Encyro Inc Data Processing Agreement

This Data Processing Agreement (the "DPA"), entered into by you, as a user of Encyro's services, the entity you represent (the "Controller") and Encyro Inc., a California (USA) Corporation (the "Processor"), collectively referred to as parties (the Parties) to this agreement, governs the processing of personal data collected from data subjects by the Controller and transferred to the Processor.

It forms part of the Terms of Service (available at https://www.encyro.com/legal) that govern the relationship between Processor and Controller.

Overview

1.1 The parties agree to enter into this agreement to comply with their data protection requirements under applicable data protection laws, including the EU General Data Protection Regulation 2016/679 and equivalent UK laws.

Definitions

2.1 "Applicable Laws" means (a) European Union or Member State laws with respect to any Personal Data in respect of which the Controller is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Personal Data in respect of which the Controller is subject to any other Data Protection Laws.

2.2 "Personal Data" means any personal data collected from data subjects covered under Applicable Laws by the Controller and processed by the Processor. Such data includes data exchanged by the data subjects with the Controller using Processor's services. It does not include data exchanged by the data subjects, using Processor's services, with any person or entity other than the Controller.

2.3 "Subprocessor" means any person or entity (excluding any employees of the Processor) appointed by or on behalf of the Processor to process Personal Data provided to the Processor by the Controller.

2.4 "Personal Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Compliance with Laws

3.1 The parties shall each comply with their respective obligations under all Applicable Laws.

Controller Obligations

4.1 Controller agrees to:

4.1.1 Provide instructions to Processor and determine the purposes and general means of Processor's processing of Personal Data in accordance with this DPA (using the functionality in the computer applications or software services provided by the Processor); and

4.1.2 Comply with the Controller's obligations to protect, secure and otherwise maintain the privacy of Personal Data subject to Applicable Laws. These obligations include: (a) establishing and maintaining a procedure for the exercise of the rights of the individuals whose Personal Data are processed on behalf of Controller; (b) processing only data that has been lawfully and validly collected and ensuring that such data will be relevant and proportionate to the respective data subjects; and (c) ensuring compliance with the provisions of this DPA by its personnel or by any third-party accessing or using Personal Data on its behalf.

4.2 The Controller instructs the Processor to

4.3.1 Process Personal Data, and

4.3.2 Transfer Personal Data to any country or territory

as reasonably necessary to provide the services offered by the Processor to the Controller.

4.3 The Controller warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in section 4.2.

4.4 The Controller understands that the Processor's online services allow the Controller to transmit Personal Data to any person or entity.

4.4.1 The Controller agrees not to use the Processor's services to transmit Personal Data to any person or entity that is not authorized to receive such data under Applicable Laws.

4.4.2 In all instances of use of the Processor's services, where the Processor's services allow the Controller to identify a person or entity using an email address, phone number, or other identifier, the Controller agrees to ensure the validity and correctness of such identification.

Processor Obligations

5.1 **Security**

5.1.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of Personal Data, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and Applicable Laws. Such measures may include appropriate encryption and access control methods, protected remote data backups, and periodic testing and audit of safeguards employed.

5.1.2 Processor shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the Processing in its area of responsibility is carried out in compliance with the requirements of applicable data protection law and that the protection of the rights of the data subject is ensured.

5.1.3 Processor shall document the implementation of the technical and organizational measures set out and required on its website. Controller may inspect that documentation to determine the suitability of using the Processor's services.

5.1.4 Processor shall establish the security of the processing pursuant to Art. 28 (3) c), 32 GDPR, in connection with Art. 5 GDPR. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR must be considered.

5.1.5 The technical and organizational measures are subject to technical progress and further development. In this respect, Processor is permitted to implement alternative adequate measures. Processor reserves the right to change the security measures taken. Processor shall

ensure that the contractually agreed level of protection is not undercut. Significant changes shall be documented.

5.1.6 The Processor shall ensure that persons authorized by the Processor to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.2 **Sub-processing**

5.2.1 Processor shall ensure that any Sub-processors appointed are required to comply with and acknowledge and respect the confidentiality of the Personal Data. Processor shall carry out commercially reasonable due diligence to ensure that the Sub-processor is capable of providing a level of protection for Personal Data consistent with this DPA. Processor may use contracts or other legal acts to ensure that each such Sub-processor is bound to the requirements of Applicable Laws.

5.2.2 Processor shall give the Controller 30 days prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Subprocessor. Such a notice may be provided by updating a list of Sub-processors that the Processor maintains on its website.

5.2.3 Processor hereby gives notice to Controller that the Sub-processors listed at https://www.encyro.com/legal/subprocessors are employed.

5.2.4 If the Controller does not approve of a Sub-processor, and the Processor does not change or remove such Sub-processor, Controller may (1) stop using the functionality that requires processing by that sub-processor if feasible (e.g., to prevent sub-processing by Meta, Controller may stop using the Sign-in with Facebook functionality), (2) stop using Encyro services for data that that they do not wish to share with that sub-processor and use Encyro services only for other data, or (3) terminate this DPA and its other agreements with the Processor as facilitated by Section 6.2.

