AVEVA DATA PROCESSING ADDENDUM

This AVEVA Data Processing Addendum (this "Data Processing Addendum") supplements and is hereby incorporated into and made a part of those certain AVEVA General Terms and Conditions, entered into by and between AVEVA and the Customer (the "GTCs") and therefore the Agreement between AVEVA and the Customer, to which this Data Processing Addendum is attached or included. Capitalised terms used in this Data Processing Addendum without definition shall have the same meanings ascribed to them in the GTCs.

1. DEFINITIONS.

1.1. **References to Personal Data, Data Subject, Data Controller, Data Processor, Processing**, or **Personal Data Breach** shall be as defined in equivalent or substantially the same definitions under the Applicable DP Legislation.

1.2. "**Applicable DP Legislation**" means any applicable laws and regulation in any relevant jurisdiction relating to the data protection, data privacy, use or processing of any Personal Data under this Agreement that apply to a Party, including where applicable: (i) EU Regulation 2018/1725 ("**GDPR**"); (ii) any laws or regulations ratifying, implementing, adopting, supplementing or replacing such applicable laws and regulation, in each case, as updated, amended or replaced from time to time and (iii) the GDPR as incorporated into law in the United Kingdom pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Data Protection Act 2018 ("**DPA**"), the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419), or any other statute or statutory provision which modifies, consolidates, re-enacts or supersedes the GDPR following the cessation of application of European Union law to the United Kingdom as a result of the withdrawal of the United Kingdom from the European Union.

1.3. "**Customer Personal Data**" shall mean the Personal Data that is uploaded into the Products as Customer Content, or which is otherwise Processed by AVEVA as a Data Processor on behalf of Customer or one of its Affiliates as a Data Controller.

1.4. "**Standard Contractual Clauses" or "SCC**" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data in countries not otherwise recognised as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time) in the form set out in this Data Processing Addendum.

1.5. "**Sub-processor**" means any third party engaged by AVEVA (including any AVEVA Affiliate) to process Customer Personal Data on behalf of Customer.

2. DATA PROTECTION.

2.1. Both Parties will comply with their respective obligations under the Applicable DP Legislation as relevant to this Agreement (and where an Affiliate of a Party is the Data Controller or Data Processor, such Party shall procure that its Affiliate complies with the Applicable DP Legislation). This Data Processing Addendum is in addition to, and does not relieve, remove or replace, a Party's obligations under the Applicable DP Legislation.

2.2. The Parties acknowledge that for the purposes of the Applicable DP Legislation, the Customer is the Data Controller and AVEVA is the Data Processor in respect of the Customer Personal Data. Customer shall not require AVEVA to undertake or engage in any processing activity regarding any Personal Data provided by Customer that requires, or would result in the capacity of a Data Controller in respect of the Personal Data. The following sets out the details of the Customer Personal Data and Processing to be undertaken by AVEVA on behalf of Customer.

Processing by AVEVA	
Scope	Processing of the Customer Personal Data pursuant to provision of the Products, Services and Support Services.
Nature of Processing	Transfer, storage, hosting and such other processing activities that are required to provide and support the Products, and as otherwise set out in this Agreement or specified by the Customer.
Purpose of Processing	The provision of Products, Services and Support Services to the Customer.
Duration of the Processing	The duration of the Term (including the term of any applicable TD), or as required to make relevant Customer Personal Data available to Customer, or such other period as required by applicable law including Applicable DP Legislation, whichever is longer.
Retention Period	As necessary for performance of obligations under the Agreement or as required by applicable law including Applicable DP Legislation, whichever is longer.
Types of Personal Data	The Customer Personal Data (as defined above) which may include but not be limited to name, email address, phone number and job title.
Categories of Data Subject	The Customer's customers, employees, suppliers and related third parties.

2.3. Without prejudice to the generality of Section 2.1, the Customer will ensure that it (or its Affiliate) has a legal basis for Processing, including all necessary and appropriate consents and notices, to enable the lawful transfer of the Personal Data to AVEVA for the duration and purposes of this Agreement.

