Data Privacy, Security and Processing Agreement ("DPA")

Customer (as defined in the Master Service Agreement/Order Form, "MSA", hereinafter referred to as the "Controller") and Planview (as defined in the MSA, hereinafter referred to as the "Processor") have agreed to the following terms and conditions regarding processing of Personal data and Personal Identifiable Information ("PII") subject to the MSA

1. Subject matter, purpose, and duration of the DPA

The Subject matter of the DPA regarding the processing of PII is the execution of the services and tasks described in the MSA by Processor and sets out to reflect the parties' agreement related to Processing of PII by Processor on behalf of Controller.

Data is loaded into Planview database as metadata for the identification and selection of resources for assignment to the work that is managed in the Service. Processing activities comprises hosting in the SaaS Service and identification of users, including offsite backup, disaster recovery redundant storage, SMTP relay, and customer support. All data including PII of users is provided by the Controller to the Service.

The undertaking of the contractually agreed Processing of PII shall be carried out in accordance with this DPA and the MSA within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA) or outside the EU/EEA, provided that the parties shall ensure compliance with the privacy regulations they are subject to and by appropriate measures. The provisions shall apply to all services of data processing provided by the Processor on behalf of the Controller, especially with regards to art. 28 of the EU 2016/679 (GDPR), and in accordance with any other privacy regulation the parties are subject to, which the Processor performs based on the MSA.

2. How this DPA Applies

This DPA is subject to the terms of, and fully incorporated and made part of, the MSA. This DPA shall replace any existing data processing addendum to the MSA unless otherwise explicitly stated herein. In the event of any conflict between this DPA and any other provision of the MSA with respect to PII, this DPA shall govern and apply.

3. Definitions

Any reference is made to further definitions set forth in Art. 4 GDPR and the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. (CCPA).

4. Scope of Processing Activities

Processor will process PII by hosting, IT System operations / maintenance, IT System service as specified in the work order / service description associated with this DPA, and store project-related information in the Service described in the MSA throughout the interface. Beginning and duration of the processing starts with the signing of this DPA and ends whenever the Controller terminates this agreement or the MSA.

5. Categories of Personal Data

The Subject Matter of the processing of PII comprise in general the following data types/categories that the Controller/users insert when using the Service: (i) contact details (e.g. name, address, e-mail address, contact details, local time zone information); (ii) employment details (e.g. company name, job title, grade, demographic and location data), (iii) IT and device systems information and traffic data (which may include user ID, IP address, and software usage pattern tracking information as cookies), (iv) data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services, (v) any personal data supplied by users of the Service.

The Controller acknowledges Processor is providing the SaaS Service whereas the Controller is providing to the Service whatever data preferred, including PII.

6. Categories of Data Subjects

The Categories of Data Subjects comprise in general

- ✓ Controller employees
- ✓ Users invited to the Service by Controller
- ✓ Authorized Agents/Contractors
- ✓ Contact Persons
- ✓ Other persons using or mentioned in the Service

7. Technical and Organizational measures (ToM's)

ToM's to be taken shall guarantee a data protection level appropriate to the risk concerning confidentiality and integrity of the Controller and users, in accordance with availability and resilience of the systems. The state of the art, 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 actions taken into account.

Processor's ToM's comprises

- ✓ ISO 27001 and 27701 certifications*
- ✓ SOC 2 reports*
- ✓ Annual Pen-tests
- ✓ Encryption
- ✓ Security and privacy e-learnings and seminars (frequently, depending on the authorization)
- ✓ Internal policies and instructions to Processor's employees (annually updated and more often if needed)
- ✓ Internal authorization for access to data, and
- ✓ Incident Management Response Plan

The ToM's are subject to constant technical progress and further development. In this respect, it is permissible for the Processor to implement alternative adequate measures. In so doing, the security of the defined measures must not be reduced. The Processor shall periodically monitor the internal processes and the ToM's to ensure that Processing within the area of responsibility is in accordance with the requirements of applicable data protection laws and privacy for the protection of the rights of the Data Subject.