5.3 **Processing**

The Processor shall process Personal Data, as instructed by the Controller using the Processor's website, software applications, or other means provided by the Processor, as following:

5.3.1 Nature and Purpose of Processing

5.3.1.1 The Processor shall store Personal Data for access by the Controller and any persons or entities, identified by the Controller per Section 4.4.2, as instructed by the Controller using the means of instruction provided by the Processor.

5.3.1.2 The Processor shall transmit Personal Data to any person or entity, identified by the Controller per Section 4.4.2, as instructed by the Controller using the means of such instruction provided by the Processor.

5.3.1.3 The Processor may review the Personal Data for abusive, offensive, or illegal content or other such requirements specified in the Processor's Privacy Policy.

5.3.1.4 The Processor may allow law enforcement agencies to access Personal Data when required by law. Unless restricted by law, the Processor shall promptly notify the Controller upon being contacted directly by a law enforcement agency to initiate such a disclosure. This notification requirement is not enforced on Subprocessors.

5.3.1.5 The Processor may employ automated methods to analyze Personal Data for the purpose of providing the Processor's services and also to support the Processor's own operational requirements including detection of malware (e.g. computer viruses), illegal content (e.g. content that violates intellectual property or copyright laws), excessive usage (e.g. denial of service or DoS attacks), network or computer system threats and attacks, or other such requirements specified in the Processor's Privacy Policy.

5.3.1.6 The Processor may make copies of, transmit to backup facilities, modify (e.g. encrypt), hash (anonymize, pseudonymize, obfuscate), and attach metadata to, the Personal Data as required by the Processor to maintain the security, privacy, integrity and resilience of the Personal Data, to meet Applicable Law and to satisfy the Processor's own data protection mandates in cases where the protection required by Applicable Law is determined to be insufficient.

5.3.2 Subject Matter and Duration of Processing

5.3.2.1 The subject matter of the DPA is set out in this DPA, the Processor's Terms of Service for all of Processor's services used by the Controller, and any related agreements entered into by the Parties.

5.3.2.2 The duration of the processing shall be the entire duration between the time that the Controller signs up for the Processor's services and the time until when the Controller terminates its account with the Processor's online or software services. The duration of processing will include an additional time period as reasonably required by the Processor to remove the Personal Data. Such a time period will include any delays due to technology limitations, legal data retention requirements, any data backup or retention period previously committed by the Processor, and security review or audit delays.

5.3.3 Types of Personal Data

The types of Personal Data include:

5.3.3.1 All data provided to the Processor after it is collected by the Controller from the data subjects, in the course of providing the Controller's services, in the sole discretion of the Controller regarding the necessity of that data and the Controller's adherence to Applicable Laws. Data types include but are not limited to health records, financial data, educational or training credentials, creative works, legal or business contracts, real estate records, insurance data, and personal contact information.

5.3.3.2 Data collected by the Processor directly due to the use of the Processor's computer systems and networks by the data subjects served by the Controller. Such data includes computer Internet Protocol (IP) addresses, times and location data, device types (such as desktop, mobile, tablet, or other), device software platform (operating system, browser, language, dialect), network provider, Internet Service Provider (ISP).

5.3.3.3 Data provided to the Processor directly by the data subjects when accessing and setting up their accounts on the Processor's website or software applications provided by the Processor to use the Processor's services. Such data includes the data subjects' username, email address, full name, address, phone number, photo, business logo, and other account configurations such as color preference and choice of design templates.

5.3.3.4 Data provided by the data subjects to the Processor for the purposes of transmission to the Controller or any other person or entity. Such data may include any type of data requested by the Controller from the data subjects or any data voluntarily sent by the data subject.

5.3.4 Categories of Data Subjects

The categories of data subjects include all persons or entities from which Controller collects data in the course of providing the Controller's services.

5.4 **Notice to Controller**

5.4.1 Personal Data Breach

5.4.1.1 Processor shall notify Controller without undue delay upon Processor or any Subprocessor becoming aware of a breach of data that includes Personal Data and shall provide to the Controller sufficient information to allow the Controller to meet any obligations to report or inform data subjects of the Personal Data Breach under Applicable Laws. However, Processor cannot itself inform data subjects, because the Processor does not have the capability to identify or determine which specific data subjects are referenced in the data files provided by the Controller without further processing and such required processing may not be feasible.

5.4.1.2 Processor shall co-operate with Controller and take commercially and technically reasonable steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

5.4.2 Disclosure of Personal Data

The Processor shall inform the Controller regarding any legally binding or voluntarily accepted request for disclosure of Personal Data by a law enforcement or supervisory authority, unless Processor is otherwise forbidden by law to inform the Controller, for example to preserve the confidentiality of an investigation by law enforcement authorities insofar as it does not require further processing of Personal Data to identify data subjects in data files provided by the Controller.

