Personal Data for as long as is necessary for the provision of the Services. |
| Nature and Purpose of Processing: | Kigen Processes Personal Data as necessary to perform the Services pursuant to the Agreement, and as it may be further specified in any technical documentation made available to Customer or further instructed by Customer pursuant to the Agreement in its use of the Services. Processing includes but is not limited to storage, transfer and analysis of Personal Data. |

| Frequency of Transfer: | Personal Data will be transferred from Kigen to sub-processors and Customer as requested by Customer during the term over which Kigen provides the Services. |
|---|---|
| Types of Personal Data: | Personal Data relating to individuals provided to Kigen via the Services, by (or at the direction of) Customer or by Customer End Users (defined in the Service Agreement), specifically ICCID, EID and MSISDN.<br><br>Special categories of Personal or Sensitive Data:  none |
| Categories of Data Subjects | Categories of Data Subjects include the individuals about whom data is provided to Kigen via the Service by (or at the direction of) Customer or by Customer End Users (defined in the Service Agreement). |

**C.  COMPETENT SUPERVISORY AUTHORITY**

[Not applicable for Processor to Controller transfers]

# ANNEX II TO EXHIBIT 1

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

Data importer will maintain at least the administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Service referred to under clause 6 of the DPA between data exporter and data importer.

Details of Kigen's security measures are provided at Appendix 1 to Exhibit 2 of this DPA.

# ANNEX III TO EXHIBIT 1

**LIST OF SUB-PROCESSORS**

The Kigen Group entity listed below engages personnel to provide service and data generation support in connection with the Kigen Hosted RSP Server Service. This support includes engineering activities related to managing the availability of the Service; data generation services, product management; and customer support.

| Entity Name | Entity Location |
|---|---|
| Kigen (India) Private Limited | India |

15 December 2021

# EXHIBIT 2

**DETAILS OF THE SERVICE AND OF THE PROCESSING ACTIVITIES**

Details of the Processing by Kigen in connection with the provision of Service consisting of **data generation and RSP server services:**

| | |
|---|---|
| Subject matter and duration of the Processing: | Provision of the Services to Customer; Kigen Processes Personal Data for as long as is necessary for the provision of the Services. |
| Nature and Purpose of Processing: | Kigen Processes Personal Data as necessary to perform the Services pursuant to the Agreement, and as it may be further specified in any technical documentation made available to Customer or further instructed by Customer pursuant to the Agreement in its use of the Services. Processing includes but is not limited to storage, transfer and analysis of Personal Data. |
| Types of Personal Data: | Personal Data relating to individuals provided to Kigen via the Services, by (or at the direction of) Customer or by Customer End Users (defined in the Service Agreement)<br><br>Special categories of Personal Data: n/a |
| Categories of Data Subjects | Categories of Data Subjects include the individuals about whom data is provided to Kigen via the Service by (or at the direction of) Customer or by Customer End Users (defined in the Service Agreement). |

Security Measures applicable to the Services are set out at Appendix 1 to this Exhibit 2.

# APPENDIX 1 TO EXHIBIT 2

## SECURITY MEASURES

1. **General Description of Kigen's Security Measures**
   Kigen's security measures are designed to:
   a. ensure the security, integrity and confidentiality of Device Data and Device Specific Data;
   b. protect against anticipated threats or hazards to the security or integrity of Device Data and Device Specific Data; and
   c. protect against unauthorized access to or use of Device Data and Device Specific Data that could result in substantial harm or inconvenience to the person that is the subject of any Personal Data therein.

2. **General Procedures**
   a. Data Storage. Device Data and Device Specific 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. Device Data and Device Specific Data that is stored on Internet-facing hosts is protected by network layer access control lists, which enforce a strict rule-set on incoming traffic. Anomalous activities, such as activities which can be indicative of an emerging attack, are logged and signaled for analysis and remediation.
   b. Data Transfers. Kigen uses cryptography standards to protect data integrity during transfers. In addition, subject to Clause 2.a above, Kigen 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. Kigen will monitor Kigen's user access to and use of the Service 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 Kigen as well as by external service providers. A summary of those reviews can be shared with Customer 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).

   Kigen 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 GSMA-accredited data center to ensure strong, secure, physical resources are fully controlled by Kigen.
   b. Reliance on accredited and certified cloud providers to assure, inter alia, secure physical resources
   c. A strong dedicated border gateway (a.k.a 'firewall') through which all traffic is routed, and which can deal with encrypted traffic.
   d. 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.
   e. 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 wat to authentication that is secured by two-factors that utilize hardware binding.

f.  Proper logging and signaling of both successful and failed attempts.

g.  Secure administrative remote access to the service network, such as secure authentication.

h.  Proper utilization of Hardware Security Modules (HSMs) 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.

6. **Key Management**

Encryption keys are used all around the hosted software application that are used to provide the Service. They are used for secure storage, secure transport, for token generation, and for authentication. 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.