orgvue

Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms part of the Master Subscription Agreement, Professional Services Agreement, Partner Agreement, End User License Agreement, or any other agreement pertaining to the delivery of services ('Agreement') between the Orgvue company, as set out in the Agreement ("Supplier") and the Customer named in such Agreement, to reflect the Parties' agreement with regards to the Processing of Personal Data.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Affiliates.

In the course of providing the Services to Customer pursuant to the Agreement, Supplier may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

If the entity signing this DPA is not a party to an effective Agreement with Supplier, this DPA shall not be valid or legally binding. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall prevail.

This DPA has been pre-signed on behalf of Supplier as the Processor.

1. Definitions

Unless specified otherwise below, capitalized words and expressions contained with this document have the same meaning as set out in the Agreement:

1.1. "**Affiliate**" means, with respect to a Party, any entity controlling, controlled by or under common control with such Party with "control" meaning the power (whether direct or indirect) to direct or cause the direction of an entity's affairs, whether by means of holding shares, possessing voting power, exercising contractual powers or otherwise and within "controlling" and "controlled" being construed accordingly.

1.2. "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

1.3. "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" and "**Supervisory Authority**" shall all have the same meaning given to those terms (or to analogous terms) in the Data Protection Laws and Regulations.

1.4. "**Customer**" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

1.5. "**Customer Personal Data**" means any Personal Data made available by the Customer to the Supplier in connection with the Agreement.

1.6. "**Data Protection Laws and Regulations**" means any applicable laws and regulations relating to the Processing, privacy, and security of Personal Data, as applicable to this DPA, including the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and any laws or regulations implementing European Council Directive 2002/58/EC; the GDPR and/or any corresponding, equivalent, amending or replacement national laws or regulations (including without limitation the UK's Data Protection Act 2018 and UK GDPR); the Swiss Federal Data Protection Act of 1992; the Australian Privacy Act; the CCPA; and any approved codes of conduct issued by any relevant data protection regulator.

1.7. "**EEA**" means the European Economic Area which currently comprises the 27 European Union Member States together with Norway, Iceland, and Liechtenstein.

1.8. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

1.9. which came into force on 25 May 2018 ("EU GDPR") and as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR").

1.10. "**IDT Addendum**" means the Standard Contractual Clauses, as amended by the 'International Data Transfer Addendum for Parties making Restricted Transfers, issued by the UK Information Commissioner in force on 21 March 2022 (and any successor clauses).

1.11. "**Restricted Transfer**" means the transfer of Personal Data outside of the UK, EEA, or Switzerland or which is otherwise considered to be a restricted transfer out of the originating country under Data Protection Laws and Regulations.

1.12. "**Standard Contractual Clauses**" means the standard contractual clauses annexed to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (and any successor clauses).

1.13. "**Sub-processor**" means any Processor engaged by Supplier.

2. Processing of Personal Data

2.1. Roles of the Parties. The parties acknowledge and agree that for the purposes of the Data Protection Laws and Regulations and with regard to the Processing of Personal Data, Customer is a Controller and Supplier is a Processor. The Supplier will engage Sub-processors pursuant to the requirements set forth in section 5 "Sub-processors" below.

2.2. Customer's Processing of Personal Data. In its use of the Services, Customer shall Process Customer Personal Data in accordance with the requirements of the Data Protection Laws and Regulations.

2.3. Supplier's Processing of Personal Data. Supplier shall treat Customer Personal Data as Confidential Information and shall Process Customer Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Supplier shall process Personal Data in accordance with the Data Protection Laws and Regulations and will notify Customer if it makes the determination that it can no longer comply with the Data Protection Laws and Regulations.

2.4. Details of the Processing. The subject-matter and purpose of Processing of Customer Personal Data by Supplier is to provide to Customer organizational design and workplace planning services via the Orgvue software application . The duration of the Processing will be for the Term of the Agreement and following the termination or the expiry of the Agreement until all Customer Personal Data is deleted from the Supplier's information technology by Supplier. The retention of aggregated information collated from the Customer and other customers relating to the access to, and use of, the Services ("**Usage Data**") by Processor will not prolong the term of these Personal Data Processing provisions under this DPA in the event that all other Customer Personal Data has been deleted by Supplier. The duration, nature, and purpose of the Processing and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Description of Processing/Transfer) to this DPA.

