GDPR Data Processor Addendum

To the extent that Kollective Technology, Inc. ("Processor") engages in the processing of personal data on behalf of its customers (each a "Controller"), in the course of carrying out Processor's obligations under the applicable services agreement with the Controller (the "Agreement"), Processor shall comply with all applicable data protection laws, including but not limited to European Union Directive 95/46/EC and Regulation 2016/679 (the General Data Protection Regulation or "GDPR"). Unless otherwise specified all terms used herein shall have the same meaning as under the GDPR.

Without limiting the foregoing, each of Controller and Processor represent, warrant, and agree:

1. Processor shall implement appropriate technical and organizational measures designed in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

2. Controller grants Processor general authorization to engage other processor(s) (i.e. sub-processor(s)). Controller authorizes and consents to the use of those sub-processors already engaged by Processor, specifically those listed in Appendix A-1; provided, however, that Processor shall comply with the requirements of Section 3. Controller may find a current list of sub-processors on Processor's website here https://kollective.com/privacy-policy/ as well as a mechanism to subscribe to notifications of new sub-processors, to which Controller may subscribe, and if Controller subscribes, Processor 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. Controller may object to Processor's use of a new sub-processor by notifying Processor promptly in writing within thirty (30) days after receipt of Processor's notice at dpo@kollective.com. In the event Controller objects to a new sub-processor, as permitted in the preceding sentence, Processor will use reasonable efforts to make available to Controller a change in the services or recommend a commercially reasonable change to Controller's configuration or use of the services to avoid Processing of personal data by the objected-to new sub-processor without unreasonably burdening Controller. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Controller may terminate the applicable order form(s) with respect only to those services which cannot be provided by Processor without the use of the objected-to new sub-processor by providing written notice to Processor.

3. Where Processor engages another processor for carrying out specific processing activities on behalf of Controller, the same data protection obligations as set out in the Agreement and herein shall be imposed on that other processor by way of a contract, and, such contract will provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR and other applicable law. Where that other processor fails to fulfil its data protection obligations, Processor shall remain fully liable to Controller for the performance of that other processor's obligations.

4. Processing may only be undertaken for purposes set forth in Appendix A-1 setting out the subject matter and duration of the processing to be undertaken, the nature and purpose of the processing, the type of personal data and categories of data subjects to be processed, or written instructions of the Controller, including without limitation specific written agreements between Processor and Controller.

5. Processor shall:
   (a) process the personal data only on documented instructions from the Controller (unless doing so would be unlawful or change the services offered), including with regard to transfers of personal data to a third country or an international organization, unless required to do so by 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. 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;
   (b) secure all personal data, including taking all measures required pursuant to GDPR Article 32;
   (c) ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
   (d) only engage another processor in compliance with the terms set forth in Sections 2 and 3;
   (e) At Controller's expense, assist the Controller, taking into account the nature of the processing, by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR (GDPR Articles 12-23);
   (f) At Controller's expense, assist the Controller in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 taking into account the nature of processing and the information available to the Processor;
   (g) at the choice of the Controller, delete or return all personal data to the Controller after the end of the provision of services relating to processing and delete existing copies unless retention of the personal data is required by law; and
   (h) make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations set forth herein and, at Controller's expense, allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, and Processor shall immediately inform Controller if, in its opinion, an instruction infringes GDPR requirements or other European Union or Member State data protection provisions.

6. If any of the personal data to be processed includes any data originating in the European Economic Area or Switzerland, then Controller and Processor will agree and enter into the Standard Contractual Clauses which have been added as Appendix A-2 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection if applicable.

Appendix A-1 to GDPR Data Processor Addendum

Data subjects

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

- Employees and contractors of the Controller

Categories of data

The personal data transferred concern the following categories of data:

- Full name
- Email address
- IP address
- Digital image
- Username

Special categories of data (if appropriate)

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

- Not Applicable. No special categories of personal data are processed by Kollective Technology, Inc.