8. Principles of the Processing Activities

Insofar as it is included in the scope of services, the principles related to Processing activities of PII as described in Art. 5 GDPR, or any other privacy regulation parties are subject to, must be adhered to by the Processor through the Controllers instructions. Thereby, Processor may carry out, retain, rectify, erase or restrict the Processing of PII only on documented instructions from the Controller, as described in this DPA, and/ or in accordance with the MSA, unless required to do so by European Union or member state law to which Processor is subject. In such a case, Processor shall inform Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

Processor shall immediately inform Controller if, in its opinion, an instruction infringes the GDPR or other European Union or member state data protection provisions.

Insofar as a Data Subject contacts the Processor directly to exercise its rights as a registered, Processor will immediately forward the Data Subject's request to the Controller

9. Sub-Processors

Sub-processing for the purpose of this DPA is to be understood as meaning services which relate directly to the provision of the principal service of the MSA.
Sub-processors are disposed globally. They are processing PII to provide the contracted services and identify events and activities between computers and agents (such as browsers, e.g. determining whether an action on a website is being performed by a human or a bot) or other identify patterns that may indicate malicious or fraudulent activity. Sub-processors also serve a service for security and operational information and event management system; aggregates system, infrastructure, and application log data for use in security, operational monitoring activities performed by Planview staff, and for email SMTP relay.

* *To verify to which Planview SaaS products ISO certifications and SOC 2 reports apply to, please visit www.planview.com/trust/compliance/*

The Processor may commission Sub-processors to fulfill the services of the MSA as the Processor has a general authorization to engage Sub-processors for purposes described above. The Controller agrees to the commissioning of Sub-processors under condition of a contractual agreement is entered into between the Processor and the Sub-processor, stipulating the same requirements as the Processor is subject to with regards to PII. Sub-processors are listed on Planview's Customer Success Center website. Notices of changes of sub-processors will be announced at least 30 days in advance on the Planview Status website which can be subscribed to for updates.

Processor is furthermore entitled to change existing Sub-processor with a new Sub-processor providing equivalent services when 1) Processor informs Controller of such outsourcing with appropriate advance notice; 2) The sub-processing is based on a contractual agreement, and 3) The change is not made solely for Processors convenience, but for the necessity of provisioning the services unmodified. Controller may refuse an exchange or addition of Subprocessor in its absolute discretion resulting in the termination of processing activities, and dissolvement of the DPA and MSA.

Processor is fully liable to the Controller for the performance of the Sub-processors processing activities related to the Controllers PII.

10. Quality Assurance and other duties of the Processor

10.1 Confidentiality – The Processor entrusts only such employees with the Processing activities outlined in this DPA who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Processor and any person acting under its authority who has access to PII, shall only process PII by specific instructions from the Controller, which includes the powers granted in this DPA, unless required to do so by law.

10.2 Assistance and information – The Processor shall cooperate, on request, with the Controller to demonstrate and ensure compliance with a supervisory authority or Data Subjects in performance of its legally obliged tasks.

10.3 Government Disclosure - Processor will notify the Controller of any request for the disclosure of Controller Personal Data 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 Processor is prohibited by law from providing such notification, Processor shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable such communication. In case Processor does not consider the disclosure request to be legally binding, Processor shall not disclose any Controller data unless otherwise instructed by the Controller.

11. Data transfer scenarios and applicable transfer mechanisms

11.1 Data transfers subject to the GDPR

Where the Controller transfers PII subject to the GDPR to Processor or one of its affiliates located in a country which does not ensure an adequate level of data protection under the GDPR, parties shall adopt the Model 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) in the terms established herein by Annex 1, clause 1.

11.2 Onward data transfers to Sub-processors

Where, for the purposes of clause 9 of this DPA, Processor transfers Controller PII to a sub-processor located in a country which does not ensure an adequate level of data protection under the applicable privacy and data protection law, Processor shall enter into the EU Model Clauses in Module Three (Processor to Processor) with the Sub-processors that access or otherwise process Controller PII outside of the EEA.

