Origen Technologies Data Processing Addendum

Origen Technologies Data Processing Addendum

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Origen Technologies General Terms and applicable Orders, or such other written or electronic agreement between Origen Technologies and Customer for the purchase of Origen Technologies Offerings ("**Agreement**"), and is made as of the Effective Date

BETWEEN

(1) _____, a company incorporated in_____with a principal place of business at_____, together with any Affiliates authorized to use the Origen Technologies Offerings under the Agreement (and provided an Affiliate is not subject to a separate Agreement with Origen Technologies), collectively referred to as "**Customer**;" and

(2) **Origen Technologies Inc.**, whose principal place of business is in 1704 1/2 South Congress Ave Austin, TX 78704 ("**Origen Technologies**"),

(Each a "**Party**" and together, the "**Parties**"). Defined terms not otherwise set forth in the Agreement but used in this DPA (Data Processing Addendum) are as set forth in the Definitions section below.

INSTRUCTIONS

This DPA has been pre-signed on behalf of Origen Technologies. To execute this DPA,

Customer must:

(a) complete the information in the section above.

(b) verify that the information is accurate, complete and is the same as the information about Customer provided in the Agreement; and

(c) submit the validly completed, signed, and unmodified DPA to Origen Technologies by email at: operations@Origentech.com

This DPA will become effective as of the date the Offerings start as listed in the applicable Order ("**Effective Date**"). This DPA will be deemed legally binding upon receipt by Origen Technologies of a fully executed copy pursuant to the instructions above and supersedes any prior agreements between Customer and Origen Technologies concerning the Processing of Personal Data.

HOW THIS DPA APPLIES

Order of Precedence. In the event of any conflict between the following documents, and only to the extent of such conflict, the order of precedence will be as follows:

(a) between the Agreement and the DPA, the DPA will prevail.

Origen Technologies DPAs (Data Processing Addendum) are not available for and do not apply to trials, evaluations, beta, and free Licenses to Offerings. A DPA executed in connection with any such licenses will be deemed null and void.

PART I–DATA PROTECTION UNDER EUROPEAN LAW

Subject to the terms of the Agreement, the below terms and conditions apply to the Processing of Personal Data.

1. Processing of Personal Data

1.1 **Roles and Responsibilities**. Customer is the Controller and Origen Technologies is the Processor. Customer grants a general authorization to: (a) Origen Technologies to appoint any other Origen Technologies Affiliate as a sub-processor; and (b) Origen Technologies and any Origen Technologies Affiliate to appoint third-party sub-processors to support the performance of the Offerings as provided below.

1.2 **Origen Technologies Processing Activities**. Origen Technologies agrees that it (and its sub-processors) will: (a) Process Personal Data only on the documented instructions from the Customer as set forth in the Agreement and this DPA; (b) ensure that only authorized personnel who are under written obligations of confidentiality have access to such Personal Data; and (c) take appropriate technical and organizational measures to secure the Personal Data as set forth in Section 7 (Technical and Organizational Measures). Origen Technologies further agrees that it will comply with the Data Protection Law applicable to Origen Technologies in the provision of Offerings under the Agreement and this DPA.

1.3 **Customer Processing Activities.** Customer agrees that if it uses the Offerings to submit Personal Data to Origen Technologies, it will: (a) do so in accordance with the requirements of Data Protection Law, including, if applicable, providing notice to Data Subjects of the use of Origen Technologies as a Processor; and (b) provide documented instructions for the Processing of Personal Data that comply with Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and how Customer or any relevant third-party acquired Personal Data. Unless specifically identified in an Order, Customer agrees to not transmit or store within the Offerings any restricted Personal Data as set forth in the Agreement.

1.4 **Details of Processing Activities.** The nature and extent of Processing Personal Data by Origen Technologies to deliver the Offerings is determined and controlled solely by Customer

2. Data Subject Requests

If Origen Technologies receives a Data Subject Request from Customer's Data Subject, it will promptly notify Customer. Origen Technologies will refrain from responding to the Data Subject except to acknowledge receipt of the Request, to which Customer hereby agrees. Customer can address Data Subject Requests within the Offering in accordance with the applicable Documentation. Upon request, Origen Technologies will provide reasonable assistance to help Customer facilitate a Data Subject Request. Origen Technologies reserves the right to charge for such assistance. Requests for assistance from Origen Technologies hereunder should be made to operations@origentech.com

3. Assistance

Origen Technologies will provide assistance to Customer as Customer reasonably requests

(taking into account the nature of Processing and the information available to Origen Technologies) in relation to Customer's obligations under Data Protection Law with respect to: (a) data protection impact assessments (as such term is defined in Data Protection Law); (b) Customer's compliance with its obligations under Data Protection Law with respect to the security of Processing; and (c) any prior consultations required with a Supervisory Authority.

