DATA PRIVACY, SECURITY, AND PROCESSING AGREEMENT (“DPA”)

This DPA is between the Customer identified in the applicable Subscription Services Agreement (“SSA”) and the Planview entity identified in the SSA (“Planview”), and governs the processing by Planview of Customer’s PII (as defined below), subject to the SSA.

1. Purpose of the DPA

For the purposes of this DPA, “PII” means personal data, personal information and/or personally identifiable information, as defined in Applicable Privacy Laws identified below. The purpose of Planview’s processing of PII is the provision to Customer of various services as described in the SSA (the “Services”). This DPA establishes the instructions given by Customer to Planview and the agreed processing activities by Planview on behalf of Customer when processing PII in connection with the Services. Planview acts as a data processor or service provider, as defined under Applicable Privacy Laws (“Processor”) and Customer acts as a data controller, business fiduciary, or data fiduciary, as defined under those Applicable Privacy Laws (“Controller”) in relation to its own data, or (if applicable) both parties act as a Processor of their respective customers’ data.

The provisions of this DPA shall apply to any and all PII processing activities performed by Planview on behalf of Customer, especially for the purposes of art. 28 of the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the “GDPR”), and in accordance with any other privacy and data protection laws the parties may be subject to in relation to the processing of PII in the context of the Services, including (if and to the extent applicable), but not limited to: (i) the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. (the “CCPA”), as amended by the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq. (“CPRA” and collectively, the “California Privacy Laws”); (ii) the Indian Digital Personal Data Protection Act, 2023 (the “DPDPA”); (iii) the Data Protection Law, DIFC Law No. 5 of 2020, as amended (the “DPL”); (iv) the Australian Privacy Act 1988 (the “Privacy Act”); (v) the UK General Data Protection Regulation as defined in section 3(10) of the Data Protection Act 2018 (the “UK GDPR”); and (vi) the Swiss Federal Act on Data Protection of 25 September 2020, as revised (the “Swiss FADP”) (collectively, the “Applicable Privacy Laws”).

2. How this DPA Applies

This DPA is subject to the terms of, and is fully incorporated in and made part of, the SSA, and shall supersede and replace any existing data processing terms in or addendum to the SSA and any prior and contemporaneous agreements, proposals, or representations, written or oral, concerning its subject matter, unless otherwise explicitly stated herein. In the event of any conflict between this DPA and any other provision of the SSA with respect to PII, this DPA shall control.

3. Definitions

Any capitalized terms used herein shall have the meaning set forth in the SSA, within this DPA, or in any of the Applicable Privacy Laws, as applicable.

4. Subject Matter, Scope, and Duration of Processing Activities

The subject matter of the processing activities performed by Planview as a Processor under this DPA is Customer Data, including PII, used by Customer in connection with the Services for project and portfolio management, digital product development, resource planning, and related business operations. Such processing activities comprise (i) collecting, storing, and using PII for the identification of Users; (ii) collecting, hosting, and storing Customer Data and project-related information, including PII; (iii) accessing or consulting Customer Data, including PII, for the provision of Support Services and/or Professional Services; (iv) recording, storing, and examining activities in information systems that process or access Customer Data for security and integrity operations (as further described in Annex 3); and (v) collecting and using Customer Data and project-related information to provide in-app AI and data fabric features and to ensure outputs meet Planview standards for consistency and quality. The processing starts with execution of the SSA and ends upon termination or expiry of the provision of the Services, notwithstanding the additional Customer Data retrieval period as described in the SSA, during which the DPA shall remain applicable. Planview may retain backup copies of Customer Data, including PII, for a limited period after the termination or expiry of the SSA, in accordance with its data retention policies, provided such copies remain under the protection of this DPA and are not accessed or processed for any purpose other than backup storage for disaster recovery.

Planview may process Customer PII (obtained directly from Customer or indirectly from third parties) for the purpose of Planview’s own administration, facilitation, and improvement of the Services, which it shall do as a Controller and therefore not subject to the provisions of this DPA, for compliance with its own legal obligations, or the pursuit of its legitimate interests. Customer shall make available to its end users, employees, authorized agents/contractors, representatives, and any other persons using or mentioned in the Services the necessary information regarding Planview’s processing of their PII as a Controller, by directing them to the Privacy Statement on the Planview website. For information purposes only, Planview’s processing of Customer PII for its own administration, facilitation, and improvement of the Services comprises the following categories of data: (i) Customer history, contract billing and payments data, disclosed information from third parties (e.g., credit reference agencies or public directories), and Customer points of contact and authorized signatories’ contact details and signature (where applicable), in each case if and to the extent this data contains PII, for Planview’s internal customer relationship management (CRM) purposes; and (ii) User behavioral data and User performance data, which is aggregated and anonymized to derive insights of usage of the Services in order to improve them.

