VELSERA DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**")is an agreement between you and the entity you represent ("**Client**" "Customer" or "Controller") acting on its own behalf and as agent for each Client Affiliate, and Velsera Inc. and its subsidiaries, including but not limited to Seven Bridges Genomics Inc., PierianDx, Inc. and UgenTec NV, each a Velsera company, **("Velsera"** or "Processor"**)** acting on its own behalf and as agent for each Velsera Affiliate. This DPA forms part of and supplements the Master Services Agreement ("**Principal Agreement**") between Client and Velsera. 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 consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an DPA to the Principal Agreement. Except where the context requires otherwise, references in this DPA to the Principal Agreement are to the Principal Agreement, including this DPA. 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.

1. **Definitions**
   1.1. 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**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with a Party, 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;
      1.1.4. "**Controller Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Controller pursuant to or in connection with the Principal Agreement;
      1.1.5. "**Contracted Processor**" means Velsera, or a Subprocessor;
      1.1.6. "**Data Protection Laws**" means EU Data Protection Laws, UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
      1.1.7. "**EEA**" means the European Economic Area;
      1.1.8. "**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;
      1.1.9. "**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")
      1.1.10. "**Restricted Transfer**" means:
         1.1.10.1. a transfer of Controller Personal Data from any Controller to a Contracted Processor; or
         1.1.10.2. an onward transfer of Controller Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments
         1.1.10.3. 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;

1.1.11. "**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;

1.1.12. "**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;

1.1.13. "**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

1.1.14. "**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.

1.1.15. "**UK Data Protection Laws**" means Data Protection Regulation Act 2018 and the Privacy and Electronic Communications Regulations 2019 (together known as the "UK GDPR") and as amended, replaced or superseded from time to time, including by the UK GDPR and laws implementing or supplementing the GDPR;

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 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 authorises 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 authorised to give the instruction set out in section 4.2.1 on behalf of each relevant Client 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 Article 32(1) of the GDPR.

6.2. 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

6.3. 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.

6.3.1. Velsera and each Velsera Affiliate shall regularly review its Technical and Organizational Security Measures to be updated as necessary.

7. **Subprocessing**

7.1. Controller authorises Velsera and each Velsera Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 7 to appoint) Subprocessors in accordance with this section 7 and any restrictions in the Principal Agreement.

7.2. Velsera and each Velsera Affiliate may continue to use those Subprocessors already engaged by Velsera or any Velsera Affiliate as at the date of this DPA. Velsera's website (currently posted at https://velsera.com) lists Sub-processors that are currently engaged by Velsera. At least 30 days before Velsera engages a Sub-processor, Velsera will update the applicable website and provide Client with a mechanism to obtain notice of that update.

7.3. If, within 30 days of receipt of that notice, Client notifies Velsera in writing of any objections (on reasonable grounds) to the proposed appointment, 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 any Controller and Controller has been provided with a reasonable written explanation of the steps taken.

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

7.4.1. ensure that the arrangement between on the one hand (a) Velsera, or (b) the relevant Velsera Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand 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 on the one hand (a) Velsera, or (b) the relevant Velsera Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Controller Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Controller(s) (and Controller shall procure that each Controller Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

7.4.3. upon request, provide to Client 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 Client may request from time to time.

7.4.4. Notwithstanding sections 7.4.1 through 7.4.3, the Standard Contractual Clauses shall only go into effect if an Alternative Transfer Solution is not available or has not been adopted.

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; 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. 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 Client without undue delay upon Velsera or any Subprocessor becoming aware of a Personal Data Breach affecting Controller Personal Data, providing Client 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. Velsera shall co-operate with Client and each Controller and take such reasonable commercial steps as are directed by Client 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 Client 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, the Contracted Processors.

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. "**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.

11.4. Velsera shall provide written certification to Client that it and each Velsera Affiliate has fully complied with this section 10 within 100 days of the Cessation Date.

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.

12.2. Subject to sections 12.1, 12.2 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. Client or the relevant Client 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 Client 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. Client or the relevant Client 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. **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 in respect of any Restricted Transfer from that Controller to that Contracted Processor.

13.2. The Standard Contractual Clauses shall come into effect as of the Effective Date of this DPA.

13.3. Section 13.1 shall not go into effect if an Alternative Transfer Solution is available and has been adopted.

13.4. 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.

Changes in Data Protection Laws, etc.

14.4. Client 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 Client 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. Client 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 Client 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 Client's notice as soon as is reasonably practicable.

14.7. Neither Client nor Velsera shall require the consent or approval of any Client 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**").

ATTACHMENT 1

STANDARD CONTRACTUAL CLAUSES

MODULE TWO:

Transfer controller to processor

SECTION I

Clause 1
Purpose and scope

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

(d) The Appendix to these Clauses containing the Appendixes 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, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3
Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

---

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

(ii) Clause 8.1(b), 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 into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data 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, as set out in Appendix I.B, 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 described in Appendix II 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 the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

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 in Appendix I.B. 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. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised 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 in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, 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 organisational measures specified in Appendix II. 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 authorised 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 take appropriate measures 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, in particular to notify the competent supervisory authority and the affected data subjects, taking into account 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Appendix I.B.