2.4. AVEVA shall process the Customer Personal Data only on the written instructions of the Customer (as detailed in Section 2.2 above and this Agreement) unless AVEVA is otherwise required by applicable laws including Applicable DP Legislation (in which case such Processing shall be carried out upon notice to Customer, where permitted by applicable law). Confirming acceptance to these terms shall constitute the Customer's written instructions for AVEVA to undertake the Processing detailed in this Agreement and Section 2.2. AVEVA shall not publish, disclose or divulge any Customer Personal Data to any third party (save for Sub-processors appointed pursuant to section 2.7 herein) without the Customer's prior written consent (such approval not to be unreasonably withheld or delayed), unless communication is required by Applicable DP Legislation or by any court or other authority of competent jurisdiction, provided that and to the extent lawfully permitted before making such communication AVEVA provides notice to the Customer and such communication must not reference the Customer (unless legally required to do so).

2.5. AVEVA shall ensure that it has in place appropriate technical and organisational measures, to protect against unauthorised or unlawful Processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data, appropriate and proportionate to the harm that might result from the same, having regard to the state of technological development and the cost of implementing any measures which shall include the measures set out in the Appendix of this Data Processing Addendum.

2.6. Where there is a transfer of Personal Data by a data exporter from within the EEA to a data importer outside the EEA, and such transfer is not governed by an "adequacy decision", is not otherwise "subject to appropriate safeguards" and no "derogation for specific situations" applies, each within the meanings given to them in Articles 45, 46 and 49 of the GDPR respectively (an "**ex-EEA Transfer**"), the ex-EEA Transfer shall be governed by the SCCs which are hereby incorporated into this Agreement and executed by the parties with AVEVA as the 'Data Importer' and the Customer as the 'Data Exporter'.

2.7. Where there is a transfer of Personal Data by a data exporter from within the UK to a data importer outside the UK and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the DPA (an "**ex-UK Transfer**"), then, subject to the remaining provisions of this section 2.7, the SCC shall apply to such ex-UK Transfer in the same way as set out in section 2.6 for ex-EEA Transfers, save that the following amendments to the application of the SCCs for these purposes shall apply (with references in this section 2.7 to Clauses being to Clauses of the SCCs):

2.7.1. the SCCs shall be read and interpreted in the light of the provisions of the UK GDPR and the DPA, and so that they fulfil the intention for them to provide appropriate safeguards as required by Article 46 of UK GDPR;

2.7.2. the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the UK GDPR and the DPA;

2.7.3. the SCCs are deemed to be amended to the extent necessary so they operate:

2.7.3.1. for ex-UK Transfers made, to the extent that the UK GDPR and the DPA apply to AVEVA's processing when making that ex-UK Transfer; and

2.7.3.2. to provide appropriate safeguards for the ex-UK Transfer in accordance with Articles 46 of the UK GDPR Laws; and

2.7.4. without prejudice to the generality of sections 2.7.1, 2.7.2 and 2.7.3 SCCs are amended as follows:

2.7.4.1. Clause 6 Description of the transfer(s) is replaced with: *"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where the Applicable DP Legislation in the UK apply to the data exporter's processing when making that transfer."*;

2.7.4.2. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK GDPR and DPA" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR and DPA;

2.7.4.3. References to Regulation (EU) 2018/1725 are removed;

2.7.4.4. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK";

2.7.4.5. Clause 13(a) and Annex I.C are not used; the "competent supervisory authority" is the ICO;

2.7.4.6. Clause 17 is replaced to state "*These Clauses are governed by the laws of England and Wales*";

2.7.4.7. Clause 18 is replaced to state: "*Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts*".

2.8. AVEVA's liability under the SCC shall form part of AVEVA's liability under the GTCs, and shall be subject to any exclusions and limitations on AVEVA's liability set out in the GTCs.

2.9. If Applicable DP Legislation require the data exporter to execute the SCC applicable to a transfer of Personal Data to a data importer as a separate agreement, AVEVA shall, on written request of the Customer, promptly execute such SCC (as applicable and incorporating such amendments as may reasonably be required to reflect the details of the transfer and the requirements of the relevant Applicable DP Legislation).

2.10. If there is any conflict or ambiguity between the terms of this Data Processing Addendum and the SCC, the term contained in the SCC shall have priority (but only to the extent and in respect of the transfer, and not in respect of any other processing activity).