5. Categories of Personal Data

The PII subject to Planview’s processing activities comprises in general the following categories/data types: (i) contact details (e.g. name, professional address, professional e-mail address, professional telephone number, login data, and local time zone information); (ii) employment details (e.g. company name, job title, grade/position, department, demographic data, and location data); (iii) project and portfolio-related information (e.g., skills, cost rates, time and expenses recorded, tasks and projects assigned, and resource capability and availability); (iv) IT and device systems information and traffic data (which may include user ID, IP address, and software usage pattern tracking information, such as data derived from cookies); (v) data subjects’ e-mail content and transmission data, which is available on an incidental basis for the provision of Support Services; (vi) any PII supplied by User to the Services.

Customer, not Planview, is solely responsible for determining what Customer Data, including PII, Customer inputs into or processes through the Services. Planview shall have no responsibility for the processing of any categories of PII beyond those listed in the above paragraph, including special categories of personal data or sensitive PII as defined under Applicable Privacy Laws, to the extent such PII is provided to or processed through the Services by Customer.

6. Categories of Data Subjects

The categories of data subjects comprise in general Customer employees, Users (as defined in the SSA), authorized consultants and other agents, or other persons mentioned in the Services.

7. Technical and Organizational Measures (“ToMs”)

The ToMs shall guarantee a data protection level appropriate to the risk concerning confidentiality, availability, and integrity of the Customer PII, in accordance with the availability and resilience of the IT systems. The state of the industry, the implementation costs, the nature, scope, and purposes of processing, as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons determine the appropriate ToMs to be implemented.

Planview’s ToMs, which are hereby expressly approved by Customer, are further specified in Annex 3 to this DPA. The ToMs are subject to constant technical progress and further development. In this respect, Customer allows for Planview to implement alternative adequate ToMs, provided that in so doing, the security of the defined measures must not be reduced. Planview shall periodically monitor its internal processes and ToMs to ensure that processing activities are carried out in accordance with the requirements of Applicable Privacy Laws for the protection of the rights of the data subjects.

8. Principles of the Processing Activities and Data Subject Rights

The processing activities shall be performed at Customer’s instructions. Therefore, Planview may carry out, retain, rectify, erase, or restrict the processing of PII only on documented instructions from Customer, as described in this DPA, and/ or in accordance with the SSA, unless required to do so by any applicable law to which Planview is subject. In such a case, Planview shall inform Customer of that legal requirement before processing, unless Planview is prohibited from informing Customer by that law on important grounds of public interest. Planview shall immediately inform Customer if, in its opinion, an instruction infringes any applicable law, including the GDPR and/or other Applicable Privacy Laws.

Insofar as a data subject contacts Planview directly to exercise their rights under Applicable Privacy Laws, Planview will immediately instruct the data subject to submit the request to Customer. Notwithstanding the foregoing, Planview shall assist Customer in the fulfilment of the latter’s obligation to respond to data subject requests for exercising their rights, insofar as this is possible, taking into account the nature of the processing and the PII effectively accessed and processed by Planview, and provided that Customer expressly requests this assistance via clear and documented instructions conveyed to Planview in a timely manner.

9. California Privacy

To the extent that Planview processes any Customer PII relating to individuals who are California residents, Planview shall comply with the applicable provisions of the California Privacy Laws. For the purposes of the California Privacy Laws, the parties agree that (i) Planview is a “Service Provider” in the performance of its obligations, not a “Third Party” or a “Contractor”, (ii) Customer is a “Business,” and (iii) the transfer of Customer PII to Planview shall not be considered a “Sale” or “Sharing.”

To the extent required by the California Privacy Laws, Planview shall (a) provide the same level of privacy protection as is required by the California Privacy Laws; (b) grant Customer the right to take reasonable and appropriate steps to help ensure that Planview uses Customer PII in a manner consistent with Customer's obligations under the California Privacy Laws; (c) notify Customer if Planview determines that it can no longer meet its obligations under the California Privacy Laws; and (d) grant Customer the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer PII.

As a Service Provider, Planview shall not (w) Sell or Share Customer PII; (x) retain, use, or disclose Customer PII for any purpose other than for the "Business Purpose", including retaining, using, or disclosing Customer PII for a commercial purpose other than those Business Purposes, or as otherwise permitted by the CPRA; (y) retain, use, or disclose Customer PII outside of the direct business relationship between Planview and Customer; or (z) combine Customer PII that Planview receives from, or on behalf of, Customer with PII that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Planview may combine PII to perform any Business Purpose as defined in the regulations adopted pursuant to paragraph (10) of subdivision (a) of Cal. Civ. Code § 1798.185, except as provided for in paragraph (6) of subdivision (e) of Cal. Civ. Code § 1798.140 and in regulations adopted by the California Privacy Protection Agency.

