DATA PROCESSING ADDENDUM

Version: 19 March 2026

This AVEVA Data Processing Addendum ("**DPA**") is incorporated into and forms part of the AVEVA General Terms and Conditions (GTCs) and the applicable Order Form, or any other agreement between AVEVA and the Customer (the "**Agreement**") and applies to the Processing of the Customer Personal Data (as defined below) by AVEVA and its Affiliates when providing Cloud Services, Support Services and Professional Services (collectively "**Services**"). The Services are described in the relevant Agreement.

In the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA shall control to the extent such conflict or inconsistency relates to the Processing of the Customer Personal Data. In the event of any direct conflict between this DPA and the EU SCCs, the UK SCC Addendum, and/or the Swiss SCC Addendum, the EU SCCs, the UK SCC Addendum, and/or the Swiss SCC Addendum (as applicable) shall prevail.

1. DEFINITIONS

"Applicable Data Protection Laws" means all applicable data protection and privacy laws or regulations in any relevant jurisdiction that apply to the Processing of Personal Data Processed Under This DPA including: (i) the EU General Data Protection Regulation EU/2016/679 ("**GDPR**"); (ii) the UK GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland and the UK Data Protection Act 2018 ("**UK GDPR**"); (iii) the Swiss Federal Act on Data Protection ("**FADP**"); and (iv) the California Consumer Privacy Act as amended by the California Privacy Rights Act ("**CCPA/CPRA**"), together with applicable US State Privacy Laws; in each case, as amended, superseded, or replaced from time to time.

"Customer Personal Data" means: (a) the Personal Data provided by or on behalf of the Customer and its Users via the CONNECT platform for the purposes of User identification, authentication, and access management; and (b) any Personal Data that the Customer or its Users may provide to AVEVA in the course of receiving Support Services or Professional Services under the Agreement, as further described in the Annex to this DPA.

"EU SCCs" means the Standard Contractual Clauses for the transfer of Personal Data to Third Countries adopted by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914, as may be amended or replaced from time to time.

"Personal Data Breach" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data Processed Under This DPA on systems managed by or otherwise controlled by AVEVA.

"Personal Data Processed Under This DPA" means collectively: (a) Customer Personal Data; and (b) Usage Metrics Data (to the extent such data constitutes Personal Data).

"Special Categories of Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, as defined in Article 9 of the GDPR and equivalent provisions under Applicable Data Protection Laws.

"Sub-processor" means any third-party provider engaged by AVEVA to assist with the Processing of Customer Personal Data.

"Swiss SCC Addendum" means the EU SCCs as modified for the purposes of the FADP, whereby references to the GDPR are read as references to the FADP, references to "Member State" include Switzerland, and the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

"Third Country" means any country outside the European Economic Area (EEA), the United Kingdom (UK), and Switzerland that has not received an adequacy decision under Applicable Data Protection Laws.

"UK SCC Addendum" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under Section 119A of the UK Data Protection Act 2018, as may be amended or replaced from time to time.

"Usage Metrics Data" means Personal Data derived from Users' interactions with the Products and Services, including login frequency, feature usage, session duration, and related telemetry data, which AVEVA Processes as an independent Data Controller.

"US State Privacy Laws" mean all state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the CCPA/CPRA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

Capitalised terms used but not defined in this DPA shall have the same meanings ascribed to them in the Agreement or the Applicable Data Protection Laws.

2. ROLES AS DATA CONTROLLER AND DATA PROCESSOR

2.1 With respect to Customer Personal Data, the Customer is the Data Controller and AVEVA is the Data Processor.

2.2 With respect to Usage Metrics Data, AVEVA is an independent Data Controller and shall Process such data for the purpose of verifying the Customer's licensed use of AVEVA Products and Services and maintaining the security, availability and performance of the Products and Services and in accordance with Applicable Data Protection Laws.

2.3 Each party shall comply with their respective obligations under Applicable Data Protection Laws.

2.4 The Customer is responsible for complying with its obligations as a Data Controller under Applicable Data Protection Laws, including obtaining any consents, providing any notices, and otherwise establishing the required legal basis.

2.5 For the purposes of US State Privacy Laws, AVEVA is a service provider and shall not sell, share, or use Customer Personal Data for any purpose other than performing the Services.

2.6 The provisions of this DPA relating to AVEVA's obligations as a Data Processor (including Sections 3, 5, 7, 10, 11 and 12) apply to Customer Personal Data only. Sections 6 (Data Transfers), 8 (Security) and 9 (Personal Data Breach) apply to all Personal Data Processed Under This DPA.

