Planforge

CONTRACT

DECLARATION OF COMMITMENT FOR DATA PROCESSING

DACLARATION OF COMMITMENT FOR DATA PROCESSING ACCORDING TO GDPR ART. 28(9)

dated

March 1, 2023

ONEPOINT Projects GmbH

Dietrich-Keller-Strasse 24/6

8074 Raaba-Grambach, Austria

(referred to as „**Processor**“)

Commits to the “Controller”

(User or Customer)

as follows:

DATA PROCESSING AGREEMENT

The Processor undertakes to perform the services outlined in Annex 1 on behalf of the Controller. The purpose of this agreement is to ensure that the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679) are met in connection with the commissioning of processors by a controller. For the purpose of this agreement, the terms of the General Data Protection Regulation shall apply.

1. RIGHT TO INSTRUCTION

1.1. The Processor shall process the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

1.2. The Processor has no obligation to seek legal assistance in order to establish whether the instructions of the Controller comply with the General Data Protection Regulation or other applicable law.

1.3. Information given by the Processor to the Controller must not be considered as legal assistance under any circumstances.

1.4. Instructions from the Controller comply with the provisions of this agreement. If complying with the Controller's instructions results in an effort of more than one working hour by the Processor, the Controller shall compensate the entire effort made by the Processor.

2. CONFIDENTIALITY

2.1. The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. DATA SECURITY

3.1. The Processor undertakes all mandatory measures pursuant to Article 32 of the General Data Protection Regulation.

3.2. The Processor fulfills its obligations under Point 3.1 by implementing the security measures described in Annex 2.

4. SUB-PROCESSING

4.1. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors or sub-processor (hereinafter collectively "Sub-Processors") in written form via email to the main contact person thereby giving the Controller the opportunity to object to such changes. If the Controller does not object within a period of two weeks, the addition or replacement is considered to be accepted. In the event of an objection, the Processor may not carry out the change in question within the scope of the commissioned processing governed by this Agreement. In any case, the Controller shall grant the Processor permission to use the Sub-Processors listed in Annex 3.

4.2. Where the Processor engages another Sub-Processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this Agreement shall be imposed on that Sub-Processors by way of a written contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of applicable data protection law.

4.3. Where that Sub-Processors fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that Sub-Processors obligations.

4.4. The Processor ensures that any transfer of Personal Data to recipients in countries outside the European Economic Area shall only take place in accordance with the provisions of Chapter V of the General Data Protection Regulation.

5. ASSISTANCE

5.1. The Processor shall assist the Controller by appropriate technical and organizational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights under Chapter III of the General Data Protection Regulation, as far as this is possible.

5.2. The Processor generally fulfills its obligations under Point 5.1 by forwarding any requests from data subjects to the Controller. As far as the Controller considers any additional support by the Processor as necessary, the Processor is obliged to render this assistance in exchange for appropriate additional compensation.

5.3. Moreover, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations under applicable data protection law, including Articles 32 to 36 of the General Data Protection Regulation. The Processor fulfills those tasks by (i) undertaking the measures mentioned in Point 2 ("Confidentiality") and 3 ("Data Security")

of this agreement; (ii) notifying the Controller of a personal data breach regarding personal data that are processed by the Processor on behalf of the Controller, as far as the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons and (iii) by providing the information listed in Annex 1 of this agreement.

5.4. The notification according to Point 5.2 (ii) shall, as far as possible under the given circumstances, describe:

a. the nature of the personal data breach, if possible including the categories and the approximate number of data subjects as well as the approximate number of personal data records concerned;
b. the likely consequences of the personal data breach;
c. the measures taken or proposed by the controller to address the personal data breach.

6. RETURN OF PERSONAL DATA

6.1. The Processor shall, at the choice of the Controller, delete or return all the personal data to the Controller after the end of the provision of services relating to processing and after an appropriate time period, unless applicable Union or EU Member State law requires storage of the personal data.

7. AUDIT

7.1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this agreement.

7.2. The Processor shall allow for pre-announced inspections during business hours, conducted by the Controller or an independent third party. Such inspections shall be performed in appropriate intervals and in a manner not disturbing the business activities of the Processor. Any costs arising from such inspections shall be borne by the Controller.

7.3. The Processor may fulfill its obligations under Point 7.2 by allowing third parties to conduct audits at least every three years and by making the audit results available to the Controller.

8. MISCELLANEOUS

8.1. Any changes to this agreement shall be made in writing. This also applies to this written form requirement.

8.2. If any provision of this agreement should be invalid it shall be replaced, to the extent permitted by law, by such provision as most closely reflects the economic intent of the invalid provision.

ANNEX 1

DATA SUBJECTS

The personal data transferred concern the following categories of data subjects:

- Users of the software solution and
- Other persons that are part of project cycles (including stakeholders)

CATEGORIES OF DATA

The personal data transferred concern the following categories of data (please indicate in detail):

- Passwords and other authentication data
- Name
- Assigned role (e.g., administrator, manager)
- Responsibilities and tasks
- Schedules
- Assigned projects
- Project data (e.g. project steps, project size and status of the project)
- Resource data (e.g., availability, absences, hourly rates, activities)
- Stakeholder (yes/no) and if yes, stakeholder data (e.g., interest, activities)
- Project risk data (e.g., responsibility for a certain project risk)
- Status reports
- Meeting minutes

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE)

The personal data transferred concern the following special categories of data: N/A

SUBJECT-MATTER OF THE PROCESSING AND PROCESSING OPERATIONS

The personal data transferred will be subject to the following basic processing operations:

Providing a web-based project and portfolio management solution.

PROCESSING PURPOSES

The personal data transferred will be processed by the Processor for the following purposes of the Controller:

For an efficient use of the project and portfolio management solution provided by the Processor.

ANNEX 2

DESCRIPTION OF SECURITY MEASURES

ADMITTANCE CONTROL

The headquarter of ONEPOINT Projects in Raaba-Grambach is situated on the sixth floor of an office building. Access to the building is possible only by entering the entrance door that is equipped with a security lock and can only be opened with the respective key. Only employees and the landlord own keys. After the termination of any employment relationship keys are immediately collected. Documentation on the keys in circulation is in place.

The representative and sales offices in the US and Germany are separate companies and do not have access to customer data in general.

ENTRY CONTROL

ONEPOINT Projects' Planforge cloud application uses SSL/TLS only.

The Planforge cloud servers are protected by state of the art security measures such as for example hardware firewalls. Administrative access to any cloud servers is encrypted and is possible via the IP address of the company network of ONE POINT projects only.

The company network of ONEPOINT Projects is also protected through firewalls. Customer data are solely stored on dedicated systems that are protected through strong passwords and may only be accessed externally through encrypted connections.

ACCESS CONTROL

The Planforge cloud application has a role rights concept and is client-capable and therefore does not enable unauthorized reading, copying, alteration or deletion of data. Any security related access is protocolled.

TRANSMISSION CONTROL

In case of electronic transmission of sensitive data it is guaranteed in all conscience that no unauthorized reading, copying, alteration or deletion is possible. Transfer of customer data for analysis purposes and cloud backups are only made encrypted through HTTPS, SSH, SFTP or a safe file sharing system.

ANNEX 3

LIST OF AGREED SUB-PROCESSORS

Vollständiger Firmenname	Adresse
IBM Cloud / SoftLayer Dutch Holdings B. V.	Paul van Vlissingenstraat 16, Amsterdam 1096 BK, Netherlands