10. Other U.S. Data Protection Laws
To the extent that Planview processes any Customer PII relating to individuals who are "Consumers" as that term is defined in the Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 et seq., the Connecticut Data Privacy Act, Public Act No. 22-15, the Utah Consumer Privacy Act, Utah Code Ann. §§ 13-61-101 et seq., and the Virginia Consumer Data Protection Act, Va. Code Ann. §§59.1-575 et seq. (collectively, the "Consumer Privacy Laws"), respectively, and upon the respective effective date of the applicable Consumer Privacy Law, Planview shall comply with the Consumer Privacy Laws' requirements.

11. Sub-Processors
Planview may engage Planview Affiliates and/or third-party service providers (collectively, the "Sub-processors"), which are dispersed globally, to carry out specific processing activities on behalf of Customer and in connection with the Services.

Customer grants Planview a general authorization to engage Sub-processors for the execution of specific tasks in connection with the Services, subject to the following conditions: (i) a contractual agreement shall be entered into between Planview and the Sub-processor, whereby the latter is bound to the same data protection requirements as Planview is subject to with regard to PII under this DPA and any applicable legislation; and (ii) Planview may add and/or replace existing Sub-processors with new Sub-processors providing equivalent services and guarantees in terms of the ToMs implemented to protect the PII, when (a) Planview informs Customer of such change with appropriate notice by announcing it at least thirty (30) days in advance on the Planview Status website, to which Customer hereby commits to subscribing to for updates; and (b) the change is not made solely for Planview's convenience, but for the necessity of improving or provisioning the Services unmodified.

Customer may reasonably object to the replacement or addition of Sub-processors for reasons related to Customer's or Planview's compliance with Applicable Privacy Laws, by sending written notice of such objection to privacy@planview.com within thirty (30) days after receiving notice of the change. Upon receipt of a valid objection, the parties will work together in good faith to find a commercially reasonable solution, such as providing the Services without the use of the objected-to Sub-processor. If no such solution is feasible, then Customer may terminate, without penalty, the applicable Order Form(s) and/or Statement(s) of Work solely with respect to the Services that cannot be provided without the use of the objected-to Sub-processor.

For the purposes of the general prior authorization granted above, Planview's authorized Sub-processors at any given time are listed on Planview's Trust website. Planview is fully liable to Customer for the performance of the Sub-processors' processing activities related to Customer Data, including PII.

12. Planview Obligations

12.1 Confidentiality. Planview entrusts only such employees and contractors who have been bound to confidentiality obligations and have previously been familiarized with the privacy and data protection provisions relevant to their work, to process Customer PII.

12.2 Assistance and Information. Upon a clear written request by Customer sent by email to privacy@planview.com, and taking into account the nature of the processing and the information at its disposal, Planview shall cooperate with and assist Customer in demonstrating and ensuring the latter's compliance with its privacy and data protection obligations. In particular, Planview shall assist Customer in (i) meeting the obligation to ensure the security of the processing, by maintaining and updating (as necessary) its own ToMs to guarantee a data protection level appropriate to the risk of the Customer PII; (ii) meeting Customer's obligation to notify data breaches to the supervisory authorities and data subjects, as detailed in section 15 of this DPA; and (iii) carrying out data protection impact assessments (DPIA) and consulting the supervisory authority, when legally required, by providing adequate information about the processing of PII in connection with the Services.

12.3 Government Disclosure**.** Planview will notify Customer of any request for the disclosure of Customer PII by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority), unless otherwise prohibited by law or a legally binding order of such body or agency. In case Planview is prohibited by law from providing such notification, Planview will use commercially reasonable efforts to obtain a waiver of the prohibition to enable such communication. In case Planview does not consider the disclosure request to be legally binding, Planview will not disclose any Customer Data unless otherwise instructed by Customer.

In any case, if Customer wishes for Planview to notify any data subject directly of (i) any request for the disclosure of Customer PII by a governmental or regulatory body or law enforcement authority, or (ii) any direct access to Customer PII by public authorities; then Customer must expressly and clearly instruct Planview to do so in writing by sending an email to privacy@planview,com.

13. Data Transfer Scenarios and Applicable Transfer Mechanisms
Customer is aware and understands that the global nature of the Services may require international transfers of Customer PII, and the parties agree to adopt appropriate measures to ensure compliance with the international data transfer requirements under Applicable Privacy Laws. This section 13 shall govern the relevant data transfer scenarios and the transfer mechanisms adopted in each of them. To the extent that the arrangement of the Services provided by Planview to Customer does not result in any of the scenarios described in this section, then the transfer mechanisms and the corresponding section shall not apply.

13.1 Data Transfers Subject to Adequacy Decisions. Customer may freely transfer PII subject to the GDPR, the UK GDPR, the Swiss FADP, and/or the DPL, to Planview or one of its Affiliates located in a third country that has been determined by the European Commission, the UK Secretary of State, the Swiss Federal Council, and/or the DIFC Commissioner of Data Protection, as applicable, to offer an adequate level of data protection, including, but not limited to, the United States of America under the EU-U.S. Data Privacy Framework (DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, or any successor framework, certification, adequacy decision, or other lawful transfer mechanism that may be adopted in the future to replace or supplement the DPF.

