VELSERA DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**") and all its Annexes apply to the Processing of Personal Data by Velsera Inc. and its subsidiaries, including but not limited to Seven Bridges Genomics Inc., PierianDx, Inc. and UgenTec NV, each a Velsera company, **(** collectively "Velsera" or "Processor"**)** acting on its own behalf and as agent for each Velsera Affiliate, when processing data on behalf of Customer ("**Customer Personal Data**" acting on its own behalf and as agent for each Customer Affiliate, related to Velsera's SaaS Services and other Professional Services (collectively, the "Services") as described in the Master Services Agreement and any applicable Ordering Document (the "**Principal Agreement**"). This DPA forms part of and supplements the "Principal Agreement" between Customer and Velsera. In case of any contradictions between this DPA and the Agreement or any other documents regarding the same subject matter, such provision in this DPA shall prevail to the extent the corresponding provisions are irreconcilable. In the event of any conflict between the terms of the SCCs and this DPA (including any exhibits), the Agreement, or any other document, the SCCs shall prevail to the extent that applicable Data Protection Laws so require.

Definitions: Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement and the GDPR. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1. "**Alternative Transfer Solution**" means a solution, other than the Standard Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Data Privacy program Framework (EU-U.S. DPF), the UK Extension to the EU-US DPF, and the Swiss-U.S. Data Privacy program Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce.

1.1.2. "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Controller Personal Data in respect of which any Controller is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Controller Personal Data in respect of which any Controller is subject to any other Data Protection Laws, provided, however, to the extent this refers to regulations in countries outside of the European Union, the United Kingdom, or the United States of America, such regulations will only constitute "Applicable Laws" to the extent the Controller has informed Processor about such requirements in relation to this DPA and to the extent such requirements are mandatory and/or of public order and apply to the contractual relationship between the Parties;

1.1.3. " **Affiliate**" has the meaning set forth in the Principal Agreement;

1.1.4. "Customer Data" has the meaning set forth in the Principal Agreement

1.1.5. "**Controller Personal Data**" means any Customer Data that is Personal Data, including, but not limited to genomic data, Processed by a Contracted Processor on behalf of a Customer pursuant to or in connection with the Principal Agreement;

1.1.6. "**Contracted Processor**" means Velsera, or a Velsera Subprocessor;

1.1.7. "**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under this DPA including, where applicable, EU Data Protection Laws, UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country if such is notified in advance to the Processor and included in this DPA;

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

1.1.9. "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.10. "**GDPR**" means EU General Data Protection Regulation 2016/679 (EU GDPR); and/or the UK General Data Protection Regulation Act 2018 (UK GDPR 2018 and the Privacy and Electronic Communications Regulations 2019 (together known as the "UK GDPR")

1.1.11. "**Restricted Transfer**" means:

1.1.11.1. a transfer of Controller Personal Data from any Controller to a Contracted Processor; or

1.1.11.2. an onward transfer of Controller Personal Data from a Contracted Processor to a

Contracted Processor, or between two establishments

1.1.11.3. of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 13 below;

1.1.12. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Velsera for Controllers pursuant to the Principal Agreement;

1.1.13. "**Standard Contractual Clauses**" means the contractual clauses set out in Attachment 1 and Attachment 2, as applicable, amended as indicated (in square brackets and italics) in that Appendix and under section 13.4;

1.1.14. "**Subprocessor**" means any person (including any third party and any Velsera Affiliate, but excluding an employee of Velsera or any of its sub-contractors) appointed by or on behalf of Velsera or any Velsera Affiliate to Process Personal Data on behalf of any Controller in connection with the Principal Agreement; and

1.1.15. "**Velsera Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Velsera, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.1.16. "**UK Data Protection Laws**" means the GDPR as it forms part of the United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR") and the Data Protection Act of 2018.;

1.2. The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3. The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. **Roles of the Parties.** Although the Parties acknowledge that their respective status is determined by the Applicable Laws, the Parties are of the view that in the context of the Principal Agreement and this DPA the Customer is a Data Controller and Velsera is a Data Processor in respect of the Processing of Controller Personal Data during the course of the provision of the services under the Principal Agreement. The Parties acknowledge that the Controller alone determines all the purposes and essential means of the Processing of said Personal Data in its role as Controller and Velsera shall Process Personal Data on behalf of the Customer in its role as Processor. Notwithstanding the foregoing, Velsera is also a Data Controller in respect of certain processing activities, of which an overview is provided in Annex I to this DPA.