11.3 Data transfers subject to the Switzerland data protection law

Where Controller transfers PII exclusively subject to Switzerland privacy and data protection law to Processor or any of its affiliates located in a country which does not ensure an adequate level of data protection under the applicable law, parties shall adopt Model Clauses as established in Annex 1, clause 2 as a transfer mechanism.

11.4 Data transfers subject to the UK GDPR

Where Controller transfers PII subject to the UK GDPR to Processor or any of its affiliates located in a country which does not ensure an adequate level of data protection under the applicable privacy and data protection law, parties shall adopt Model Clauses as established in Annex 1, clause 3 as a transfer mechanism.

12. Privacy Contact

Processor has designated a Data Privacy Officer (DPO) authorized to respond to inquiries concerning Processing of PII and shall reasonably cooperate with Controller concerning all such inquiries if so requested. DPO can be contacted at privacy@planview.com

13. Data Breaches

Processor will notify Controller without undue delay after becoming aware of a data breach that may jeopardize the risk of confidentiality of Controllers data and/or protection of PII Data Subjects. Processor will collaborate with Controller and fulfil all reasonable requests by Controller for updates, as long as it is not interfering with Processors own work of investigating and limiting the effects of the breach. Processor will reply to questions Controller may have without undue delay to the extent possible and as frequently and reasonably necessary until the breach has been rectified.

14. Supervisory powers of the Controller

Controller shall ensure that the Processor is able to verify compliance with the obligations its subject to. The Processor undertakes to give the Controller necessary information on request and, in particular, to demonstrate the execution of the ToM's. Evidence of such measures, which concern not only the specific DPA, may be provided by a suitable certification by IT-security or data protection auditing body. Controller shall utilize Processors external assessment reports (ISO 27001, 27701 and SOC2 Type 2) for auditing, inspection and questionnaire purposes. If questions remain or additional clarification is needed, Processor and Controller will determine a mutually agreeable venue for review of any outstanding items, such as additional inspections, or to have them carried out by an 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 Processor (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 Processors provision of the Services and other normal operations.

The Processor may claim remuneration for enabling Controller audits, inspections and questionnaires if Controller requires additional documentation not reasonably motivated due to Processors normal Processing activities.

15. Termination

When the Processing activities ends, Processor shall terminate the Controllers Service account and delete any access to the system by Controller and users, and if applicable, at the choice of the Controller, return or destroy all documents, processing and utilization results, and data sets related to the MSA that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. All Controller data is deleted at the earliest convenience after contract termination if Controller don't specify a specific time frame. Written assurance of deletion or destruction of any Controller information will be provided by request to DPO.

16. Miscellaneous

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

Controller may terminate this DPA and/or the Agreement, in the event: 1) Processor 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' following receipt of notice from Controller; 2) Processor provides notice to Client pursuant to Section 9(4) of Sub-processors of this DPA; or 3) 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 Processor's or Controller's processing of the PII.

Notwithstanding the amendment made herein, the parties confirm that all other terms and conditions of the MSA remains as stated there and are in full force and effect.

AOB

Planview’s processing of PII for the purpose of Planview’s own administration and facilitation of the SaaS comprises

- ✓ Key Contract Data (Contractual/Legal Relationships, Contractual or Service Interest, for identification and service development)
- ✓ Customer History (for internal CRM system)
- ✓ Contract Billing and Payments Data (for internal CRM system)
- ✓ Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories, for internal CRM system)
- ✓ User behavioral data (for measuring the use of the service and support)
- ✓ User performance data (for measuring the use of service to tailor better features and support)

Planview is a Controller for these processing activities. Planview is processing the data for legal obligations or legitimate interest. Processing activities comprises third party disclosure to Processors as stated in clause 9. Additional information regarding Planview’s processing of PII can be found in the Privacy Statement on the Planview website.

PLANVIEW WILL NOT SELL PII TO ANY OTHER PARTY. NEITHER WILL PLANVIEW RETAIN, USE OR DISCLOSE PII FOR ANY PURPOSE OTHER THAN FOR THE SPECIFIC PURPOSE OF PERFORMING THE SERVICES, INCLUDING RETAINING, USING, OR DISCLOSING PII FOR A COMMERCIAL PURPOSE OTHER THAN PROVISION OF THE SERVICES.