13.2 Data Transfers Subject to the GDPR. Where Customer transfers PII subject to the GDPR to Planview or one of its Affiliates located in a country that does not ensure an adequate level of data protection under the GDPR, parties shall adopt the standard contractual clauses set out in the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries (hereinafter "EU Model Clauses") as a transfer mechanism. Where adopted between the parties, the EU Model Clauses shall follow Model Two (Controller to Processor) or (if applicable) Model Three (Processor to Processor) in the terms established herein by Annex 1, clause 1.

13.3 Data Transfers Subject to the Swiss FADP. Where Customer transfers PII subject to the Swiss FADP to Planview or any of its Affiliates located in a country that does not ensure an adequate level of data protection under the Applicable Privacy Law, the parties shall adopt the EU Model Clauses as established in Annex 1, clause 2 as a transfer mechanism.

13.4 Data Transfers Subject to the UK GDPR**.** Where Customer transfers PII subject to the UK GDPR to Planview or any of its Affiliates located in a country that does not ensure an adequate level of data protection under the Applicable Privacy Law, the parties shall adopt the EU Model Clauses, supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under Section 119A(1) Data Protection Act 2018, as updated, amended, replaced, or superseded from time to time by the UK Government (the "UK IDTA"), as established in Annex 1, clause 3 as a transfer mechanism.

13.5 Data Transfers Subject to the DIFC DPL. Where Customer transfers PII subject to the DPL to Planview or any of its Affiliates located in a country that does not ensure an adequate level of data protection under the Applicable Privacy Law, the parties shall adopt the EU Model Clauses, supplemented by the UK IDTA where applicable, as established in Annex 1, clause 4, as a transfer mechanism.

13.6 Onward Data Transfers to Sub-processors**.** Where, for the purposes of section 11 of this DPA, Planview transfers Customer PII to a Sub-processor located in a country that does not ensure an adequate level of data protection under the Applicable Privacy Law, Planview shall enter into the EU Model Clauses in Module Three (Processor to Processor), supplemented by the UK IDTA and/or with the necessary adaptations pursuant to the Swiss FADP or the DPL, as applicable, with the Sub-processors that access or otherwise process Customer PII outside of the EEA, UK, Switzerland, and/or DIFC, as the case may be. Notwithstanding the foregoing, Planview and the Sub-processor may alternatively implement any other valid data transfer mechanism recognized under Applicable Privacy Laws, provided such mechanism ensures a level of protection for Customer PII that is at least equivalent to that afforded by the EU Model Clauses.

14. Privacy Contact

Planview has designated a Data Privacy Officer (DPO) authorized to ensure compliance with Applicable Privacy Laws, and to respond to inquiries concerning Planview’s processing of PII. Planview’s DPO can be contacted at privacy@planview.com.

15. Data Breaches

Planview will notify Customer without undue delay after becoming aware of a data breach that may jeopardize the confidentiality, availability, and/or integrity of Customer Data and/or the protection of PII. Planview will collaborate with Customer and fulfil all reasonable requests by Customer for information or updates, as long as it does not interfere with Planview’s own work of investigating and limiting the effects of the breach. Planview will reply to questions Customer may have without undue delay to the extent possible and as frequently and reasonably necessary until the breach has been rectified.

16. Supervisory Powers of Customer

Planview undertakes to provide Customer with the legally required information about the processing of PII to demonstrate Planview's compliance with its data protection obligations and, in particular, to demonstrate the execution of the ToMs, upon Customer’s written request. Evidence of such measures, which concern not only Customer PII but also, more generally, Customer Data, may be provided by a suitable certification or report issued by an independent third-party IT-security or data-protection auditing body. Customer shall utilize Planview’s external assessment certificates and/or reports (ISO 27001, 27701 and/or SOC2 Type 2) for auditing, inspection, and questionnaire purposes. If questions remain or additional clarification is needed, then the parties will determine a mutually agreeable procedure for review of any outstanding items, such as additional inspections, which may be carried out by an external auditor (under the condition such auditor is bound by a non-disclosure agreement), to be designated in each individual case upon thirty (30) days’ written notice to Planview (unless a shorter period is required to meet a legal requirement or request by a supervisory authority or government authority), and shall be conducted in a manner that minimizes any disruption of Planview’s provision of the Services and other normal business operations.

If Customer requires Planview to respond to privacy and security questionnaires or assessments that are not capable of being readily completed by referencing existing Planview policies and procedures, or the summary assessment results referenced herein, then Planview will have the right to charge Customer for the time of its personnel in connection therewith.