5.4.3 Complaints

Processor shall inform controller regarding any notices or complaints received by the Processor, with respect to Personal Data, from the data subjects or their legal representatives. Processor will not respond to any such request without Controller's prior written or emailed authorization. Furthermore, Processor may not be able to associate Personal Data present in data files provided by Controller with the respective data subjects.

5.4.4 Address for Notice

Controller agrees that any reports, notification, or other notice by Encyro pursuant to this DPA may be made electronically. Controller shall provide its electronic contact information to info@encyro.com or update it within its Encyro account.

5.5 **Assistance to Controller**

Processor will provide reasonable assistance to Controller regarding:

5.5.1 Any requests from data subjects in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of Personal Data that Processor processes for Controller. In the event that a data subject sends such a request directly to Processor, Processor will promptly send such request to Controller. Processor cannot fix erroneous data or inform data subjects without the Controller linking the data subject and the respective Personal Data, as Processor is not able to associate data subjects with Personal Data without further processing Personal Data.

5.5.2 Where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any supervisory authority.

5.6 **Required Processing**

If Processor is required by Applicable Laws to process any Personal Data for a reason other than providing the services described in this DPA, Processor will inform Controller of this requirement in advance of any processing, unless Processor is legally prohibited from informing Controller of such processing (e.g., as a result of secrecy requirements that may exist under applicable EU member state laws).

5.7 **Audit Rights**

Processor shall make available to Controller, on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the processing of Personal Data.

5.7.1 These audit rights only arise to the extent that this DPA or the Processor's website does not provide sufficient information to meet the requirements of Applicable Law. Pursuant to Art. 28 (5) of the GDPR, the Processor's compliance with approved codes of conduct pursuant to Art. 40 of the GDPR or an approved certification procedure pursuant to Art. 42 of the GDPR may be used to demonstrate sufficient guarantees within the meaning of Art. 28 (1) and (4) of the GDPR instead of on-site inspections. The Processor undertakes to inform the Controller without undue delay of the exclusion of approved codes of conduct pursuant to Art. 41 (4) GDPR and the revocation of a certification pursuant to Art. 42 (7) GDPR.

5.7.2 Reasonable advance notice of audit, at least 3 days prior to an inspection or audit, is required. No more than one audit may be conducted within a year, except when a continuation audit is required after rectification of deficiencies identified in a previous audit.

5.7.3 Processor reserves the right to protect its trade secrets, operational know-how, and intellectual property during such an audit.

5.7.4 If Controller commissions a third party to carry out the inspection, Processor shall oblige the third party in writing in the same way as Processor is obliged to Controller on the basis of this Agreement. In addition, Controller shall oblige the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional confidentiality obligation (e.g. German lawyers). Upon request of Processor, Controller shall submit to Processor the obligation agreements with the third party. Controller may not commission a competitor of Processor with the inspection.

5.7.5 Processor may demand compensation from the Controller for enabling the inspection, depending on the time and effort involved. The amount shall be determined in accordance with

the hourly rates for consulting services customary at the time of implementation on the part of the Processor.

5.8 **Deletion or Return of Personal Data**

5.8.1 Processor shall, within a reasonable time period, after cessation of any services involving the processing of Personal Data, delete, or return to Controller, at the choice of the Controller, all copies of the Personal Data in possession of the Processor and its Subprocessors. The reasonable time period will include any delays due to technology limitations, legal data retention requirements, any data backup or retention period previously committed by the Processor, and security review or audit delays.

5.8.2 Processor may retain Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws. In such cases, Processor shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only processed as necessary for the purpose(s) of complying with Applicable Laws.

5.9 **Data Transfers**

Controller acknowledges and agrees that, in connection with the performance of the services under this DPA, Personal Data will be transferred to the Processor's or its Subcontractor's facilities in the US. For transfers of Personal Data by Processor to any countries that are not considered to be providing adequate data protection, Processor agrees it will provide at least the same level of privacy protection as required by Applicable Laws for EU Personal Data and will enter into the EU Commission's Standard Contractual Clauses. The same applies for UK Personal Data, where Processor will enter into the UK Addendum to the EU-SCCs. If a Subprocessor has Binding Corporate Rules in place, which are recognized by the EU Commission, this shall be the legal basis for the data transfer instead of the SCCs. Processor shall promptly notify Controller of any inability by Processor to comply with the provisions of this Section 5.9.

Term and Termination

6.1 This DPA shall remain in effect as long as Processor carries out Personal Data processing operations on behalf of Controller, as indicated by the Controller continuing to retain an online account on the Processor's website, or until this DPA is superseded by a newer DPA with a more recent effective date.

6.2 This DPA may be terminated at any time by the Controller or the Processor with or without cause, without prejudice to any fees paid by the Controller to the Processor or to any expenses incurred by either party in connection with services provided subject to this DPA. Upon termination:

6.2.1 Controller will cease the use of any of the Processor's services, and inform the Processor in writing regarding such cessation.

6.2.2 The Processor will return or delete Personal Data according to Section 5.8 of this DPA.