3. **Authority.** Velsera warrants and represents that, before any Velsera Affiliate Processes any Controller Personal Data on behalf of any Controller, Velsera's entry into this DPA as agent for and on behalf of that Velsera Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Velsera Affiliate.

4. **Processing of Controller Personal Data**

4.1. Velsera and each Velsera Affiliate shall:

4.1.1. comply with all applicable Data Protection Laws in the Processing of Controller Personal Data; and

4.1.2. not Process Controller Personal Data other than on the relevant Controller's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Velsera or the relevant Velsera Affiliate shall to the extent permitted by Applicable Laws inform the relevant Controller of that legal requirement before the relevant Processing of that Personal Data.

4.2. Each Controller instructs Velsera and each Velsera Affiliate (and authorizes Velsera and each Velsera Affiliate to instruct each Subprocessor) to:

4.2.1. Process Controller Personal Data; and in particular, transfer Controller Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

4.2.2. warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 4.2.1 on behalf of each relevant Customer Affiliate.

4.3. Annex I to Attachment 1 of this DPA sets out certain information regarding the Contracted Processors' Processing of the Controller Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Controller may make reasonable amendments to Annex I of Attachment 1 by written notice to Velsera from time to time as Controller reasonably considers necessary to meet those requirements. Nothing in Annex I to Attachment 1 (including as amended pursuant to this section 4.3) confers any right or imposes any obligation on any party to this DPA.

4.4. The Parties acknowledge that some Velsera companies, specifically PierianDx, Inc. and UgenTec NV, may use anonymized and aggregate data, such as data generated by Velsera for the purposes below. Strictly related to these purposes, Velsera may also provide the anonymized and aggregate data to third parties, it being noted that Velsera is solely responsible to ensure full compliance thereof with Applicable Laws. As these anonymized and aggregate data cannot in any manner be linked to a corresponding data subject, these data do not constitute Personal Data in the context of the Agreement. The other provisions of this DPA do not apply to these anonymized and aggregate data. After the data has been fully anonymized and aggregated by Velsera, the other provisions of this DPA do not apply to this anonymized and aggregated data. In this respect, Velsera is sole controller. Anonymized and Aggregated Data may be used:

4.4.1. to provide summaries and insights on the use of the Velsera platforms and the assays for the Velsera platforms to the Controller (to the extent these Services are included in the Principal Agreement),

4.4.2. to perform statistic (non-clinical) analyses and to create demographic overviews of test results in order to detect or predict epidemics, spread of illnesses, etc.,

4.4.3. to create fully anonymized demo data, and

4.4.4. to improve or increase the services offered by Velsera.

5. **Velsera and Velsera Affiliate Personnel.** Velsera and each Velsera Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Controller Personal Data, including ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Controller Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, and ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. **Security of the Processing.**

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Velsera and each Velsera Affiliate shall in relation to the Controller Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Annex III of this DPA.

6.2. Velsera and each Velsera Affiliate shall ensure that any person authorized by Velsera to Process Controller Personal Data (including its employees, contingent workers, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)

6.3. In assessing the appropriate level of security, Velsera and each Velsera Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach. Velsera and each Velsera Affiliate shall have no obligation to assess the contents or accuracy of Controller Personal Data, including identifying information subject to any specific legal, regulatory, or other requirement. The Controller is responsible for reviewing the information made available by Velsera relating to data security and making an independent determination as to whether the Services meet the Controller's requirements and legal obligations under applicable Data Protection Laws.

6.4. Velsera and each Velsera Affiliate shall, in relation to the Processing of Controller's Personal Data, implement the Technical and Organizational Security Measures set out in Annex III of this DPA.

Velsera and each Velsera Affiliate shall regularly review its Technical and Organizational Security Measures to be updated as necessary, to ensure a level of security appropriate to the risk, as outlined in Article 32(1) of the GDPR, provided that these updates shall not materially diminish the overall security of the Services or Controller Personal Data.