17. Termination

When the processing activities end, Planview shall terminate Customer’s Subscription Services account in the Planview Product(s) and delete any access to the system by Customer and Users. If applicable, at the choice of Customer, Planview will return or destroy all Customer Data related to the Services that have come into its possession, including PII, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant, and discarded material. All Customer Data is deleted as soon as practicable after contract termination or expiry, notwithstanding Planview’s retention of backup copies of Customer Data for a limited period pursuant to section 4 of this DPA, and unless any applicable law to which Planview is subject requires the storage of such data (including PII). Written assurance of deletion or destruction of any Customer Data will be provided if Customer makes a written request therefor to Planview’s DPO.

18. Miscellaneous

This DPA is governed by the law that governs the SSA and any dispute between the parties is to be handled as set out in the SSA.

Customer may terminate this DPA and/or the SSA, in the event: (i) Planview is in substantial breach of any representations or warranties given by it under this DPA and fails to cure such breach with ninety (90) days’ after receipt of notice from Customer; or (ii) a supervisory authority or other regulatory authority or other tribunal or court finds that there has been a breach of any relevant laws in that jurisdiction by virtue of Planview’s or Customer’s processing of the PII.

ANNEX 1

Standard Contractual Clauses Terms

1. EU Model Clauses

For the purpose of section 13.2 of this DPA, the parties agree that the EU Model Clauses, Module Two (Controller to Processor) and Module Three (Processor to Processor) shall be incorporated herein by reference. Customer is the data exporter and Planview is the data importer, and the parties agree to the following:

1.1 Docking Clause

The option under clause 7 of the EU Model Clauses shall not apply.

1.2 Documentation and Compliance

The parties agree that the documentation and compliance requirements described in clause 8.9 of the EU Model Clauses shall be carried out in accordance with section 16 of this DPA.

1.3 General Authorization for Use of Sub-processors

For the purpose of clause 9 of the EU Model Clauses, Option 2 shall apply. For the purpose of clause 9 (a) of the EU Model Clauses, Planview has general authorization to engage Sub-processors in accordance with section 11 of this DPA. Planview lists the Sub-processors on Planview's Trust website and any intended change or addition to the list will be communicated to Customer at least thirty (30) days in advance. Where Module 3 (Processor to Processor) of the EU Model Clauses is applicable between Customer and Planview, pursuant to the first paragraph of section 1 of this DPA, Customer hereby warrants that it has obtained the Controller's general authorization for Planview's engagement of Sub-processors in accordance with section 11 of this DPA, and further commits to specifically informing the Controller in writing of any changes or additions to Planview's list of authorized Sub-processors of which Customer is notified, at least within twenty (20) days after receiving Planview's notification, as described in clause 1.4 of this Annex.

Where Planview enters into EU Model Clauses, Module 3 (Processor to Processor) with its Sub-processors, Customer grants Planview authority to provide general authorization on Customer's behalf for the engagement of Sub-processors by Sub-processors previously engaged in the provision of the Services, and also approval authority for the addition or replacement of any of such Sub-processors.

1.4 New Sub-processor Notification and Objection Right

For the purpose of clause 9(a) of the EU Model Clauses, Customer agrees that notices of additions or changes to Planview's Sub-processors will be announced on the Planview Status website, to which Customer commits to subscribing to for updates as established in section 11 of this DPA. Both parties agree that objections to the replacement or addition of Sub-processors shall also be governed by section 11 of this DPA.

1.5 Redress

The option under clause 11 of the EU Model Clauses shall not apply.

1.6 Supervision

For the purpose of clause 13 of the EU Model Clauses, where Customer is not established in an EU member state, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR, and in the instance that at least one of the data subjects whose personal data is transferred under this DPA are located in Sweden, then the Swedish Authority for Privacy Protection (IMY) shall be the authority indicated in Annex I.C.

1.7 Governing Law

For the purposes of clause 17 of the EU Model Clauses, Option 1 shall apply, and the governing law shall be the laws of Sweden.

1.8 Choice of Forum and Jurisdiction

The parties agree that, for the purposes of clause 18 of the EU Model Clauses, the applicable courts shall be the courts of Sweden.

1.9 Description of the Transfer and Technical and Organizational Measures

The information described in Annex 2 and 3 of this DPA shall be incorporated into Annex I and II of the EU Model Clauses, respectively.

2 Swiss Law

For the purpose of section 13.3 of this DPA, the parties agree that the EU Model Clauses, Module Two (Controller to Processor) and Model Three (Processor to Processor) shall apply in the terms established in clause 1 of this Annex 1 with the necessary adaptations described in the following clauses. Customer shall be the data exporter and Planview the data importer, and the parties agree to the following adaptations:

2.1 Supervision

For the purpose of clause 13 of the EU Model Clauses and insofar as the data transfer is governed by the Swiss FADP, the Swiss Federal Data Protection and Information Commissioner shall be the authority indicated in Annex I.C.

2.2 Applicable Law for Contractual Claims

For the purpose of clause 17 of the EU Model Clauses, the laws of Sweden shall apply.

