Planforge

CONTRACT

DECLARATION OF COMMITMENT FOR DATA PROCESSING

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

dated

September 1, 2023

Planforge GmbH

Dietrich-Keller-Strasse 24/6

8074 Raaba-Grambach, Austria

(referred to as „**Processor**“)

commits to the “Controller”

(referred to as 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. SUBJECT MATTER OF THE CONTRACT

1.1. The Processor shall provide the Controller with a web-based project and portfolio management solution based on the main contract. In doing so, the Processor will have access to personal data and process it solely on behalf of and in accordance with the instructions of the Controller. The scope and purpose of the data processing by the Processor shall be determined by the main contract (and its associated service description). The Controller shall be responsible for assessing the permissibility of the data processing.

1.2. The duration of this commitment shall be determined by the duration of the main contract, provided that no further obligations arise from the following provisions.

2. RIGHT TO INSTRUCTION

2.1. 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 data, unless that law prohibits such information on important grounds of public interest.

2.2. The Processor is not obliged to seek legal advice to determine whether the instructions of the Controller comply with the General Data Protection Regulation or other applicable law.

2.3. Information provided by the Processor to the Controller shall under no circumstances be considered as legal advice.

2.4. Instructions issued by the Controller shall be in accordance with the subject matter of this agreement. If the Processor incurs expenses in the amount of more than one working hour as a result of following the instructions, the entire expense shall be reimbursed by the Controller.

2.5. If the Processor is of the opinion that an instruction of the Controller violates data protection regulations, it shall notify the Controller thereof without undue delay. The Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller. The Processor may refuse to implement an instruction that is obviously unlawful.

3. CONFIDENTIALITY

3.1. The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality.

4. DATA SECURITY

4.1. The Processor shall take all mandatory measures pursuant to Article 32 of the General Data Protection Regulation. The information obtained shall not be disclosed to third parties or exposed to their access. Documents and data shall be secured against disclosure to unauthorized persons, taking into account the state of the art.

4.2. The Processor shall fulfill its obligation under point 4.1 by implementing the security measures described in Annex 2. The Processor reserves the right to change the security measures taken, while ensuring that the contractually agreed level of protection is not compromised.

5. SUB-PROCESSING

5.1. The Processor shall inform the Controller by writing an email to the main contact person of any intended change regarding the involvement or replacement of other Processors or Sub-Processors (hereinafter collectively "Sub-Processors"), giving the Controller the opportunity to object to such changes. If the Controller does not object within two weeks, the addition or replacement shall be deemed approved. In the event of an objection, the Processor may not make the subject change within the scope of the commissioned processing governed by this agreement. In any case, the Controller shall grant the Processor permission to involve the sub-processors listed in Annex 3.

5.2. If the Processor uses another sub-processor to carry out certain processing activities on behalf of the Controller, the same data protection obligations shall be imposed on that sub-processor by way of a contract, providing in particular sufficient guarantees that appropriate technical and organizational measures will be implemented in such a way that the processing will be carried out in accordance with the requirements of the applicable data protection law.

5.3. 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.

5.4. 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.

6. ASSISTANCE

6.1. To the extent possible, 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.

6.2. The Processor generally fulfills its obligations under Point 6.1 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 provide this assistance in exchange for appropriate additional compensation.

6.3. 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 3 ("Confidentiality") and 4 ("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 data subjects and (iii) providing the information listed in Annex 1 of this agreement.

6.4. The notification according to Point 6.3 (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 affected;
b. the likely consequences of the personal data breach;
c. the measures taken or proposed by the Controller to address the personal data breach.

7. AUDIT

7.1. The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set forth 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 audits shall be conducted at reasonable intervals and in a manner that does not disrupt the Processor's business operations. Costs incurred as a result of such audits 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 results of the audits available to the Controller.

8. LIABILITY

8.1. In the internal relationship with the Processor, the Controller shall be solely responsible to the data subject for compensation of damage suffered due to data processing or use within the scope of the commissioned processing that is inadmissible or incorrect under the data protection laws.

8.2. The parties shall each release themselves from liability if one party proves that it is not responsible in any respect for the circumstance that caused the damage to a data subject.

9. RETURN OF PERSONAL DATA

9.1. The Processor shall, at the choice of the Controller and within a reasonable time period, delete or return all the personal data to the Controller after the completion of the provision of services relating to processing, unless there is an obligation to store the personal data under Union or Member State law.

10. MISCELLANEOUS

10.1. Amendments to this agreement shall be made in writing. This also applies to this written form requirement.

10.2. This agreement is subject to Austrian law. The exclusive place of jurisdiction shall be Graz.

10.3. If any provision of this agreement is invalid or ineffective, it shall, to the extent permitted by law, be replaced by a provision that comes closest in economic terms to the invalid or ineffective provision.

10.4. The Processor shall be entitled to make legally compliant amendments to this declaration at any time. Should he (have to) make a change, he undertakes to transmit the latest valid version of this declaration of commitment to the responsible party in electronic form without being asked to do so.

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):

- First name, Last name
- Contact data (address, e-mail address)
- Passwords and other authentication data
- Logging data

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

PHYSICAL ACCESS CONTROL

The headquarter of Planforge 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

Planforge' 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 Planforge only.

The company network of Planforge 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

Company Name	Adress
IBM Cloud / SoftLayer Dutch Holdings B. V.	Paul van Vlissingenstraat 16, Amsterdam 1096 BK, Netherlands
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855 Luxembourg