Processing operations

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

- Full name- Setting up user accounts
- Email address- Setting up user accounts
- Username- Setting up user accounts
- IP address- Used by Kollective application to build peering network
- Digital image- Provide video streaming or live event services

Current Sub-processors:

Name of Sub-processor	Address	Place of Processing	Basis of legal transfer	Purpose of Processing
Microsoft	One Microsoft Way, 98052, Redmond, WA, United States of America	USA, Netherlands	Standard Contractual Clauses	Office O365 products and Azure cloud data storage and processing
Amazon	USA	USA	Standard Contractual Clauses	Cloud data storage
Marketo	901 Mariners Island Boulevard Suite #500 (Reception) San Mateo, CA 94404 USA	USA	Standard Contractual Clauses	Storage of names and email addresses for marketing
SalesForce.com	Salesforce Tower 415 Mission Street, 3rd Floor San Francisco, CA 94105 USA	USA	Standard Contractual Clauses	Storage of names and email addresses for procurement contacts
Intacct	Sage Intacct 300 Park Avenue, Suite 1400 San Jose, CA 95110 USA	USA	Standard Contractual Clauses	Storage of names and email addresses for contracts/ order processing
SumoLogic	305 Main Street Redwood City, CA 94063 USA	USA	Standard Contractual Clauses	Processing of PII for log analytics
Auth0	10800 NE 8th, St Suite 700 Bellevue, WA 98004 USA	USA	Standard Contractual Clauses	Storage of IP addresses, email addresses, user names, and names for security and authentication
Zendesk	989 Market St San Francisco, CA 94103	USA	Standard Contractual Clauses	Storage of email addresses and user names for user login credentials
Datastax	975 Freedom Circle 4th Floor Santa Clara, CA 95054, USA	USA, Netherlands	Standard Contractual Clauses	Storage of IP addresses for establishing peering mesh
Planhat	Planhat AB c/o iOffice Kungsgatan 64 111 22 Stockholm, Sweden	USA	Standard Contractual Clauses	Storage of name and email addresses for IT user contacts for optimizing customer service

Current Affiliates

- Kollective Technology Limited
- Kollective Technology PTE LTD
- Kollective Technology Pty Ltd
- Kollective Technology GK
- Kollective Technology (KT) GmbH

Description of the technical and organizational security measures implemented by Processor:

A. Purpose and Scope

In developing the technical and organizational measures implemented by Kollective to ensure secure processing in accordance with Art. 32 GDPR, Kollective has taken into account the following key factors:

1. State of the art
2. Implementation costs
3. The nature, scope, context and purposes of processing
4. The likelihood and severity of risks of the processing for data subjects
5. The organizational measures taken to ensure that the level of protection for the processing of personal data is adequate

Kollective shall take appropriate technical and organizational measures in accordance with Art. 32 GDPR such as:

1. Encryption of personal data
2. Confidentiality, integrity, availability and resilience of processing systems and services
3. The ability to restore the availability and access to personal data
4. A process for the regular review of the technical and organizational measures

B. Overview

1. Pseudonymization and Encryption of Personal Data

a. Kollective does not perform pseudonymization.
b. Kollective policies require the encryption of sensitive information during transmission over public networks and business data at rest.

2. Effectiveness of the Implemented Technical and Organizational Measures

Kollective has established a procedure for the regular review of the effectiveness of the technical and organizational measures in order to ensure the security of the processing of personal data (Art. 32 (1) GDPR).

3. Information Security Policy

There is an organizational information security policy (ISP), in which essential behaviors regarding IT security and data protection are described. Employees are contractually obliged to observe and comply with the ISP. Furthermore, upon the start of employment, employees are required to read and sign the ISP and renew their acknowledgment annually. Training courses on information security are distributed annually and are compulsory for continued employment.