2.3 Place of Jurisdiction for Actions Between the Parties

Pursuant to clause 18 (b) of the EU Model Clauses, Sweden shall be the place of jurisdiction for actions between the parties.

2.4 Place of Jurisdiction for Actions Brought by Data Subjects

The term 'member state' shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18 (c) of the EU Model Clauses.

3 UK Law

For the purpose of section 13.4 of this DPA, the parties agree that the EU Model Clauses, as supplemented by the UK IDTA, shall be incorporated herein by reference. Customer shall be the data exporter and Planview the data importer, and the parties agree to the following adaptations:

Part 1*Table 1*

(i) The Start Date is the date on the applicable Order Form and/or Statement of Work.
(ii) The Exporter is Customer, as established in Section 1 of Annex 2. The Importer is Planview, as established in Section 1 of Annex 2.
(iii) The Exporter's Key Contact is the one established in Section 1 of Annex 2.
(iv) The Importer's Key Contact is Cajsa Weibring, Associate General Counsel EMEA, APAC & DPO, privacy@planview.com.
(v) The Signatures are as established in the SSA.

3.2 *Table 2*

The parties choose the EU Model Clauses, including the Appendix Information and with only the following modules, clauses or optional provisions of the EU Model Clauses brought into effect for the purposes of this IDTA:

(i) Module in operation – Two and Three
(ii) Clause 7 – See Section 1.1 above.
(iii) Clause 9 – See Section 1.3 above.
(iv) Clause 11 – See Section 1.5 above.

3.3 *Table 3*

(i) Annex 1A: See Annex 2.

(ii) Annex 1B: See Annex 2.
(iii) Annex II: See Annex 3.
(iv) Annex III: N/A.

3.4 *Table 4*
The Importer and Exporter may end this IDTA.

Part 2
Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

4 DIFC Law

As set out in section 13.5 of this DPA regarding transfers of Personal Data to a Third Country that is not yet considered adequate by the DIFC Commissioner of Data Protection, the standard contractual clauses (SCCs) available at the link selected below are deemed to be appended to this DPA and binding on the parties in order to comply with Article 27 of the DPL. Customer shall be the data exporter and Planview the data importer, and the parties agree to the following adaptations:

4.1 Applicable Standard Contractual Clauses
☐ DIFC SCCs
☒ EU Model Clauses – Selected modules as agreed by the parties in section 1 above.
☒ UK SCCs / UK IDTA – Appropriate selections and/or UK IDTA completed as set out in section 3 above.
☐ Other SCCs (to be provided by Exporter or Importer).

4.2 Parties' Representatives
(i) The Data Exporter's representative is the one established in section 1 of Annex 2. No other information is necessary in order for the contract to be binding and the signature is as established in the SSA.
(ii) The Data Importer's representative is Cajsa Weibring, Associate General Counsel EMEA, APAC & DPO, privacy@planview.com. No other information is necessary in order for the contract to be binding and the signature is as established in the SSA.

4.3 Annexes
(i) Annex 1 – See Annex 2.
(ii) Annex 2 – See Annex 3.
(iii) Annex 3 – N/A.

5 Conflict

The EU Model Clauses shall be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the EU Model Clauses, the EU Model Clauses shall prevail.

ANNEX 2

Description of the Transfer

1. List of parties

Data exporter(s):

Name: Customer, as established in the SSA

Address: As established in the SSA

Contact person's name, position, and contact details: the contact details associated with Customer's Planview account or as otherwise specified in the SSA

Activities relevant to the data transferred under these Clauses: Contracting the Services as further defined in the SSA

Signature and date: as established in the SSA

Role (controller/processor): Controller (Module Two) and/or Processor (Module Three)

Data importer(s):

Name: Planview entity established in the SSA

Address: As established in the SSA

Contact person's name, position, and contact details: Cajsa Weibring, Associate General Counsel EMEA, APAC & Data Privacy Officer, privacy@planview.com

Activities relevant to the data transferred under these Clauses: Execution of the Services

Signature and date: As established in the SSA

Role (controller/processor): Processor

2. Categories of data subjects whose personal data is transferred:
Employees of Customer, Users (as defined in the SSA), authorized consultants and other agents, or other persons mentioned in the Services, as further described in the SSA and in this DPA.

3. Categories of personal data transferred:
(i) contact details (e.g. name, professional address, professional e-mail address, professional telephone number, login data, and local time zone information); (ii) employment details (e.g. company name, job title, grade/position, department, demographic data, and location data); (iii) project and portfolio-related information (e.g., skills, cost rates, time and expenses recorded, tasks and projects assigned, and resource capability and availability); (iv) IT and device systems information and traffic data (which may include user ID, IP address, and software usage pattern tracking information, such as data derived from cookies); (v) data subject's e-mail content and transmission data, which is available on an incidental basis for the provision of Support Services and/or Professional Services; (vi) any PII supplied by Users to the Services.