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 ([2]) (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 defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order 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 take into account 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 referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation 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 30 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. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. 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

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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 authorised 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 in Appendix II the appropriate technical and organisational measures, taking into account 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 authorised 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, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(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 under paragraph (c) 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 as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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) 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 Appendix 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 Appendix 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 behaviour is monitored, are located, as indicated in Appendix I.C, 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 authorising 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 in particular 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 authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other

(iii) any relevant contractual, technical or organisational 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 the third 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 organisational 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 by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar 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 in order 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.

---

documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular 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, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data 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 (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s)/Controller:

Client/Customer:

As stated in the Principal Agreement

Data importer(s)/Processor
Velsera
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.

Available at www.velsera.com

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

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

a. limiting access of Client Content to (i) Velsera employees who have a need to know or otherwise access Client 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 Client Content to enable Velsera to perform its obligations under this DPA, and who are bound in writing by confidentiality obligations sufficient to protect Client 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 Client 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 Client Content from information of Velsera or its other customers so that Client 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 Client 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 Client Content must be disposed of or sent off-site for servicing, ensuring all Client 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 Client will have been assessed for vulnerabilities using a combination of manual and automated methods prior to delivery to Client. 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 Client.

ANNEX III
ADDITIONAL SAFEGUARDS

Preamble

This Annex III supplements the Standard Contractual Clauses for the purpose of providing for additional safeguards in order to ensure adequate protection in response to the requirements specified by the CJEU in its judgment of 16 July 2020, case C-311/18 (Schrems II).

1. Additional Obligations of the Data importer

1.1. The data importer guarantees that he is capable of complying with his obligations stemming from the Standard Contractual Clauses and that local legislation does not prevent him from adhering to the Clauses.

1.2. The data importer shall in any case refrain from a disclosure of Personal Data to governmental or other administrative bodies for purposes of law enforcement or national security ("Relevant Disclosure") on a voluntary and/or cooperative basis. This includes but is not limited to potential requests for voluntary assistance issued under Executive Order 12333 (in the US).

1.3. In case of a request or order for a Relevant Disclosure, the data importer will pro-actively, *inter alia* by seeking respective legal advice, determine and execute any appropriate legal actions or remedies at its disposal in order to avoid a Relevant Disclosure, if in the reasonable judgement of the data importer, such disclosure would go beyond what is necessary in a democratic society; that is, where the disclosure cannot be regarded as a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others. The data importer will use all appropriate legal actions and remedies at its disposal until it has been finally and conclusively judged by a competent court that the data importer must abide by the request or order. This includes but is not limited to:

1.3.1. use every reasonable effort to redirect the third party to request data directly from the data exporter;
1.3.2. challenging the legality of an order for a Relevant Disclosure or any nondisclosure order imposed on the data importer by the appropriate legal remedy, e.g. by filing a petition in accordance with the relevant procedural laws to modify or set aside the order;
1.3.3. challenging a directive issued to the data importer pursuant to applicable laws by the appropriate legal remedy including filing a petition to modify or set aside such directive with the competent court;
1.3.4. when challenging an order, the data importer will seek available interim measures to suspend the effects of the order until the court has decided on the merits.

1.4. The data importer shall provide reasonable assistance to any natural person affected by a Relevant Disclosure who is seeking to suppress this information in a legal proceeding against him or who is bringing a civil suit for damages due to the disclosure or who is seeking other available redress for violations of applicable laws due to the disclosures.

1.5. The data importer will take adequate technical and organizational measures to prevent any Relevant Disclosure, as far as permissible under applicable laws. The data importer warrants that (i) he has not purposefully created back doors or similar programming that could be used to access Personal Data (ii) he has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data, and (iii) that national law or government policy does not require the data importer to create or maintain back doors or to facilitate access to personal data or systems or for the data importer to be in possession or to hand over the encryption key.

1.6. The technical and organizational measures taken by the data importer shall as far as technically feasible include encryption of all Personal Data while at rest or in transfer.

1.7. The data importer shall document the adherence to the SCC and to this Annex II in an appropriate manner and provide any such documentation to the data exporter upon first request. This shall include statistics on the received and/or answered requests or orders for Relevant Disclosures and general

information in relation to the data importer's processes and procedures relating to such requests and orders. The data importer shall demonstrate his capability to adhere to the SCC and this Annex III, including the efficiency implemented technical and organizational measures, upon the data exporter's request.

1.8. Once every year, the data importer shall pro-actively provide to the data exporter a summary of the requests to disclose personal data he and his Sub-Processors have received in the previous year to the extent the data importer and Sub-Processors are not prohibited from a respective disclosure. Section 2.2 applies. In case no such requests occurred, the data importer will provide a respective statement.

1.9. During the term of this Annex III, the data exporter has the right to instruct the data importer to implement further measures or to change implemented measures to the extent any such additional measure is required to fulfill the requirements enshrined in Artt. 44 et seq GDPR pertaining to Personal Data; to fulfill any requirements or obligations put up by a competent data protection supervisory authority; or in case a competent data protection supervisory authority orders the data exporter to implement any such additional measures.