4. Deletion or Return of Personal Data

Upon termination of the Hosted Service, Customer may at its sole option and expense, delete or retrieve Customer Content, including any Personal Data contained therein, from the Hosted Services as provided in the Agreement. For On-Premises Products, Origen Technologies does not Process or store Customer Content, except to the extent it may be included in diagnostic files submitted in connection with Origen Technologies' Support Program, which are deleted in accordance with Origen Technologies' Policy. In the event Origen Technologies is required under applicable law to retain Personal Data Processed under this DPA after termination of the Agreement, Origen Technologies will protect the Personal Data

5. Inspections and Audit

5.1 Origen Technologies will contribute to audits requested by Customer, not more than once annually (except in the event of a Data Breach or request from a Supervisory Authority) to demonstrate Origen Technologies' compliance with its obligations under this DPA

5.2 If Customer is required under Data Protection Law to request any further information to confirm Origen Technologies' compliance with its obligations under this DPA, such additional information (including any on-site inspections) will be provided and/or conducted at Origen Technologies' then-current Configuration and Implementation Services rates, considering the number of resources and time required. Customer and Origen Technologies will mutually agree upon the scope, timing, and duration of any on-site inspection, including with respect to any third-party inspector selected by the Customer. Customer will promptly notify Origen Technologies of any non-conformance discovered during an on-site audit.

5.3 Requests for assistance from Origen Technologies as provided herein should be made to operations@Origentech.com or such other location as Origen Technologies may make available on its website from time to time.

6. Technical and Organizational Measures

Origen Technologies provides the technical and organizational measures required under applicable Data Protection Law for the security of the Personal Data it Processes

7. International Data Transfers

Data Transfers under the EU Clauses. The standard contractual clauses pursuant to European Commission Decision 2021/914/EU ("EU Clauses") including the modules for controller-processor transfers attached hereto, are incorporated into this DPA, and apply where the application of the EU Clauses, as between the Parties, is required under applicable Data Protection Law for the transfer of Personal Data. Customer acknowledges that Origen Technologies will Process Personal Data outside the EEA including in the United States in compliance with this DPA, the EU Clauses, the Agreement, and applicable Data Protection Law. For the purposes of the EU Clauses: (a) Customer is the "data exporter"; and (b) Origen Technologies is the "data importer."

Where the EU Clauses are required under Swiss data protection law applicable to the

transfer of Personal Data, the following additional provisions will apply:

(a) the terms below will have the following substituted meanings for the purposes of the EU Clauses:

i. "GDPR" means the Federal Act on Data Protection of 19 June 1992 (SR 235.1; "FADP") and its revised version of 25 September 2020 ("Revised FADP"), which is scheduled to come into force on 1 January 2023.

ii. "European Union," "Union" or "Member States" means Switzerland, provided that the term "member state" 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 (Switzerland)

iii. "Supervisory authority" means the Federal Data Protection and Information Commissioner ("FDPIC"); and

(b) the EU Clauses will protect the Personal Data of Customer until the entry into force of the Revised FADP.

7.1 **Data Transfers under the U.K. Clauses.** The standard contractual clauses (processors) pursuant to European Commission Decision 2010/87/EU ("UK Clauses"), are incorporated into this DPA and apply where the application of the UK Clauses, as between the Parties, is required under applicable Data Protection Law in the United Kingdom ("U.K.") for the transfer of Personal Data. In the UK Clauses, all references to the Data Protection Directive shall be deemed to refer to the Regulation (EU) 2016/679 (as implemented into U.K. law by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, as amended) and the U.K. Data Protection Act 2018; all references to "European Union", "Union" or "Member States" shall be deemed to refer to the United Kingdom; and all references to "Supervisory Authority" shall be to the U.K. Information Commissioner. Customer acknowledges that Origen Technologies will Process Personal Data outside the U.K. including in the United States in compliance with this DPA, the UK Clauses, the Agreement, and applicable Data Protection Law.