3. Rights of Data Subjects

3.1. Data Subject complaints and requests. Supplier shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject to exercise any of their rights under the Data Protection Laws and Regulations, related to the Customer Personal Data, each such request being a "Data Subject Request". Supplier shall not respond to a Data Subject Request itself, except that Customer authorizes Supplier to redirect the Data Subject to the Customer.

3.2. Request as necessary to allow Customer to respond directly. Taking into account the nature of the Processing,

Supplier shall reasonably assist Customer by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Supplier shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Supplier is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Supplier's provision of such assistance.

4. Supplier Personnel

4.1. Confidentiality. Supplier shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of the Customer Personal Data, have received appropriate training on their responsibilities, and are subject to the duty of confidentiality. Supplier shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Reliability. Supplier shall take commercially reasonable steps to ensure the reliability of any Supplier personnel engaged in the Processing of Customer Personal Data.

4.3. Limitation of Access. Supplier shall not access Customer Personal Data without Customer's express consent. Supplier shall ensure that Supplier's access to Customer Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4. Data Protection Officer. Supplier has appointed a data protection officer. The appointed person may be reached at privacy@orgvue.com.

5. Sub-processing

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that (a) Supplier's Affiliates may be retained as Sub-processors; and (b) Supplier and Supplier's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Supplier or a Supplier Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. List of Current Sub-processors and Notification of New Sub-processors. The current list of Sub-processors engaged by Supplier for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed under the Sub-processor List which can be found on Supplier's Trust Center webpage at https://trust.orgvue.com/subprocessors Customer hereby consents to these Sub- processors, their locations and processing activities as it pertains to Customer Personal Data. Supplier shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services. Such notification can be provided by Supplier updating its Sub-processor List, providing for the Customer the ability to sign up for email notice of such updates at https://trust.orgvue.com.

5.3. Objection Right for New Sub-processors. Customer may make reasonable and good faith objections to Supplier's use of a new Sub-processor by notifying Supplier promptly in writing within thirty (30) days of receipt of Supplier's notice in accordance with the mechanism set out in section 5.2. If Customer objects to a new Sub-processor as permitted in the preceding sentence, Supplier will: (i) use reasonable efforts to make available to Customer a change in the Services; (ii) recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer; or (iii) continue to provide the Services without the objected-to new Sub-processor.

5.4. Liability. Supplier shall be liable for the acts and omissions of its Sub-processors to the same extent Supplier would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

6. Security

6.1. Controls for the Protection of Personal Data. Supplier shall maintain proper administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Customer Personal Data. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Personal Data (other than by Customer or Users). The terms of Supplier's security provisions found at https://www.orgvue.com/legal/terms-and-conditions/orgvue-security-provisions/ are hereby incorporated by reference.

6.2. Audit. Supplier shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA as set forth in this section.

6.3. Third-Party Certifications and Audits. Supplier has obtained the third-party certifications and audits set out in Supplier's Trust Center found at https://trust.orgvue.com.

6.4. Data Protection Impact Assessment. Upon Customer's good faith written request, Supplier shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Supplier.

7. Personal Data Incident Management and Notification

7.1. Supplier maintains security incident management policies and procedures and shall promptly notify Customer (and in any event without undue delay) after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data, including Customer Personal Data, transmitted, stored or otherwise Processed by Supplier or its Sub-processors of which Supplier becomes aware (a "**Personal Data Incident**"), save where such Personal Data Incident is unlikely to result in a risk for the rights and freedoms of Data Subjects and Supplier is not otherwise required by law to notify Customer of such Customer Personal Data Incident. Supplier shall provide details of such Personal Data Incident and make reasonable efforts to identify the cause of such Personal Data Incident and take such steps as Supplier deems necessary and reasonable to remediate the cause of such a Personal Data Incident to the extent the remediation is within Supplier's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

7.2. Supplier will not inform any third party of a Personal Data Incident without first obtaining Customer's prior written consent, unless and to the extent that Supplier is otherwise required to provide notice by law.