4. 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:
N/A

5. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):
On a continuous basis when the Services are used.

6. Nature of the processing:
(i) collecting, storing, and using PII for the identification of Users; (ii) collecting, hosting, and storing Customer Data and project-related information, including PII; (iii) accessing or consulting Customer Data, including PII, for the provision of Support Services and/or Professional Services; (iv) recording, storing, and examining activities in information systems that process or access Customer Data for security and integrity operations (as further described in Annex 3); and, (v) collecting and using Customer Data and project-related information to provide in-app AI and data fabric features and to ensure outputs meet Planview standards for consistency and quality.

7. Purpose(s) of the data transfer and further processing:
To execute and fulfill the commitments of the SSA with Customer.

8. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
For the duration of the provision of the Services, plus the additional Customer Data retrieval period as described in the SSA. Planview may retain backup copies of Customer Data, including PII, for a limited period after the termination or expiry of the provision of the Services, in accordance with its data retention policies, provided such copies remain under the protection of this DPA and are not accessed or processed for any purpose other than backup storage for disaster recovery.

9. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
To execute and fulfill the commitments of the SSA, for the duration of the provision of the Services. Detailed information on the different processing activities subject to the transfers, including their subject matter and nature, are specified on Planview's Trust website of Sub-processors.

ANNEX 3

Technical and Organizational Measures

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

Planview shall maintain administrative, physical, and technical safeguards for protection of the security, confidentiality, availability, and integrity of Customer Data, including PII (collectively, the “**Security Measures**“).

1. Security Management

Planview will maintain an effective security management program subject to executive review, support, and accountability of related policies and practices, comprising:

(i) A written information security policy that complies with applicable laws and regulations, meets or exceeds applicable industry standards, and that, at a minimum, includes defined information security roles and responsibilities and a formal and effective risk management program;

(ii) Completion of risk assessments of all systems processing Customer Data;

(iii) Completion of internal audits to measure the effectiveness of controls;

(iv) Review of security incidents, including effective determination of root cause and corrective action;

(v) A formal controls framework based on an external standard, such as SOC 2, ISO 27001, or other relevant frameworks; and

(vi) A process to document non-compliance with the Security Measures and to identify and quantify the risks and mitigation plans. The mitigation plan must be approved by the Planview Chief Information Officer (CIO), the Planview Chief Information Security Officer (CISO), or authorized Planview employee who can accept responsibility and accountability on behalf of Planview.

2. Facilities

Planview will ensure that its third-party data center service providers’ facilities that store or process Customer Data have sufficient measures in place to:

(i) Protect from unauthorized physical access, damage, and interference using physical security controls that can include, but are not limited to, card key access, redundant power, redundant infrastructure, and solid wall construction for all exterior walls;

(ii) Limit and screen all entries and exits employing measures that can include, but are not limited to, on-site security guards, badge readers, electronic locks, and monitored closed circuit television (CCTV); and

(iii) Ensure systems processing Customer Data are physically isolated from service areas that provide access points into and out of the premises.

3. Employee Access, Screening and Controls

Planview will have and maintain policies and practices that include, at a minimum, the following controls and safeguards applied to Planview employees and contractors (collectively, “Planview Representatives”):

(i) Pursuant to applicable law, and subject to *Planview’s Applicant Screening and Assessment Policy*, Planview will conduct appropriate background checks on all Planview Representatives who may have access to Customer Data and withhold access to Customer Data to any Planview Representative who has failed to pass such background investigation;

(ii) Access to data is governed by Planview’s *Access Control Standard*. Controls are implemented to ensure that access granted to all Planview Representatives is based on least-privilege principles and that only those Planview Representatives with an actual need-to-know will have access to Customer Data including, but not limited to, the use of a formal access management process for requesting, reviewing, approving, provisioning, and revocation of such access;

(iii) All Planview Representatives with access to Customer Data will undergo adequate training in the care, protection, and handling of Customer Data;

(iv) Planview will maintain a disciplinary policy and process to be enforced when Planview Representatives violate any Planview security or privacy policy or access Customer Data without prior authorization;

(v) Access to Planview source code must be limited and controlled to only permit access to authorized Planview Representatives; and

(vi) A separation of duties process will be followed to prevent a single Planview Representative from controlling all key aspects of a critical transaction or business process related to Customer Data or systems.

4. Authentication and Access Management

Planview will provide strong authentication and access control methods to protect Customer Data including, but not limited to, (i) complex passwords at least eight characters long; (ii) maximum 90-day password lifetime; (iii) unique named user IDs; (iv) session time out configuration, and/or (v) multi-factor authentication.

5. Change Management

Operating procedures must be documented and managed by a change control process. Planview will have and maintain written policies and procedures to review, test, and approve (as appropriate) changes affecting Planview infrastructure and systems that process Customer Data. Acceptance criteria for new information systems, upgrades, and new versions must be established, and suitable tests of the system(s) carried out during development and prior to acceptance.

