

Xorolia Data Processing Agreement

1. INTRODUCTION

This agreement (“**Data Processing Agreement**” or “**DPA**”) regulates Content Formula Limited (“**Data Processor**”) processing of personal data on behalf of the customer (“**Data Controller**”) and is attached as an addendum to the Xorolia Software as a Service Agreement (“**SAASA**”) and the Software Purchase Agreement (“**SPA**”) in which the parties have agreed the terms for the Data Processor’s delivery of services to the Data Controller. The Software Purchase Agreement (SPA) also contains the parties’ contact details and other details pertinent to data protection including types and categories of data being processed.

2. DATA PROTECTION LAWS

The Data Processing Agreement shall ensure that the Data Processor complies with the applicable data protection and privacy legislation (“**Data Protection Law**”), including The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

3. PROCESSING OF PERSONAL DATA

3.1. The purpose of the processing under the SAASA is the provision of the Xorolia software, service, documentation, marketing and information materials (“**Service**”) by the Data Processor as specified in the SAASA.

3.2. In delivery of the Service for the Data Controller the Data Processor will process certain categories and types of the Data Controller’s data which shall include Personal Data, as defined in clause 3.3 below.

3.3. Personal Data includes any information relating to an identified or identifiable natural person as defined in GDPR, article 4 (1) (1) (“**Personal Data**”). The categories and types of Personal Data processed by the Data Processor on behalf of the Data Controller are listed in Software Purchase Agreement (SPA). The Data Processor only performs processing activities that are necessary and relevant to perform the Service. The parties shall update the relevant part of the SPA whenever changes occur to the processing activities that necessitate an update.

3.4. The Data Processor shall have and maintain a register of processing activities in accordance with GDPR, article 32 (2).

4. INSTRUCTION

4.1. The Data Processor may only act and process the Personal Data in accordance with the documented instruction from the Data Controller (“**Instruction**”), unless required by law to act without such instruction. The Instruction at the time of entering into this Data Processing Agreement is that the Data Processor may only process the Personal Data with the purpose of delivering the Service as described in the SAASA. Subject to the terms of this Data Processing Agreement and with mutual agreement of the parties, the Data Controller may issue additional written instructions consistent with the terms of this Data Processing Agreement. The Data

Controller is responsible for ensuring that all individuals who provide written instructions are authorised to do so.

4.2. The Data Controller guarantees to process Personal Data in accordance with the requirements of Data Protection Laws. The Data Controller's instructions for the processing of Personal Data shall comply with Data Protection Laws. The Data Controller will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which it was obtained.

4.3. The Data Processor will inform the Data Controller of any instruction that it deems to be in violation of Data Protection Laws and will not execute the instructions until they have been confirmed or modified.

5. THE DATA PROCESSORS OBLIGATIONS

5.1. CONFIDENTIALITY

5.1.1. The Data Processor shall treat all the Personal Data as strictly confidential information. The Personal Data may not be copied, transferred or otherwise processed in conflict with the Instruction, unless the Data Controller has agreed in writing.

5.1.2. The Data Processor's employees, contractors and sub-contractors ("**Staff**") shall be subject to an obligation of confidentiality that ensures that the Staff shall treat all the Personal Data under this DPA with strict confidentiality.

5.1.3. Personal Data will only be made available to Staff that require access to such Personal Data for the delivery of the Service and this DPA.

5.2. The Data Processor shall also ensure that Staff processing the Personal Data only process the Personal Data in accordance with the Instruction.

5.3. SECURITY

5.3.1. The Data Processor shall implement the appropriate technical and organizational measures as set out Data Protection Laws, including in accordance with GDPR, article 32. The security measures are subject to technical progress and development. The Data Processor may update or modify the security measures from time to-time provided that such updates and modifications do not result in the degradation of the overall security.

5.3.2. The Data Processor will if necessary, assists the Data Controller in ensuring compliance with the obligations pursuant to GDPR, article 32 taking into account the nature of processing and the information available to the Data Processor;

5.3.3. The Data Processor shall provide documentation for the Data Processor's security measures if requested by the Data Controller in writing.

5.4. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

If the Data Processor's assistance is necessary and relevant, the Data Processor shall assist the Data Controller in preparing data protection impact assessments in accordance with GDPR, article 35, along with any prior consultation in accordance with GDPR, article 36.

5.5. RIGHTS OF THE DATA SUBJECTS

5.5.1. If the Data Controller receives a request from a data subject for the exercise of the data subject's rights under the Data Protection Laws and the correct and legitimate reply to such a request necessitates the Data Processor's assistance, the Data Processor shall assist the Data Controller by providing the necessary information and documentation. The Data Processor shall be given up to 14 days to assist the Data Controller with such requests in accordance with the Data Protection Laws.