8. Return and Deletion of Personal Data

8.1. On Customer's written request at any time, and in any event on termination or expiry of the Agreement, Supplier shall delete all Personal Data within ninety (90) days (and will cause its Sub-processors to do the same), unless Supplier is legally obliged to store Persona Data for a longer period.

9. Cross-Border Transfers

9.1. The following provisions in this section 9 apply only to the extent that the Processing under the Agreement constitutes a Restricted Transfer, where Customer is entering into an agreement with a Supplier entity not in the UK or EEA.

9.2. the Parties agree that:

(a) where the Restricted Transfer is subject to the UK GDPR, the IDT Addendum (referencing the applicable modules of the Standard Contractual Clauses) shall apply to such transfer; and

(b) where the Restricted Transfer is subject to the EU's GDPR, the Controller to Processor module of the Standard Contractual Clauses shall apply to such transfer,

and for the purposes of the IDT Addendum and Standard Contractual Clauses: (i) Customer is the data exporter

and Supplier is the data importer, (ii) Schedule 1 contains the relevant processing details, (iii) section 6.1 contains the security details, (iii) section 5 contains the details on sub-processing, (iv) the Parties agree that the optional clauses shall not be included, (v) for the Standard Contractual Clauses, the governing law and jurisdiction is the Netherlands and the Supervisory Authority shall be the Supervisory Authority of the country where the Customer is established or, if not established in the EEA, the Supervisory Authority of Ireland, and (vi) for the IDT Addendum, the governing law and jurisdiction and the Supervisory Authority shall be the UK.

(c) where the Restricted Transfer relates to a Customer based in Switzerland, the Standard Contractual Clauses shall be interpreted as to apply also to Switzerland and to Data Subjects and organizations in Switzerland save that, in respect of such Restricted Transfer: (i) the Federal Data Protection and Information Commissioner shall have responsibility for ensuring compliance with Swiss privacy laws and shall be the Supervisory Authority; and (ii) the Standard Contractual Clauses shall be subject to Swiss law and jurisdiction.

(d) where the Restricted Transfer relates to a Customer based in another territory not covered by (a) to (c) above, to the extent required and appropriate under such Data Protection Laws and Regulations, the Standard Contractual Clauses shall be interpreted so as to apply also to transfers from such Customer save that, in respect of such transfer: (i) the appropriate regulator in such jurisdiction shall have responsibility for ensuring compliance with such jurisdictions' privacy laws and shall be the Supervisory Authority; (ii) the Standard Contractual Clauses shall be subject to such jurisdictions' law and jurisdiction; and (iii) any references to the European Union shall be read as being references to the relevant exporting jurisdiction.

Schedule 1: Description of Processing/Transfer

Personal Data shall be processed under the Agreement as set out below.

Subject matter and duration of the Processing:

The subject matter is the provision of the Services by Supplier to the Customer under the Agreement, including to provide to Customer organizational design and workplace planning services via the Orgvue software application, and any improvements by the Supplier to the Services for the Term of the Agreement. The duration will be for the Term and following the termination or the expiry of the Agreement until all Personal Data is deleted from the Supplier's information technology by Supplier. The retention of aggregated Usage Data by Supplier will not prolong the term of these Personal Data Processing provisions in the event that all other Personal Data has been deleted by Supplier.

Frequency of the Processing:

Orgvue is delivered as Software as a Service (SaaS) and hosted on the Amazon Web Services (AWS) platform. Customers will dictate the frequency of data transfers into their instance of Orgvue.

Nature and purpose of the Processing:

Personal Data will be Processed for purposes of providing the Services in accordance with the Agreement.

Type of Personal Data:

Personal Data Processed in providing the Services may include the following categories of data: names, user IDs, email addresses, job titles, salary, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by Users via the Services.

No sensitive data is transferred.

Categories of Data Subject:

Personal Data submitted, stored, sent, or received via the Services may relate to Users and the Customer's employees and contractors as the Data Subjects.