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 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 product. Processing activities comprises hosting in the SaaS product, 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 product.

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, and store project-related information in the product 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 product

- ✓ Personal Master Data (Key Personal Data, *for identification*)
- ✓ Contact Data (*for logging in to the system*)
- ✓ IP addresses (*for identification*)

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

6. Categories of Data Subjects

The Categories of Data Subjects comprise in general

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

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 certification,
SOC 2 reports,
Annual Pen-tests,
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 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 (i.e. additional third-party contractors) that processes parts of the services 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.

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 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; and 2) The sub-processing is based on a contractual agreement. Controller may refuse an exchange or addition of Sub-processor 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. The Controller shall be informed of any inspections and measures conducted by the supervisory authority, insofar as they relate to the MSA. This also applies if the Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding Processing of PII in connection with this DPA.

10.3 Transfers – In the event Processor transfers PII to Sub-processors outside EEA for the purpose of facilitating the Services provided, transfer must be subject to adequate transfer mechanisms, such as approved adequate level of protection by reason of its domestic law or of the EU Commission/International commitments it has entered into, or the provisions in the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2010/87/EU, "Model Processor Contract", incorporated herein by Annex 2). Processor is authorized to enter into Model Processor Contract with a third-party entity on behalf of Controller for the transfer and processing of Controllers personal data if such processing is necessary for the fulfilment of the services as described in the MSA.

Pursuant to such Model Processor Contract, Controller established in the EEA are the "data exporter," and Processor and each Sub-processor that accesses or otherwise Processes PII outside of the EEA shall be a "data importer". The Processing activities in Annex 1 to the Model Processor Contract shall be such activities as necessary for Processor to provide the product and/or Services for Customer as described in the MSA, and the security measures and ToM's in Annex 1 Model Processor Contract shall be those identified in Annex 1 of this DPA.

11. 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

12. 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.

13. 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 ITsecurity or data protection auditing body. Controller shall utilize Processors external assessment reports (ISO 27001, SOC2 Type 2) for auditing 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 Products and/or Services and other normal operations

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

14. Termination

When the Processing activities ends, Processor shall terminate the Controllers product 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 customer data is deleted at the most 30 days adjacent to the termination of a contract. Servers/backups of content are deleted after 90 days. Written assurance of deletion or destruction of any Controllers information will be provided by request to DPO.

15. 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 Product Interest, *for identification and product 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.

Annexes

Annex 1 Technical and organizational Measures (ToM's) of Security and Privacy
[Annex 2 EU (2010/87/EU) Standard Contractual Model Clauses] *If applicable*
[Annex 3 Sub-processors list applicable by date of the DPA entering into force] *On request by Controller*

Annex 1 - Technical and Organizational Measures (ToM's) of Security and Privacy

Hosting

Data Centers for hosting Controllers data are located in different areas depending on the service offered, listed on Planview's Customer Success Center website.

Data Protection enablement

1. Confidentiality
- Hardware located in secure facilities meeting rigorous industry standards such as ISO 27001 / 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.

Sub-processing as per Art. 28 GDPR may be completed by corresponding instructions from the Customer, e.g.: clear and unambiguous contractual arrangements, formalized Order Management, strict controls on the selection of vendor, duty of pre-evaluation, supervisory follow-up checks.

ANNEX 2

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name, address and contact details of the data exporting organisation: As defined in the MSA (Controller)

(the data exporter)

and

Name, address and contact details of the data importing organization: As defined in the MSA (Processor)

(the data importer)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions
For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer
The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause
1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or

have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer (1)

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(1) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability
1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless

any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (1). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

(1) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): N/A

Signature .....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Cajsa Weibring

Position: Data Privacy Officer

Address: Klarabergsgatan 60, 111 21 Stockholm, SWEDEN

Other information necessary in order for the contract to be binding (if any): N/A

Signature .....

Appendix 1
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Exporting personal data to data importer by utilizing the SaaS product as further described in the MSA

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

Providing a SaaS solution for Work and Resource Management as further described in the MSA.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

Employees of the Data Controller, consultants and other agents as further described in the MSA.

Categories of data
The personal data transferred concern the following categories of data (please specify):

Key personal data (name, address, mail and other contact data) to identify the user of the product, any other personal data that users provide to the system

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

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 product. Processing activities comprises hosting in the SaaS product. All data including personal data of users is provided by the Data Controller to the product

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: Cajsa Weibring

Authorised Signature .....

Appendix 2
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

ISO 27001 certification,
SOC 2 reports,
Annual Pen-tests
Internal policies and instructions to employees,
Internal authorization for access to data,
Security and Privacy e-learning and seminars, and
Incident Management Response Plan

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: Cajsa Weibring

Authorised Signature .....