6.5. Velsera shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for reviewing the information made available by Velsera relating to data security and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations under the applicable Data Protection Laws.

7. **Subprocessing**

7.1. Controller provides Velsera and each Velsera Affiliate a general authorization to the current Subprocessors (and permit each Subprocessor appointed in accordance with this section 7 to appoint their Subprocessors) identified in Annex III of the SCCs as of the effective date of this DPA. For the avoidance of doubt, the above authorization constitutes Customer's prior written consent to the subprocessing by Velsera for purposes of Clause 9 of the Standard Contractual Clauses and in accordance with this section 7.

7.2. Velsera Shall amend Annex II of the SCCs with any addition of Subprocessors, and notify Customer of such changes

7.3. If, within 30 days of receipt of that notice, Customer notifies Velsera in writing of its objections to the proposed appointment on the basis that such addition would cause the Customer to violate applicable legal requirements, neither Velsera nor any Velsera Affiliate shall appoint (or disclose any Controller Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by Controller and Controller has been provided with a reasonable written explanation of the steps taken. If the Customer does not object within such period, the respective Subprocessor may be commissioned to Process Customer Personal Data.

7.4. With respect to each Subprocessor, Velsera or the relevant Velsera Affiliate shall:

7.4.1. ensure that the arrangement between Velsera or the relevant Velsera Affiliate, and the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Controller Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR;

7.4.2. if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between Velsera, or the relevant Velsera Affiliate, and the Subprocessor); and

7.4.3. upon request, provide to Customer for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Customer may request from time to time.

7.5. Velsera and each Velsera Affiliate shall ensure that each Subprocessor performs the obligations under this DPA, as they apply to Processing of Controller Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of Velsera.

8. **Data Subject Rights.** Taking into account the nature of the Processing, Velsera and each Velsera Affiliate shall assist each Controller by implementing appropriate Technical and Organizational Security Measures, insofar as this is possible, for the fulfilment of the Controllers' obligations, as reasonably understood by Processor, to respond to requests to exercise Data Subject rights under the Data Protection Laws. Velsera shall:

8.1. promptly notify Controller if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Controller Personal Data (commonly known as DSARs); and

8.2. ensure that the Contracted Processor does not respond to that request except on the documented instructions of Controller or the relevant Controller Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Velsera shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor

responds to the request.

8.3. Where the Data Subject seeks to exercise any of its rights under the applicable Data Protection Laws (collectively, "Data Subject Access Request" or "DSAR"), Customer will be responsible for responding to any such DSAR. To the extent Customer is unable to access the relevant Customer Personal Data within the Velsera offerings, Velsera shall (upon Customer's written request and taking into account the nature of the Processing) provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

8.4. Controller shall submit any written request for assistance related to Data Subject Requests (DSARs) in accordance with Article 15 of the GDPR. Controller shall not be responsible for costs arising from Velsera's provision of regular assistance, which are considered as the costs involved with enabling the Controller to comply with its legal obligations towards Data Subjects or Authorities (such as correcting, deleting or amending Personal Data of Data Subjects or assistance in relation to Data Breaches). If the costs are the result of the Controller's instructions with a broader scope, such costs will be borne by the Controller.

9. **Personal Data Breach**

9.1. Velsera shall notify Customer without undue delay upon Velsera becoming aware of a Personal Data Breach affecting Controller Personal Data, providing Customer with sufficient information to allow each Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

9.2. Notification shall be sent to the email registered by the Customer within the Service, and where no such email is registered, the Customer acknowledges that the means of notification shall be at Velsera's reasonable discretion.

9.3. Velsera shall co-operate with Controller and take such reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

10. **Data Protection Impact Assessment and Prior Consultation.** Velsera and each Velsera Affiliate shall provide reasonable assistance to each Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Controller by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to Velsera.

11. **Deletion or Return of Controller Personal Data**

11.1. Subject to sections 11.2 and 11.3, Velsera and each Velsera Affiliate shall promptly and in any event within 90 days of the date of cessation of any Services involving the Processing of Controller Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Controller Personal Data, unless otherwise agreed to by the Parties in the Principal Agreement. "**Delete**" means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed.