2.11. AVEVA shall, in relation to any Customer Personal Data Processed in connection with the performance by AVEVA of its obligations under this Agreement:

2.11.1. ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and

2.11.2. taking into account the nature of the Processing and the information available to AVEVA, assist the Customer, at the Customer's cost, in responding to any request from a Data Subject under Applicable DP Legislation and in ensuring compliance with its obligations under the Applicable DP Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators, as applicable;

2.11.3. notify the Customer without undue delay on becoming aware of a Personal

Data Breach;

2.11.4. on termination of the Agreement, delete or return Customer Personal Data and copies thereof to the Customer unless required by applicable law including Applicable DP Legislation to continue to store the Customer Personal Data (in which case AVEVA shall retain the same as required by applicable law and its confidentiality obligation under this Agreement) for the Retention Period; and

2.11.5. make available to the Customer all information necessary to demonstrate AVEVA's compliance with its obligations under this Section 2.11 and subject to AVEVA's reasonable security procedures, business and operational requirements and AVEVA's confidentiality obligations, allow for audits, including inspections, conducted by the Customer its supervisory authority or regulator, at Customer's own cost and expense, upon Customer giving AVEVA prior written notice of no less than thirty (30) days of its intent to conducts such audit or inspection. For the avoidance of doubt, such audit and inspection shall only be for the purposes of determining AVEVA's compliance with its obligations under this Data Processing Addendum.

2.12. The Customer hereby consents to AVEVA appointing third-party sub-processors of Customer Personal Data under this Agreement ("Sub-processors"), provided that:

2.12.1. (i) The Customer has provided its prior written consent for appointment of such Sub-processor; or (ii) Sub-processor is an Affiliate of AVEVA or identified AVEVA's list of Sub-processors as specified at https://www.aveva.com/en/legal/trust/data-processing/ and as updated by AVEVA from time to time and notified to the Customer;

2.12.2. The Customer may object in writing to use of a Sub-processor, and shall describe its reasons for the objection, and may request corrective steps to be taken;

2.12.3. If the Customer objects to the use of a Sub-processor, AVEVA shall use it best efforts to address the objection through one of the following options (to be selected at AVEVA's sole discretion): (i) AVEVA will abort its plans to use the Sub-processor for the processing of Customer Personal Data; or (ii) AVEVA will take the corrective steps requested by the Customer in its objection (which removes the Customer's objection) and proceed to use the Sub-processor for the processing of Customer Personal Data. If AVEVA is unable to address the objection through such means, AVEVA may cease to provide, or the Customer may agree not to use (temporarily or permanently), the particular aspect of the Service or Product that would involve the use the Sub-processor for the processing of Customer Personal Data. Termination rights, as applicable and agreed in this Agreement, shall apply accordingly; and

2.12.4. AVEVA has entered into, or (as the case may be) will enter into with the third-party sub-processor a written agreement incorporating terms which are substantially similar to those set out in this Data Processing Addendum. AVEVA acknowledges and agrees that it remains liable to the Customer for any breach of the terms of this Data Processing Addendum by any Sub-processor.

.

Data Transfer Agreement Incorporating Standard Contractual Clauses

Module 2: Transfer Controller to Processor

CUSTOMER, as detailed in Appendix, Annex 1

(hereinafter referred to as data exporter)

And

AVEVA, as detailed in Appendix, Annex 1

(hereinafter referred to as data importer)

herewith agree as follows.

STANDARD CONTRACTUAL CLAUSES

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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1(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 Annex I.B.

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data 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 Annex 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 Annex 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 Annex 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 Annex 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 Annex 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 (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) 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 thirty (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. 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 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 to 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 Annex

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 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 behaviour is monitored, are located, as indicated in Annex 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;

(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.

(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.

APPENDIX

ANNEX I

A. LIST OF PARTIES

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

1. Name:

   Address:

   Contact person's name, position and contact details:

   Activities relevant to the data transferred under these Clauses:

   Receipt of software services from Data importer

   Signature and date: As per the relevant Transaction Document

   Role (controller/processor): Controller

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

2. Name:

   Address:

   Contact person's name, position and contact details:

   The Data Protection Officer **-** dataprotection@aveva.com

   Activities relevant to the data transferred under these Clauses:

   Provision of Software Services to Data Exporter

   Signature and date: As per the relevant Transaction Document

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees and contractors of Data Exporter, Data Exporter's affiliates, sub-contractors and related third parties

Categories of personal data transferred

Name, Job title or position, business email address, business telephone number, IP address

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

Continuous

Nature of the processing

Collection, organisation, storage, consultation, use, dissemination and erasure of personal data in relation to the purpose.