3. PROCESSING OF CUSTOMER PERSONAL DATA

3.1 AVEVA and any persons acting under its authority under this DPA, including Sub-Processors and Affiliates, shall Process Customer Personal Data only for the purposes of performing Services in accordance with the Customer's written instructions as specified in the Agreement and this DPA, and as otherwise required by applicable laws. Where AVEVA is required to Process Customer Personal Data to comply with applicable laws, AVEVA shall inform the Customer of that requirement before Processing, unless prohibited by law.

3.2 If AVEVA reasonably believes that the Customer's instructions infringe Applicable Data Protection Laws, AVEVA shall promptly inform the Customer. AVEVA shall not be required to independently assess the lawfulness of the Customer's instructions and shall not be liable for carrying out any Processing in accordance with the Customer's written instructions.

3.3 AVEVA shall ensure that any person authorised to Process Customer Personal Data under this DPA is subject to appropriate obligations of confidentiality, whether contractual or statutory. AVEVA's employees are required to complete annual data protection and cyber security training and to comply with AVEVA's corporate data and security policies and procedures.

3.4 AVEVA may aggregate or de-identify Customer Personal Data such that it no longer constitutes Personal Data under Applicable Data Protection Laws. Such data is not Customer Personal Data for the purposes of this DPA.

3.5 AVEVA will notify the Customer promptly of any legally binding demand for disclosure of Customer Personal Data, unless prohibited by law. AVEVA will disclose only the minimum amount of Customer Personal Data necessary to comply and will provide the Customer with reasonable assistance to facilitate the Customer’s timely response to such demand.

3.6 AVEVA may disclose Customer Personal Data to its Affiliates or to a successor entity in connection with a merger, acquisition, or reorganisation of its business, provided that: (a) AVEVA notifies the Customer as soon as reasonably practicable, unless prohibited by law; and (b) any recipient is bound by data protection obligations no less protective than those in this DPA.

4. DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA

4.1 The categories of Data Subjects and Personal Data Processed under this DPA are set out in Annex 1 to this DPA. AVEVA does not process any Special Categories of Personal Data in connection with the Services.

5. SUB-PROCESSING

5.1 The Customer authorises AVEVA to engage Sub-processors for the Processing of Customer Personal Data. AVEVA shall ensure that each Sub-processor is bound by written data protection obligations no less protective than those set out in this DPA. AVEVA shall remain liable for the acts and omissions of its Sub-processors to the extent required by Applicable Data Protection Laws.

5.2 AVEVA shall maintain a current list of Sub-processors, available to the Customer upon written request or at AVEVA's Legal Resources page: https://www.aveva.com/en/legal/. AVEVA shall provide at least thirty (30) calendar days' advance notice before authorising a new Sub-processor to Process Customer Personal Data.

5.3 If the Customer has reasonable grounds to object to a new Sub-processor, it shall notify AVEVA in writing within fourteen (14) calendar days of AVEVA's notice and the Parties shall discuss the objection in good faith with a view to reaching a resolution.

5.4 Upon request (no more than once per twelve (12) month period), AVEVA shall make available relevant third-party certifications (such as SOC 2 or ISO 27001) relating to its Sub-processors' data protection practices.

6. DATA RESIDENCY AND DATA TRANSFERS

6.1 Where applicable, when the relevant Product or Service is first deployed and configured, the Customer may select the primary cloud region where the Customer Personal Data shall reside at rest. The cloud regions currently available are set out in the AVEVA Service Descriptions for Cloud Services: https://www.aveva.com/en/legal/service-description/. Backup data shall be stored in the same cloud region as the primary Customer Personal Data.

6.2 Notwithstanding the foregoing, AVEVA may transfer Customer Personal Data outside the Customer's selected cloud region as necessary to perform the Services under the Agreement, including operational support, maintenance, and incident response which may be delivered from locations including, but not limited to, the United States, India and other Third Countries. AVEVA shall comply with the requirements of this DPA regardless of where Customer Personal Data is stored or Processed.

6.3 Where the Processing involves the international transfer of Customer Personal Data of residents of a country within the EEA, Switzerland, or the United Kingdom to AVEVA, its Affiliates, or Sub-Processors in a Third Country, and no other legal basis for the international transfer exists, such transfers shall be subject to the EU SCCs, the UK SCC Addendum, and/or the Swiss SCC Addendum (as applicable).

6.4 For international transfers to Third Countries, the Parties hereby incorporate by reference:

(a) the EU SCCs (Module One and Module Two) for transfers subject to the GDPR;

(b) the UK SCC Addendum for transfers subject to UK GDPR; and

(c) the Swiss SCC Addendum for transfers subject to the FADP.

6.5 Where Customer Personal Data is subject to data protection laws of jurisdictions other than the EEA, Switzerland, or the United Kingdom that impose restrictions on cross-border transfers, each Party shall ensure that any transfer complies with Applicable Data Protection Laws. Where an additional transfer mechanism or agreement is required under Applicable Data Protection Laws, the Parties shall cooperate in good faith to put such mechanism or agreement in place.