11.2. Subject to section 11.3, Controller may in its absolute discretion by written notice to Velsera within 30 days of the Cessation Date require Velsera and each Velsera Affiliate to (a) return a complete copy of all Controller Personal Data to Controller by secure file transfer in such format in Controller Personal Data is maintained or stored by Processor; and (b) delete and procure the deletion of all other copies of Controller Personal Data Processed by any Contracted Processor. Velsera and each Velsera Affiliate shall comply with any such written request within 30 days of the date such written request is received. Any additional data transfer requests by Controller shall be subject to the terms and conditions included in the Principal Agreement including applicable cost responsibilities.

11.3. Each Contracted Processor may retain Controller Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Velsera and each Velsera Affiliate shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

12. **Audit rights**

12.1. As part of the review and evaluation of the security measures, most Velsera companies will, once every year, have a security audit performed by an independent third-party expert, according to generally accepted audit standards which will be documented in a written security report. The Controller may request a copy of this security report in lieu of undertaking an independent security audit as it relates to the security measures observed under this DPA in Annex III (TOMs).

12.2. Subject to sections 12.1, 12.3 and 12.4, Velsera and each Velsera Affiliate shall make available to each Controller on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to reasonable audits, including inspections, by any Controller or an auditor mandated by any Controller in relation to the Processing of the Controller Personal Data by the Contracted Processors.

12.3. Information and audit rights of the Controllers only arise under section 12.2 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

12.4. Customer or the relevant Customer Affiliate undertaking an audit shall give Velsera or the relevant Velsera Affiliate reasonable notice of no less than thirty (30) days, of any audit or inspection to be conducted under this section and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

12.4.1. to any individual unless he or she produces reasonable evidence of identity and authority;

12.4.2. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Controlleror the relevant Customer Affiilate undertaking an audit has given notice to Velsera or the relevant Velsera Affiliate that this is the case before attendance outside those hours begins; or

12.4.3. for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

12.4.3.1. Customer or the relevant Customer Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Velsera's or the relevant Velsera Affiliate's compliance with this DPA; or

12.4.3.2. A Controller is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Controller or the relevant Controller Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Velsera or the relevant Velsera Affiliate of the audit or inspection.

13. **Cross-border and Restricted Transfers**

13.1. Subject to sections 13.3, each Controller (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses (SCCs) in respect of any Restricted Transfer from that Controller to that Contracted Processor. For clarity, for transfers from the United Kingdom and Switzerland, references in the SCCs shall be interpreted to include applicable terminology for those jurisdictions (e.g., “Member State” shall be interpreted to mean “United Kingdom” for transfers from the United Kingdom.) The Standard Contractual Clauses (SCCs) are attached to this DPA as Schedule 1, to implement appropriate safeguards for such transfers of Customer Personal Data. In the event that any data transfers under the Agreement are subject to the UK GDPR, the UK Addendum, set out in Schedule 2, shall apply.

13.2. The Standard Contractual Clauses shall come into effect as of the Effective Date of this DPA to the extent the data being transferred relates to individuals or Data Subjects from a Restricted Country that does not have an Alternative Transfer Solution available and adopted in accordance with Article 46 of the GDPR.

13.3. Section 13.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably

practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

14. **General Terms**

Governing law and jurisdiction

14.1. Without prejudice to Clause 17 (Governing Law) and Clause 18 (Choice of Forum and Jurisdiction) of the Standard Contractual Clauses:

14.1.1. the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

14.1.2. this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

14.2. Nothing in this DPA reduces Velsera's or any Velsera Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Velsera or any Velsera Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14.3. Subject to section 14.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail to the extent of any conflict in connection with the Processing of Controller Personal Data.

Changes in Data Protection Laws, etc.

14.4. Customer may:

14.4.1. by at least 60 (sixty) calendar days' written notice to Velsera from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 13.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

14.4.2. propose any other variations to this DPA which Controller reasonably considers to be necessary to address the requirements of any Data Protection Law.