For the purposes of the UK Clauses: (a) Customer is the "data exporter"; (b) Origen Technologies is the "data importer";

7.2 Origen Technologies will promptly notify Customer if it determines that it can no longer meet its obligations under the EU Clauses or the UK Clauses.

7.3 Origen Technologies reserves the right to adopt an alternative compliance standard to the EU Clauses or the UK Clauses for the lawful transfer of Personal Data, provided it is recognized under Data Protection Law. Origen Technologies will provide 30 days' advance notice of its adoption of an alternative compliance standard and such alternative compliance standard will automatically apply as set out in Origen Technologies' notification at the end of the notice period.

8. Personal Data Breach

8.1 **Personal Data Breach Notification.** Origen Technologies will notify Customer without undue delay after becoming aware of a Personal Data Breach. Where appropriate in respect of any Personal Data which has been the subject of a Personal Data Breach, Origen

Technologies will provide reasonable assistance to Customer to the extent required for Customer to comply with Data Protection Law, which may include assistance in notifying Data Subjects and the relevant Supervisory Authority, providing a description of the Personal Data Breach, including where possible: (a) the nature of the Personal Data Breach and the categories and approximate number of Data Subjects and/or Personal Data records concerned; (b) the name and contact details of Origen Technologies' data protection officer or other contact point; (c) a description of the likely consequences of the Personal Data Breach; and (d) to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects and provide to Customer a description thereof. Where, and in so far as, it is not possible to provide the above information at the same time, further information will be provided without undue further delay as it becomes available.

8.2 **Customer Notification to Origen Technologies.** If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority, Data Subject, or the public under Data Protection Law, to the extent such notice refers to Origen Technologies, whether or not by name, Customer agrees to consult with Origen Technologies in good faith and in advance and consider any clarifications or corrections Origen Technologies may request to the notification consistent with Data Protection Law.

9. General

9.1 Origen Technologies will inform Customer, immediately upon becoming aware, if in Origen Technologies' opinion any instructions provided by Customer under this DPA infringe Data Protection Law.

9.2 Origen Technologies' aggregate liability to Customer arising out of or related to the DPA will be subject to the same limitations and exclusion of liability as apply under the Agreement, whether liability arises under the Agreement or this DPA.

9.3 The Parties agree that Origen Technologies will be a Controller of: (a) Customer business contact information that is Personal Data required to administer the Offerings; and (b) any Personal Data contained within Usage Data as described in the Agreement, and terms of this DPA will not apply.

9.4 This DPA will be governed by and construed in accordance with the governing law provisions set forth in the Agreement.

Part II—California Data Protection

1. Roles and Responsibilities

1.1 Origen Technologies is a "service provider" for the purposes of the services it provides to Customer pursuant to the Agreement, according to the meaning given to that term of the California Civil Code, as of the date of execution of this DPA.

1.2 Origen Technologies agrees that, to the extent that Customer discloses a Consumer's Personal Information to Origen Technologies, Origen Technologies will Process that Personal Information only on behalf of Customer and pursuant to the Agreement and this DPA.

2. Origen Technologies Processing of Personal Information of Consumers

2.1 Origen Technologies certifies that it shall not Process, retain, use, or disclose a Consumer's Personal Information for any purpose other than for the specific purpose of performing the Offerings specified in the Agreement.

Origen Technologies agrees that it shall not Sell a Consumer's Personal Information.

Definitions

"**Data Protection Law**" means all applicable laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, applicable to the Processing of Personal Data including the General Data Protection Regulation on the protection of natural persons regarding the processing of personal data and on the free movement of such data("**GDPR**")

"**Data Subject**" as defined under Data Protection Law.

"**Data Subject Request**" means a request from or on behalf of a Data Subject relating to access to, or rectification, erasure, or data portability in respect of that person's Personal Data or an objection from or on behalf of a Data Subject to the processing of its Personal Data.

"**Personal Data**" means all data which is defined as 'personal data' under Data Protection Law, and which is provided by a Customer to Origen Technologies (directly or indirectly), and accessed, stored, or otherwise processed by Origen Technologies as a Processor as part of its provision of the Offerings to a Customer and to which Data Protection Law applies from time to time.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data while being transmitted, stored, or otherwise processed by Origen Technologies.