Purpose(s) of the data transfer and further processing

Processing for provision of contractual services and ancillary purposes

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

The duration of the Processor's commercial relationship with the Controller plus any relevant limitation period required under local law

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

Processing for provision of contractual / support services during the term of the agreement with the Controller and for the relevant limitation period required under local law

C. COMPETENT SUPERVISORY AUTHORITY

The Data Protection Commissioner of the Republic of Ireland.

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

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

AVEVA shall exercise reasonable efforts to implement the following measures in connection with information security of Customer Personal Data:

a) backing-up the Customer Personal Data at regular intervals;
b) ensuring that AVEVA is able, to restore lost or damaged Customer Personal Data from the latest back-up;
c) not using the Customer Personal Data except as required for the performance of its obligations under the Agreement;
d) upon Customer's written request, grant Customer access to current ISO 27001:2013 certificate and annual SAE18 SOC 2/ISAE3402 SOC (Type II) reports in respect of specific Software supplied under the Agreement (where stated to be available for that Software in the applicable Transaction Document or Software Schedule) addressing data security requirements stated in this Data Processing Addendum;
e) complying with information management procedures and safeguards based on Good Industry Practice, including those concerning the security of the Customer Personal Data. For the purpose of this Data Processing Addendum, "Good Industry Practice" means that degree of skill, care and prudence which would ordinarily be expected of a skilled and experienced supplier of software products and services of the same or a similar nature to the Products, Services and Support Services;
f) maintaining and enforcing safeguards against the destruction, loss, or alteration of Customer Personal Data that are no less rigorous than those maintained by AVEVA for its own information of a similar nature or that otherwise comply with Good Industry Practice;
g) in the event of any destruction, loss, or reduction in the accessibility or usability of Customer Personal Data which is caused by AVEVA, restoring such data using Good Industry Practice data restoration techniques;
h) taking all necessary precautions, in accordance with Good Industry Practice, to prevent any Malicious Code (as defined in the AVEVA Software and Support Addendum) affecting the Products or Services and the Customer Personal Data, including but not limited to using the latest versions of anti-malware software (including latest definitions and updates) available from an industry accepted anti-malware software vendor to check for and delete Malicious Code;
i) notifying the Customer as soon as practicable upon becoming aware of any Security Incident and providing the Customer with a detailed description of the Security Incident, the type of Customer Personal Data that is the subject of the Security Incident, the identity of any affected individuals and all other information and cooperation which the Customer may reasonably request. For the purpose of this Data Processing Addendum, "Security Incident" shall mean any incident resulting in loss, destruction or material alteration of Customer Personal Data, or unauthorized third-party access to Customer Personal Data;
j) taking immediate action, at AVEVA's own cost, to investigate any Security Incident, to identify, prevent and mitigate the effects of such Security Incident and, with the Customer's prior agreement, to carry out any recovery or other action necessary to remedy the Security Incident. AVEVA must ensure that any such recovery or other action does not compromise any technical information or artefacts (including, for example, logs) which would reasonably be required by the Customer to understand the Security Incident, mitigate its effects and/or prevent its recurrence;
k) not issuing, publishing or otherwise making available to any third party any press release or other communication concerning a Security Incident without the Customer's prior approval (such approval not to be unreasonably withheld or delayed), unless communication is required by Applicable DP Legislation or by any court or other authority of competent jurisdiction provided that before making such communication AVEVA to the extent lawful provides notice to the Customer that it will be making such communication and such communication must not reference the Customer (unless legally required to do so);
l) use of data centres where Customer Personal Data is stored, accessed or otherwise processed, in accordance with Good Industry Practice;
m) keeping any Customer Personal Data in electronic form logically separated from any information, data or material of any third party;
n) ensuring that access to the Products, Services and Customer Personal Data by AVEVA's personnel is restricted on a strictly need to know basis and that all AVEVA's personnel who are granted such access have completed appropriate security training in line with the AVEVA Group Data Privacy policy; and
o) performing continuous service improvement and continuous monitoring of the Services used in connection with the provision of the Products and Services and promptly rectifying any security vulnerabilities identified by such testing.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors at the following link:

https://www.aveva.com/en/legal/trust/data-processing/