14.5. If Customer gives notice under section 14.4.1:

14.5.1. Velsera and each Velsera Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 7.4.3; and

14.5.2. Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Velsera to protect the Contracted Processors against additional risks associated with the variations made under section 14.4.1 and/or 14.5.1.

14.6. If Customer gives notice under section 14.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

14.7. Neither Customer nor Velsera shall require the consent or approval of any Customer Affiliate or Velsera Affiliate to amend this DPA pursuant to this section 14.5 or otherwise.

Severance

14.8. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part

had never been contained therein.

Term and Termination

14.9. This DPA shall enter into effect as of the date of the Principal Agreement (the "Effective Date"). This DPA will continue in force until the termination of the Agreement (the **Termination Date**").

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

MODULE TWO:

Transfer controller to processor

If, and to the extent, Applicable Data Protection Law requires the parties to enter into the SCCs in connection with the Processing of Personal Data, each party is deemed to have executed the SCCs by entering into this DPA. The below shall apply to the SCCs, including the election of specific terms and/or optional clauses as described in more detail in
(i) through (x) below, and any optional clauses not expressly selected are not included:

(a) The Module 2 terms apply to the extent Customer is a Data Controller;

(b) The optional Clause 7 (Docking Clause) in Section I of the SCCs is incorporated, and Authorized Affiliates may accede to this DPA and the SCCs under the same terms and conditions as Customer via mutual agreement of the Parties;

(c) For purpose of Clause 9 of the SCCs, **Option 2 ("General written authorization")** is selected and the process and time period for the addition or replacement of Sub-processors shall be as described in Section 7 (sub- processing) of this DPA and identified in Annex III of the SCCs;

(d) For purposes of Clause 13 and Annex I of the SCCs, the following shall apply [CUSTOMER TO SELECT APPLICABLE PROVISION]:

[Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(e) For purpose of Clause 17 and Clause 18 of the SCCs, the Member State for purpose of governing law and jurisdiction shall be the Republic of Ireland.

DATA EXPORTER

Name:……

Authorised Signature _____

DATA IMPORTER

Name:**Velsera Inc.**

Authorised Signature _____

ANNEX I

A. LIST OF PARTIES

Data exporter(s)/Controller:

Customer/Customer:

As stated in the Principal Agreement

Data importer(s)/Processor
Velsera Inc.
529 Main Street, Suite 6610
Boston, MA 02129
United States of America
dpo@velsera.com

B. DESCRIPTION OF TRANSFER

1. Velsera as Processor

Categories of data subjects whose personal data is transferred

As stated in the Principal Agreement

Categories of personal data transferred

As stated in the Principal Agreement

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None, unless specifically notified by Controller by the Effective Date of this DPA.

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

As stated in the Principal Agreement

Nature of the processing

As stated in the Principal Agreement

Purpose(s) of the data transfer and further processing

As stated in the Principal Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As stated in the Principal Agreement

List for transfers to (sub-) processors, including subject matter, nature and duration of the processing.

See Annex III.

2. Velsera as Controller

Categories of data subjects whose personal data is transferred

Patient pseudonymized data (PierianDx, Inc and UgenTec NV)

User identification information

Categories of personal data transferred

Anonymized and aggregate non-personal data (PierianDx, Inc and UgenTec NV): information that has been stripped of subject-information and aggregated with information of others or anonymized so that the subject cannot reasonably be identified as an individual

Personal (e-)identification data such as e-mail address, name, title, geography, IP address, cookies, session information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

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

As stated in the Principal Agreement

Nature of the processing

To provide the Services, as stated in the Principal Agreement

Purpose(s) of the data transfer and further processing

To provide the Services, as stated in the Principal Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

As permitted under Applicable Laws and regulations or as otherwise stated in the Principal Agreement