7. REQUESTS FROM DATA SUBJECTS

7.1 Users may exercise their data subject rights (including access, rectification and deletion) directly through the CONNECT platform account settings where such functionality is available.

7.2 Where a Data Subject request cannot be fulfilled through the CONNECT platform, AVEVA shall provide the Customer with reasonable assistance to respond to such request. To the extent legally permitted, AVEVA shall promptly redirect any request from a Data Subject to the Customer. Unless required by Applicable Data Protection Laws, AVEVA will not respond substantively to any request without the Customer's prior instruction.

8. SECURITY

8.1 AVEVA shall implement and maintain appropriate technical and organisational measures designed to protect Personal Data Processed Under This DPA against misuse, accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access, in accordance with Applicable Data Protection Laws. AVEVA shall continually review and seek to improve its security measures and reserves the right to modify them from time to time, provided that any such modification shall not materially diminish the overall level of protection afforded to Personal Data Processed Under This DPA during the term of the Agreement.

9. PERSONAL DATA BREACH

9.1 AVEVA shall notify the Customer without undue delay and in any event within seventy-two (72) hours after becoming aware of a Personal Data Breach involving Customer Personal Data in AVEVA's possession, custody, or control.

9.2 Such notification shall include, to the extent reasonably available at the time of notification: (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and records concerned; (b) the contact details of AVEVA's data protection officer or other designated contact; (c) a description of the likely consequences; and (d) a description of the measures taken or proposed to address the breach. Where it is not possible to provide all information at the time of initial notification, AVEVA shall provide such information in phases without further undue delay.

9.3 The Customer shall coordinate with AVEVA on the content of any public statements or required notices to Data Subjects and/or Supervisory Authorities. Neither Party shall name or identify the other Party in any public statement relating to a Personal Data Breach without the other Party's prior written consent, unless required by Applicable Data Protection Laws.

9.4 AVEVA's notification of a Personal Data Breach under this Section shall not be construed as an acknowledgement of fault or liability by AVEVA.

10. PROVIDING INFORMATION AND ASSISTANCE

10.1 The Customer may provide additional documented instructions to AVEVA related to the Processing of Customer Personal Data. AVEVA shall comply with such instructions, provided that: (a) the instructions are reasonable and technically feasible within the Products and/or Services; (b) where such instructions impose additional costs on AVEVA beyond the scope of the Agreement, the Parties shall agree such costs in advance; and (c) AVEVA shall not be required to comply with any instruction that would cause AVEVA to breach Applicable Data Protection Laws.

10.2 The Parties acknowledge that AVEVA's systematic Processing of Customer Personal Data is limited to authentication and access management data as described in Annex 1 to this DPA. To the extent that the Customer or its Users provide additional Personal Data in the course of Support Services or Professional Services, the Customer is responsible for ensuring that such disclosure is necessary and proportionate, and AVEVA shall Process such data solely for the purpose of delivering the relevant Service. Accordingly: (a) the risk to Data Subjects arising from such Processing is low; (b) AVEVA shall provide reasonable assistance to the Customer in responding to its obligations under Applicable Data Protection Laws, to the extent that such obligations relate to the Customer Personal Data; and (c) such assistance shall be proportionate to the nature and scope of the Processing and shall be provided at the Customer's cost where it falls outside the standard scope of the Products and/or Services.

11. RETURN AND DELETION OF DATA

11.1 Upon expiry or termination of the Agreement, AVEVA shall deactivate all User accounts and securely delete Customer Personal Data within sixty (60) calendar days, except where retention is required by applicable law. Where retention is required, AVEVA shall continue to comply with the relevant provisions of this DPA and shall not actively Process such data for any other purpose until deletion is complete. AVEVA shall provide written confirmation of deletion upon request.

12. AUDIT

12.1 AVEVA shall make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA, including, where available, relevant third-party audit reports, certifications (such as SOC 2 or ISO 27001), or summaries of security measures (collectively, "Compliance Materials").

12.2 The Customer shall first review the Compliance Materials before exercising any further audit right. Where the Compliance Materials do not reasonably satisfy the Customer's obligations under Applicable Data Protection Laws, the Customer may carry out an audit of AVEVA's Processing of Customer Personal Data, subject to the following conditions: (a) audits shall be limited to once per calendar year, unless required by Applicable Data Protection Laws or following a Personal Data Breach; (b) any such audit shall take the form of conference calls with AVEVA's relevant personnel and/or AVEVA's completion of reasonable security questionnaires submitted by or on behalf of the Customer; (c) the Customer must provide AVEVA with a written audit plan at least thirty (30) days in advance; and (d) any such audit shall be conducted at the Customer's sole cost and expense.