Planview	Customer
Signature Cajsa Weibring	Signature
Name Cajsa Weibring	Name
Title VP SR Legal Counsel & DPO	Title
Date March 16, 2022	Date

Annex 1

Standard Contractual Clauses Terms

1. EEA Model Clauses

For the purpose of clause 11.1 of this DPA, the parties agree that the model clauses resulting from 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"), Module Two (Controller to Processor) shall be incorporated herein by reference. Controller is the data exporter and Processor is the data importer, and the Parties agree to the following:

1.1 Docking clause
The option under clause 7 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 clause 14 of this DPA

1.3 General authorization for use of sub-processors
For the purpose of clause 9 EU Model Clauses, Option 2 shall apply. For the purpose of clause 9 (a) EU Model Clauses, Processor has general authorization to engage sub-processors in accordance with clause 9 of this DPA. Processor lists the sub-processors on Planview's Customer Success Center website and any intended change to the list will be communicated to Controller at least 30 days in advance. Where Processor enters into EU Model Clauses, Module 3 (Processor to Processor) with its sub-processors, Controller grants Processor authority to provide general authorization on Controller's behalf for the engagement of sub-processors by sub-processors previously engaged in the provision of the service 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) EU Model Clauses, Customer agrees that notices of changes of sub-processors will be announced on the Planview Status website which can be subscribed to for updates as established in clause 9 of this DPA. Both parties agree that objections to an exchange or addition of sub-processor shall also be governed by clause 9 of this DPA.

1.5 Supervision
For the purpose of clause 13 EU Model Clauses, the Swedish Authority for Privacy Protection (IMY) shall be the authority indicated in Annex I.C.

1.6 Notification of the data importer in case of access by public authorities
For the purposes of clause 15(1)(a) EU Model Clauses, Processor shall exclusively notify Controller (and not the Data Subjects) in case of government access requests. Controller shall be solely responsible for promptly notifying the Data Subject as necessary.

1.7 Governing Law
For the purposes of clause 17, 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 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 1 and 2 of the EU Model Clauses.

2. Swiss Law

For the purpose of clause 11.3 of this DPA, the parties agree that the EU Model Clauses, Module 2 (Controller to Processor) shall apply in the terms established in clause 1 of this Annex (1) with the necessary adaptations described in the following clauses. The Model Clauses shall also apply to the transfers of information relating to an identified or identifiable legal entity where such information is protected in similar terms as PII under Swiss Data Protection Law until such laws are amended to no longer cover legal entities. Controller shall be the data exporter and Processor the data importer, and the Parties agree to the following adaptations:

2.1 Supervision
For the purpose of clause 13 EU Model Clauses, 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 EU Model Clauses, Swiss law shall apply

2.3 Place of jurisdiction for actions between the parties
Pursuant to clause 18 (b), 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) EU Model Clauses.

2.5 References to the GDPR
Any reference to the GDPR shall be understood as a reference to the Swiss Federal Data Protection Act.

3. UK Law

For the purpose of clause 11.4 of this DPA, the parties agree that, the Model Clauses resulting from the EU Commission Decision C(2010)593 of 5 of February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (UK Model Clauses) shall be incorporated herein by reference. Controller shall be the data exporter and Processor the data importer, and the Parties agree to the following adaptations:

3.1 References to EU law and Member States
Any reference in the UK Model Clauses to EU Data Protection Law shall be interpreted as a reference to the GDPR as transposed into the UK national law (UK GDPR). Any reference to the EU Member States shall be interpreted as a reference to the UK.

3.2 Supervision
Any reference in the UK Model Clauses to a supervisory authority shall be interpreted as a reference to the UK Information Commissioner's Office (ICO).

3.3 Description of the transfers, and technical and organizational security measures
The information described in Annex 2 and 3 of this DPA shall be incorporated into Appendices 1 and 2 of the UK Model Clauses respectively, with the necessary adaptations.