5.5.2. If the Data Processor receives a request from a data subject for the exercise of the data subject's rights under the Data Protection Laws and such request is related to the Personal Data of the Data Controller, the Data Processor must immediately forward the request to the Data Controller and must refrain from responding to the person directly.

5.6. PERSONAL DATA BREACHES

5.6.1. The Data Processor shall give immediate notice to the Data Controller if a breach occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or otherwise processed re the Personal Data processed on behalf of the Data Controller (a "Personal Data Breach").

5.6.2. The Data Processor shall make reasonable efforts to identify the cause of such a breach and take those steps as they deem necessary to establish the cause, and to prevent such a breach from reoccurring.

5.6.3. The Data Processor will if necessary further assists the Data Controller in ensuring compliance with the obligations pursuant to GDPR, article 33-34, regarding notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subjects taking into account the nature of processing and the information available to the Data Processor;

5.7. DOCUMENTATION OF COMPLIANCE AND AUDIT RIGHTS

5.7.1. Upon request by a Data Controller, the Data Processor shall make available to the Data Controller all relevant information necessary to demonstrate compliance with this DPA, and shall allow for and reasonably cooperate with audits, including inspections by the Data Controller or an auditor mandated by the Data Controller. The Data Controller shall give notice of any audit or document inspection to be conducted and shall make reasonable endeavours to avoid causing damage or disruption to the Data Processors premises, equipment and business in the course of such an audit or inspection. Any audit

or document inspection shall be carried out with reasonable prior written notice of no less than 30 days and shall not be conducted more than once a year.

5.7.2. The Data Controller may be requested to sign a non-disclosure agreement reasonably acceptable to the Data Processor before being furnished with the above.

5.8. DATA TRANSFERS

The Data Processor will not transfer personal data to countries outside of the Data Controller's and Data Processor's region, except where such transfer is required under Data Protection Laws. This means that data processed on behalf of European data controllers will not be transferred to third countries, except where such transfer is required by EU or Member State law to which the Data Processor is subject.

6. SUB-PROCESSORS

6.1. The Data Processor is given general authorisation to engage third-parties to process the Personal Data ("Sub-Processors") without obtaining any further written, specific authorization from the Data Controller, provided that the Data Processor notifies the Data Controller in writing about the identity of a potential Sub-Processor (and its processors, if any) before any agreements are made with the relevant Sub-Processors and before the relevant Sub-Processor processes any of the Personal Data. If the Data Controller wishes to object to the relevant Sub-Processor, the Data Controller shall give notice hereof in writing within ten (10) business days from receiving the notification from the Data Processor. Absence of any objections from the Data Controller shall be deemed a consent to the relevant Sub-Processor.

6.2. In the event the Data Controller objects to a new Sub-Processor and the Data Processor cannot accommodate the Data Controller's objection, the Data Controller may terminate the Service by providing written notice to the Data Processor.

6.3. The Data Processor shall complete a written sub-processor agreement with any Sub-Processors. Such an agreement shall at minimum provide the same data protection obligations as the ones applicable to the Data Processor, including the obligations under this Data Processing Agreement. The Data Processor shall on an ongoing basis monitor and control its Sub-Processors' compliance with the Data Protection Law. Documentation of such monitoring and control shall be provided to the Data Controller if so requested in writing.

6.4. The Data Processor is accountable to the Data Controller for any Sub-Processor in the same way as for its own actions and omissions.

6.5. The Data Processor is at the time of entering into this Data Processing Agreement using the Sub-Processors listed in the SPA. If the Data Processor initiates sub-processing with a new Sub-Processor, such new Sub-Processor shall be added to the list in the SPA.

7. LIMITATION OF LIABILITY

- 7.1. The total aggregate liability to the Customer, of whatever nature, whether in contract, tort or otherwise, of the Data Processor for any losses whatsoever and howsoever caused arising from or in any way connected with this engagement shall be subject to the “Limitation of Liability” clause set out in the Software as a Service Agreement (SAASA).
- 7.2. Nothing in this DPA will relieve the Data Processor of its own direct responsibilities and liabilities under the GDPR.

8. TERMINATION

- 8.1. The Data Processing Agreement shall remain in force until the SAASA is terminated.
- 8.2. Following expiration or termination of the SAASA, the Data Processor will delete or return to the Data Controller all Personal Data in its possession as provided in the Agreement except to the extent the Data Processor is required by law to retain some or all of the Personal Data (in which case the Data Processor will archive the data and implement reasonable measures to prevent the Personal Data from any further processing and to protect it from theft). The terms of this DPA will continue to apply to such Personal Data.