C. COMPETENT SUPERVISORY AUTHORITY

Data Protection Commission of the Republic of Ireland.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES (TOMs) INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. **Required Safeguards**. Velsera's safeguards for the protection of Customer Content shall include:

a. limiting access of Customer Content to (i) Velsera employees who have a need to know or otherwise access Customer Content to enable Velsera to perform its obligations under this DPA and (ii) Velsera contractors, agents and representatives who have a need to know or otherwise access Customer Content to enable Velsera to perform its obligations under this DPA, and who are bound in writing by confidentiality obligations sufficient to protect Customer Content in accordance with the terms and conditions of this DPA;

b. securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;

c. implementing network, device application, database and platform security, including appropriate network segmentation and use of intrusion detection tools;

d. securing information transmission, storage and disposal;

e. implementing authentication (including appropriately complex and unique passwords) and access controls within media, applications, operating systems and equipment;

f. encrypting Customer Content stored or transmitted using a security technology or methodology generally accepted in the field of information security;

g. implementing procedures to keep security current and address vulnerabilities as they arise;

h. strictly segregating Customer Content from information of Velsera or its other customers so that Customer Content is not commingled with any other types of information;

i. conducting penetration testing and vulnerability scans and promptly implementing, at Velsera's sole cost and expense, a corrective action plan to correct the issues that are reported as a result of the testing;

j. implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law and this Exhibit; and

k. providing appropriate privacy and information security training to Velsera's employees**.**

l. providing security configuration training for Customer staff by a Velsera information security professional.

m. in the event any hardware, storage media, or mobile media used to collect, receive, transmit, store or otherwise process Customer Content must be disposed of or sent off-site for servicing, ensuring all Customer Content has been sanitized from such hardware and/or media using methods at least as protective as the NIST Guidelines for Media Sanitation (NIST 800-88).

n. Establishing and maintaining secure application development practices to ensure that all software written by or on behalf of Velsera and utilized by Customer will have been assessed for vulnerabilities using a combination of manual and automated methods prior to delivery to Customer. Vulnerabilities will be corrected before being released into production. At a minimum, all known and published vulnerabilities be addressed prior to any developed application being used in production by or on behalf of Customer.

ANNEX III
LIST OF GDPR SUBPROCESSORS

Sub-processor Service	Entity	Usage	Personal Data Type	Entity Location	Website
Amazon Web Services (AWS)	Amazon Web Services, Inc.	Cloud computing infrastructure	Submitted 'omics data, user data	United States	https://aws.amazon.com/
Google Cloud Platform (GCP)	Google LLC	Cloud computing infrastructure	Submitted 'omics data, user data	United States	https://cloud.google.com/
Google Workspace	Google LLC	Email and business applications	user data	United States	https://workspace.google.com/
Stripe	Stripe, Inc.	Payment processing services (credit card payments only)	Credit card data	Dublin, Ireland	https://stripe.com/
Snowflake	Snowflake Inc.	Data warehouse (ARIA only)	Submitted 'omics data	United States	https://www.snowflake.com/
Atlassian / JIRA	Atlassian	Support Ticketing System	user data	Australia	https://www.atlassian.com/
Seven Bridges Genomics UK, Ltd.	Velsera Inc.	Providing user support and professional services	Submitted 'omics data, user data	United Kingdom	https://www.sevenbridges.com/
Seven Bridges Genomics d.o.o	Velsera Inc.	Providing user support and professional services	Submitted 'omics data, user data	Serbia	https://www.sevenbridges.com/
Seven Bridges Genomics Inc.	Velsera Inc.	Providing user support and professional services	Submitted 'omics data, user data	United States	https://www.sevenbridges.com/
PierianDx, Inc.	Velsera Inc.	Providing user support and professional services	Submitted 'omics data, clinical data, user data	United States	https://www.pieriandx.com/

PierianDx India Private Ltd.	Velsera Inc.	Providing user support and professional services	Submitted ‘omics data, clinical data, user data	India	https://www.pieriandx.com/
UgenTec NV	Velsera Inc.	Providing user support and professional services	Submitted ‘omics data, clinical data, user data	Belgium	https://www.ugentec.com/
Microsoft Corporation	Microsoft Office 365	Email and business applications	user data	United States	https://www.microsoft.com/
Aha!	Aha Labs Inc.	Product Roadmapping Tool	user data	United States	https://www.aha.io/
ZenDesk	ZenDesk, Inc.	Support Ticketing System	User data	EEA	https://www.zendesk.com/