3.4 Future Changes to the Model Clauses
If and when the UK government or the Information Commissioner approves the use of the EU Model Clauses for the purposes of the UK GDPR, the EU Model Clauses shall apply instead in the terms of Clause 1 of this Annex (1). In such case, the EU Model Clauses shall be incorporated with the necessary adaptations to comply with the UK GDPR, or any recommendation issued by the ICO. The supervisory authority shall be the ICO, and the governing law England & Wales.

4. Conflict

The 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 Model Clauses, the Model Clauses shall prevail.

Annex 2

Description of the Transfer

1. 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 EU*]

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

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]

Name: Planview International AB

Address: Klarabergsgatan 60, 111 21 Stockholm, SWEDEN

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

Activities relevant to the data transferred under these Clauses: Execution of Services as further defined in the Services Agreement

Signature and date: Cajsa Weibring March 16, 2022

Role (controller/processor): Processor

2. Categories of data subjects whose personal data is transferred
Employees of the Customer, consultants and other agents as further described in the Services Agreement and related Data Processing Agreement (if any).

3. Categories of personal data transferred
(i) contact details (e.g. name, address, e-mail address, contact details, local time zone information); (ii) employment details (e.g. company name, job title, grade, demographic and location data), (iii) IT and device systems information and traffic data (which may include user ID, IP address, and software usage pattern tracking information as cookies), (iv) data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services, (v) any personal data supplied by users of the Service.

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 Service is used

6. Nature of the processing
Data is loaded into Planview database as metadata for the identification and selection of resources for assignment to the work that is managed in the Service. Processing activities comprises hosting in the SaaS Service, including offsite backup, disaster recovery redundant storage, SMTP relay, and customer support. All data including PII of users is provided by the Customer to the Service.

7. Purpose(s) of the data transfer and further processing
The purpose of processing personal data is to execute and fulfill the commitments of the Service Agreement with Customer. Processing of personal data also takes place when informing users of feature and functionality enhancements and additional marketing of functionalities and other Services of company's different products.

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 Service Agreement.

9. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
The purpose of transfer of personal data is to execute and fulfill the commitments of the Service Agreement. Detailed information the different processing activities subject to the transfers are specified on Planview's Customer Success Center website of Sub-processors https://success.planview.com/trust/Planview_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 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.

ISO 27001 certification

ISO 27701 certification[*]

*SOC 2 reports**

Annual Pen-tests

Encryption

Security and privacy e-learnings and seminars (frequently, depending on the authorization)

Internal policies and instructions to Processor's employees (annually updated and more often if needed)

Internal authorization for access to data

Incident Management Response Plan

Planview requires its sub-processors to adhere to equivalent obligations as those required from Planview's customers (where Planview is a Processor), including security and privacy specific requirements that are not only legally but also contractually required for specific reasons

Data Protection enablement

1. Confidentiality
- Hardware located in secure facilities meeting rigorous industry standards such as ISO 27001 and 27701 / SOC 2
- Access to production systems limited to authorized personnel utilizing multi-factor authentication
- Supplier uses standard encryption methods (TLS for data in transit / AES for data at rest) to ensure data safety.

2. Integrity
- Data backups performed regularly and available for restoral should corruption occur
- Write access to data strictly administered.
- Data / input validation to ensure complete, accurate data

3. Availability and Resilience

Supplier has implemented suitable measures to ensure that PII is protected from accidental destruction or loss. This is accomplished by:
- Redundant service infrastructure within data centers.
- Secure data centers that provide highest physical security, redundant power and infrastructure redundancy.

4. Procedures for regular testing, assessment and evaluation
- Third party penetration testing performed at regular intervals
- Business continuity exercises performed at regular intervals
- Protection by Design and Default
- Ongoing evaluations to identify and remediate vulnerabilities

Data Protection Impact Assessments of vendors (i.e. Sub-processors) are performed before contracting, and regularly thereafter.

[*] *To verify to which Planview SaaS products ISO certifications and SOC 2 reports apply to, please visit www.planview.com/trust/compliance/*