Data Processing Agreement, “the Contract”

between

Customer (as defined in the Service Agreement) the Controller – hereinafter referred to as

the Customer –

and

Planview (as defined in the Service Agreement) the Processor – hereinafter referred to as

the Supplier

1. Subject matter and duration of the Contract

   (1) Subject matter

   The Subject matter of the Contract regarding the processing of data is the execution of the
   following services or tasks by the Supplier as the Data Processor (Definition of the services or
   tasks) as follows:

   The Customer is the Data Controller and uses Supplier’s online software solution “Enterprise One”
   as a so-called Software as a Service (SaaS). The terms for the use of Enterprise One is regulated
   under the “Service Agreement”. This Contract forms an integrated part of the Service Agreement.

   Enterprise One provides, among other things, an integrated solution for strategic planning, time
   reporting, portfolio and resource management, program management, financial planning and
   enterprise architecture.

   Customer created content may relate to personal data, e.g. by defining responsibilities, naming
   them in protocols or identifying them as creator of content etc.

   (2) Duration

   The Contract is valid during the term of the Service Agreement.

2. Specification of Contract Details

   (1) Nature and Purpose of the intended Processing of Data

   The undertaking of the contractually agreed processing of personal data shall be carried out in
   accordance with the Contract and the Service Agreement 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 Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures (e.g. Privacy Shield).

(2) Type of Data

The Subject Matter of the processing of personal data comprises the following data types/categories:

- Personal Master Data (Key Personal Data)
- Contact Data
- Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
- Customer History
- Contract Billing and Payments Data
- Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories)
- Other Personal Data that the Customer/users insert when using Enterprise One

(3) Categories of Data Subjects

The Categories of Data Subjects comprise:

- Customers
- Potential Customers
- Subscribers
- Employees
- Suppliers
- Authorised Agents
- Contact Persons
- Other persons using or mentioned in Enterprise One

3. Technical and Organisational Measures

(1) The Supplier shall establish Technical and Organisational Measures in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR as set out in Appendix 1. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, 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 within the meaning of Article 32 Paragraph 1 GDPR must be taken into account.

(2) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced.
4. **Rectification, restriction and erasure of data**

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Customer, but only on documented instructions from the Customer or in accordance with the Service Agreement.

Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject’s request to the Customer.

(2) Insofar as it is included in the scope of services, the erasure policy, ‘right to be forgotten’, rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Customer without undue delay.

5. **Quality assurance and other duties of the Supplier**

In addition to complying with the rules set out in this Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 Paragraph 2 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

- a) The Supplier is not obliged to appoint a Data Protection Officer. The Supplier shall designate a Contact Person on behalf of the Supplier.
- b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Customer, which includes the powers granted in this contract, unless required to do so by law.
- c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR and as set out in Appendix 1.
- d) The Customer and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.
- e) The Customer shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Contract. This also applies insofar as the Supplier 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 the processing of personal data in connection with the processing of this Contract.
- f) Insofar as the Customer is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Contract data processing by the Supplier, the Supplier shall make every reasonable effort to support the Customer.
- g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment.

(2) The Supplier may commission subcontractors (additional contract processors) according to this Contract or after prior written or documented consent from the Customer. The Customer agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

<table>
<thead>
<tr>
<th>Company subcontractor</th>
<th>Address/Country</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sungard</td>
<td>Woking, England UK</td>
<td>Colocation</td>
</tr>
<tr>
<td>Azure</td>
<td>London, England UK</td>
<td>Database backup Service</td>
</tr>
<tr>
<td>Neverfail</td>
<td>Manchester, England UK</td>
<td>DRaaS</td>
</tr>
<tr>
<td>Akamai</td>
<td>Massachusetts, US</td>
<td>CDN / WAF</td>
</tr>
<tr>
<td>Sumologic</td>
<td>California, US</td>
<td>Log Storage / Log Analytics</td>
</tr>
<tr>
<td>Planview GmbH</td>
<td>Gartenstraße 67, 71635 Karlsruhe, Germany</td>
<td>Customer Service Maintenance First and second level support Cloud Operations Support</td>
</tr>
<tr>
<td>Proofpoint</td>
<td>Sunnyvale, California, US</td>
<td>SMTP relay</td>
</tr>
</tbody>
</table>

Supplier is furthermore entitled to change the existing subcontractor with a new subcontractor providing equivalent services when:

- The Supplier informs the Customer of such outsourcing with appropriate advance notice; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Customer to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.
(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures.

(5) Further outsourcing by the subcontractor requires the consent of the Customer (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Customer

(1) The Customer has the right, after consultation with the Supplier and in accordance with Article 28, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Customer is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Customer the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only the specific Contract, may be provided by a suitable certification by IT security or data protection auditing body.

(4) The Supplier may claim remuneration for enabling Customer inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Customer, when applicable, in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

   a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

   b) The obligation to report a personal data breach promptly to the Customer

   c) The duty to assist the Customer with regard to the Customer’s obligation to provide information to the Data Subject concerned and to immediately provide the Customer with all relevant information in this regard.

   d) Supporting the Customer with its data protection impact assessment

   e) Supporting the Customer with regard to prior consultation of the supervisory authority

(2) The Supplier may claim compensation for support services which are not included in the Service Agreement and which are not attributable to failures on the part of the Supplier.
9. Customer instructions

(1) Instructions of the Customer are stipulated in this agreement and in the Service Agreement.

(2) The Supplier shall inform the Customer immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Customer confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Customer, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Customer, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Customer or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract 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. A certification of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Customer at the end of the contract duration to relieve the Supplier of this contractual obligation.
Appendix 1 - Technical and Organizational Measures

1. **Confidentiality (Article 32 Paragraph 1 Point b GDPR)**
   - Hardware stored in locked cages.
   - Fingerprint access and entrance and security staff, CCTV cameras.
   - Access to systems can only be done by approved personnel with the correct access rights.

2. **Integrity (Article 32 Paragraph 1 Point b GDPR)**
   - Supplier uses encryption, tls to ensure data safety.
   - Data processing system are only able to access Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied, modified or removed without authorization.
   - Data Entry Control - All handling of user data is logged and audited.

3. **Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)**
   - Supplier has implemented suitable measures to ensure that Personal Data 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 (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)**
   - Data Protection Management;
   - Incident Response Management;
   - Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
   - Order or Contract Control
     No third party data processing as per Article 28 GDPR without corresponding instructions from the Customer, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of service provider, duty of pre-evaluation, supervisory follow-up checks.