The Parties' authorized signatories have duly executed this DPA:

CUSTOMER		**ORIGEN TECHNOLOGIES INC.**
By:	_____	By: _____
Name:	_____	Name: _____
Title:	_____	Title: _____

EXHIBIT 1

STANDARD CONTRACTUAL CLAUSES

(Controller to Processor Module) 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 regarding the processing of personal data and on the free movement of such data (General Data Protection Regulation) 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 Clauses in a wider contract and/or to add other clauses or additional safeguards, if 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 8.1(b) and Clause 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e)

(iv) Clause 12(a), (d) and (f)

(v) Clause 13

(vi) Clause 15.1(c), (d) and (e)

(vii) Clause 16(e)

(viii) Clause 18(a) and (b).

(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 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 (Intentionally left blank)

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 organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law.

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the

additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management, and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall act appropriately to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, to notify the competent supervisory authority and the affected data subjects, considering the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 and offences, the data importer shall apply the specific restrictions and/or additional safeguards.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer.

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question.

(iii) the onward transfer is necessary for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory, or judicial proceedings; or

(iv) the onward transfer is necessary to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may consider relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information, including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer has the data exporter 's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third- party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub- processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall

set out the appropriate technical and organizational measures, considering the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization, or association under the conditions of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member Statelaw.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that

part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject because 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.

(f) The Parties agree that if one Party is held liable, 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.

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

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred

personal data; the economic sector in which the transfer occurs; the storage location of the data transferred.

(ii) the laws and practices of the third country of destination -including those requiring the disclosure of data to public authorities or authorizing access by such authorities -relevant considering the specific circumstances of the transfer, and the applicable limitations and safeguards.

(iii) any relevant contractual, technical, or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of thethird

country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical, or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, as far as it concerns the processing of personal data under these Clauses. If 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. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response

provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

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. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, as far 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 that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. 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 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 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member

(b) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member in which he/she has his/her habitual residence.

(c) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: _____

Address: _____

Contact person's name, position, and contact details: _____

Activities relevant to the data transferred under these Clauses: data exporter determines the subject-matter of the processing and data importer processes data as required to deliver the Offerings

Signature and date: _____

Role (controller/processor): Controller

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Origen Technologies Inc.

Address: 1704 1/2 South Congress Ave Austin, TX 78704

Contact person's name, position, and contact details: Origen Technologies Data Protection Officer, operations@Origentech.com

Activities relevant to the data transferred under these Clauses: Processing operations as required to deliver the Offerings to the data exporter.

Signature and date: _____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Origen Technologies Offerings, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners, vendors and their respective employees or contractors (who are natural persons)
- Data exporters' assigned users of the Origen Technologies Offerings
- Data exporters' employees, agents, contractors, or advisors (who are natural persons)

Categories of personal data transferred

Data exporter may submit Personal Data to the Origen Technologies Offerings, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Business contact information (e.g., company email, phone, physical business address)
- Personal contact information (e.g., email, mobile phone, address)
- ID data
- Connection data
- Location data

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data importer and data exporter do not envisage that special categories of data will be processed under these clauses.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

Data exporter determines the subject-matter, nature and duration of the processing and data importer's sub-processors process personal data as required to deliver the Origen Technologies Offerings.

Purpose(s) of the data transfer and further processing

Data exporter is requesting, and data importer will provide, the Origen Technologies Offerings to the data exporter pursuant to 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

Data exporter determines the retention periods applicable to Customer Content (including any Personal Data therein).

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

Please refer to sub-processors as set forth in Annex III. Data exporter determines the subject-matter, nature and duration of the processing and data importer's sub-processors process personal data as required to deliver the Origen Technologies Offerings.

A. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, considering the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer provides the technical and organizational measures required under applicable Data Protection Law, as defined in the DPA, for the security of the Personal Data it processes as set forth in the Agreement. The specific technical and organizational measures are listed in the applicable Security Addenda identified below and may contain, as applicable, measures designed for:

- Pseudonymization and encryption of personal data.
- Ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- User identification and authorization.
- Protection of data during transmission.
- Protection of data during storage.
- Physical security of locations at which personal data are processed.
- Event logging.
- System configuration, including default configuration.
- Internal IT and IT security governance and management.
- Certification / assurance of processes and products.
- Allowing data portability and ensuring erasure.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller, and, for transfers from a processor to a sub- processor, to the data exporter

Data importer requires that any sub-processor it engages to provide the Origen Technologies Offerings on its behalf in connection with the DPA does so only based on a written contract which imposes on such sub-processor terms no less protective of Personal Data than those imposed on data importer in the DPA, including the transfer of Personal Data to a third country or international organization in accordance with Data Protection Law.