12.3 The Customer may appoint a qualified third-party auditor, subject to AVEVA's prior written approval (not to be unreasonably withheld), and provided that such auditor executes a confidentiality agreement with AVEVA on terms reasonably acceptable to AVEVA.

12.4 Where the Customer's competent Supervisory Authority requires a direct audit of AVEVA under Applicable Data Protection Laws, AVEVA shall cooperate with and provide reasonable assistance to the Supervisory Authority in accordance with its legal obligations.

12.5 The Customer shall treat any audit findings as Confidential Information in accordance with the Agreement and use them solely for the purpose of assessing AVEVA's compliance with this DPA and Applicable Data Protection Laws.

13. LIMITATION OF LIABILITY

13.1 The liability of each Party under or in connection with this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement. Any claims arising under or in connection with this DPA shall count towards, and not be in addition to, any aggregate liability cap set out in the Agreement.

14. TERM

14.1 This DPA shall take effect on the Effective Date of the Agreement and shall automatically terminate upon the later of: (a) the expiry or termination of the Agreement; and (b) the date on which AVEVA no longer retains any Customer Personal Data.

15. NOTICES AND CONTACT

15.1 All notices under this DPA shall be in writing and sent to the contact details specified in the Agreement. Data protection enquiries and instructions relating to this DPA shall be directed to AVEVA's Privacy Team at: dataprotection@aveva.com.

ANNEX 1 - Description of Processing Activities

PART A — CONNECT Platform (Systematic Processing)

AVEVA's Role	Data Processor
Subject Matter	Processing of Personal Data via the CONNECT platform in connection with the provision of Cloud Services.
Purpose of Processing	User identification, authentication, and access management to enable Users to access and use AVEVA Products and Services.
Duration	For the duration of the Agreement, plus the 60-day post-termination deletion period set out in Section 11.
Data Subjects	Authorised Users of the Customer, being employees, contractors, or authorised representatives of the Customer.
Categories of Personal Data	• Account identifiers: first name, last name, business email address • Authentication data: User credentials (username, password hash), multi-factor authentication tokens • Access management data: role assignments, permissions, access logs • Technical identifiers: IP address, device identifiers, session identifiers, browser type • Timestamps: login/logout times, account creation and modification dates
Special Categories	None. AVEVA does not process any Special Categories of Personal Data in connection with the Services.
Transfers to Third Countries	As described in Section 6 of this DPA. Operational support may be provided from the United States, India, and other Third Countries where AVEVA and its Sub-processors operate.

PART B — Support Services and Professional Services (Incidental Processing)

AVEVA's Role	Data Processor
Subject Matter	Processing of Personal Data provided by the Customer or its Users in the course of receiving Support Services or Professional Services.
Purpose of Processing	Resolving support queries; troubleshooting; delivering professional services engagements as described in the applicable Statement of Work or Service Description.
Duration	For the duration of the relevant support case or professional services engagement.
Data Subjects	Authorised Users of the Customer; other individuals whose Personal Data Users may share in support tickets, screen-sharing sessions, or professional services engagements.
Categories of Personal Data	As determined by the Customer — may include any Personal Data shared by Users in support tickets, screen-sharing sessions, uploaded files, or professional services engagements. The Customer's Users are responsible for ensuring that such disclosure is necessary and proportionate.
Special Categories	Not expected. The Customer and its Users shall not provide Special Categories of Personal Data to AVEVA unless strictly necessary and with prior written notice to AVEVA.

Transfers to Third Countries	As described in Section 6 of this DPA. Support and professional services may be delivered from the United States, India, and other Third Countries where AVEVA and its Sub-processors operate.

PART C — Usage Metrics Data (Controller Processing)

AVEVA's Role	Independent Data Controller
Subject Matter	Processing of Usage Metrics Data derived from Users' interactions with AVEVA Products and Services.
Purpose of Processing	Verifying the Customer's licensed use of AVEVA Products and Services; maintaining the security, availability and performance of the Product and Services, as described in the Agreement.
Data Subjects	Authorised Users of the Customer.
Categories of Personal Data	• Login frequency and session duration • Feature usage and interaction data • Telemetry data • Technical identifiers (to the extent constituting Personal Data)
Legal Basis	AVEVA's legitimate interests (Article 6(1)(f) GDPR) in verifying licensed use, performance monitoring and securing its Products and Services.
Retention	In accordance with AVEVA's data retention practices and Applicable Data Protection Laws.

Note: *AVEVA shall ensure that Users are informed of the Processing of Usage Metrics Data in accordance with its transparency obligations under Applicable Data Protection Laws, whether through an in-product privacy notice, the CONNECT platform, or other appropriate means.*