6. Business Continuity and Disaster Recovery

Planview must have and maintain written business continuity and disaster recovery plans, which are tested/reviewed annually at a minimum.

7. Secure Data Deletion

Planview will maintain a process for secure destruction and deletion of Customer Data to ensure deleted Customer Data cannot be practicably read or reconstructed.

8. Vulnerability Management

Planview will have and maintain the following vulnerability management processes for all devices used to connect to the Planview network and services:

(i) Configuration Scanning and Remediation: Planview will align to industry best practices for build out, minimization of services, and secure configuration for Planview applications;

(ii) Vulnerability Scanning and Remediation: Planview will implement a scanning and management system to scan Planview’s network, systems, and applications for vulnerabilities; Planview will regularly scan for vulnerabilities and remediate detected vulnerabilities for components in production environments;

(iii) Secure Coding: Planview must adhere to security development best practices for development and testing for all code, APIs, and applications deployed and implemented in support of Services including, but not limited to, security testing or scanning for purchased or contracted code for use in the Services; and

(iv) Identifying Malicious Threats: Planview will have and maintain solutions to identify and prevent malicious attackers or code from accessing or compromising Customer Data or systems that process Customer Data.

Exceptions to vulnerability management controls must be documented and mitigated based on defined business process controls.

9. Security Incident Response

Planview will:

(i) Maintain a security incident response plan, procedures, and means to respond in a manner consistent with industry standards.

(ii) Notify Customer without undue delay once Planview confirms any known data incident or malicious incursion involving Customer Data or Services utilized by Customer;

(iii) Cooperate with Customer in investigating and remediating the data incident and mitigating any further risk to Customer Data, or risk to data subjects, as long as such cooperation does not interfere with Planview’s own investigation and remediation of the incident;

(iv) Provide assistance to Customer including, as applicable, making available to Customer relevant records, logs, files, data reporting, and other materials required to comply with applicable law or regulation as reasonably required by Customer, subject to third-party confidentiality restrictions, at Planview’s sole cost and expense; and

(v) Preserve evidence where possible and cooperate with Customer and legal authorities as applicable during the investigation of the incident or legal subpoena pertaining to Customer Data, including accessibility of information for legal cases, preservation, availability, and monitoring.

10. Security Reviews

Planview will undertake regular reviews of its Security Measures to ensure they remain effective and appropriate for protecting Customer Data, and in compliance with applicable industry standards, laws, and regulations. Risks detected in regular reviews will be mitigated by Planview in a timely manner.

When implementing, reviewing, and updating its Security Measures and policies, Planview will consider:

(i) Information available from the Planview’s existing vulnerability, remediation, audits, or incident related activities;
(ii) The changing nature of threats, exploits, and actual incidents relating to compromise of information hosted on connected computing platforms;
(iii) The confidential nature of Customer Data and potential harm which could result from accidental, unauthorized, or unlawful processing, loss, access, or damage to, or destruction of, such information;
(iv) Available and emerging means of detecting malicious activities and rendering them less effective or ineffective; and
(v) The state of technological development and the cost of implementing such measures.

11. Encryption

Planview has and will maintain: (i) established methods to encrypt Customer Data in transit and at rest; and (ii) established methods to securely store passwords following industry standard practices.

12. Media Transfer

Where physical media transfer is permitted, Planview must transport physical media containing PII in sealed containers with documented chain of custody.

13. Network and Systems Security

(i) Network segments connected to the internet must be protected by firewalls configured to protect all devices behind it and properly address known security concerns according to industry best practices; firewalls must deny all network traffic other than traffic permitted for business functionality;
(ii) Planview must maintain the ability to reasonably detect a potential hostile attack;
(iii) Planview must have defined means of securing and maintaining the confidentiality, integrity, and availability of system builds for computers and network devices on the network;
(iv) Development and production environments must be separated to reduce the risks of unauthorized access or changes to the operational system;
(v) Validation checks must be incorporated into applications to detect corruption of information through processing errors or deliberate acts; and
(vi) Planview must use a trusted and reliable external time source to synchronize internal system clocks.

14. System and Logging Capabilities

Planview will maintain hardware, software, and/or procedural mechanisms that record, examine, and alert (upon detection of a security event) activity in information systems that process or access Customer Data, including appropriate logs and automated reports. Logs must be retained to assist in investigations and access control monitoring, including, but not limited to, end user access and activities and information security events.

15. Compliance Program

Planview will maintain a compliance program that includes independent third-party audits and/or certifications, such as SOC2 Type II report, ISO 27001 certificate, or equivalent, and make available to Customer, upon written request, copies of the most up-to-date version of the third-party certifications or reports in relation to services purchased by Customer.

16. Privacy by Design

Planview will incorporate privacy by design and privacy by default principles into processes, services, and systems at the earliest state and throughout the lifecycle of the processing activities.