C. Controls

1. Logical and Physical Access Controls

a. Remote access to the hosted environment through the corporate network is restricted to the VPN which also employs WIKID two-factor authentication. Accounts are reviewed and approved according to the Kollective Least Privilege policy.

b. Administrative level access is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.

c. All access (Administrative & Non-Administrative) is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.

d. Kollective Technology administrative and general user account passwords have the following password parameters:

- Minimum eight (8) characters in length and require an alphanumeric combination.
- Passwords are set with a 90-day expiration date.
- History: five (5) remembered passwords
- Auto-lockout: 30 minutes
- Auto-lockout after five (5) logon attempts

e. Kollective Technology IT performs periodic network testing using penetration and vulnerability assessment tools (e.g. Qualys.). The results of these reviews are summarized in a report by Kollective Technology IT and presented to management.

f. All administrative access to servers and network devices must be approved by Operations Management.

g. HR provides termination notices to IT. Upon receipt of this notification, IT terminates the account on the date of termination or within one day of receipt of the notice.

h. Systems are configured to require a separate user ID and password.

i. Kollective Technology's employees are required by policy to periodically change their passwords and select passwords that are at least 8 characters and include a combination of alphabetic and non-alphabetic characters.

j. Access to the Equinix data centers is only accessible to authorized Operations personnel.

k. Data transmission between the user organizations and Kollective Technology is protected against disclosure to third parties utilizing appropriate security protocols (e.g. SSL, TLS, etc.).

l. Kollective policies require the encryption of sensitive information during transmission over public networks and business data at rest.

m. Backup data is encrypted during creation.

n. McAfee virus protection receives automatic virus definition updates. Uploaded content is scanned during the upload process via a command line scanner before the content can be stored on the Linux server. Nightly, content servers are scanned for viruses. Scan vendor may differ based on environment.

o. Incidents are followed up on by Security Response Team as needed and documented in an email with the appropriate parties being notified.

2. **Systems Operations Controls**
   - **a.** Full backups of the KDMS database are done on a daily basis. IT monitors the backup completion. Issues or anomalies are investigated and resolved to ensure a full backup is successfully achieved.
   - **b.** Annually a test of restores is performed to ensure that data can be restored from backups if needed.
   - **c.** Kollective IT performs periodic network testing using penetration and vulnerability assessment tools (e.g. Qualys.). The results of these reviews are summarized in a report by Kollective IT and presented to management.
   - **d.** Operations personnel follow defined protocols for evaluating reported events. Security related events are assigned to the security group for evaluation.
   - **e.** For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.

3. **Change Management Controls**
   - **a.** Management performs a review of operating system software, network configuration and database software to ensure configuration settings and patch levels are in compliance with the Corporate minimum security baselines and that out-of- compliance configurations are corrected appropriately.
   - **b.** Emergency changes must obtain Operational Certification and reviewed by operations management.
   - **c.** Changes are reviewed at the weekly release management meeting and scheduled for production to migration.
   - **d.** The appropriate requestor, business owners, or project sponsor reviews and approves changes prior to introduction into the production environment. Approvals for release into production are based upon Quality Assurance (QA) certification and are also captured in the weekly release management meeting.
   - **e.** Separate environments are used for development, testing, and production.
   - **f.** Developers do not have the ability to make changes to software in production.

4. **Availability Control**
   - **a.** Processing capacity is monitored on an ongoing basis. Issues or anomalies are investigated and resolved to ensure a predetermined capacity levels are successfully maintained.
   - **b.** Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available.
   - **c.** Business continuity and disaster recovery plans, including restoration of backups, are updated and tested annually.

5. **Confidentiality Controls**
   - **a.** The ISP contains explicit language that does grant Kollective access and use of confidential information in a controlled manner.
   - **b.** Application code restricts the ability to access, modify, and delete client data to only authorized individuals.
   - **c.** Policies and procedures are in place to restrict sharing of confidential client information with vendors or other third parties.
   - **d.** Management is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to users, related parties, and vendors.
   - **e.** Kollective has a documented data retention policy and has automated processes in place to retain and dispose of information in accordance with those policies.

6. **Monitoring of Controls**
   a. Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.

7. **Rick Management and Design and Implementation Controls**
   a. Kollective has a defined risk acceptance policy that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Identified risks are rated using a risk ranking, and Kollective develops risk mitigation strategies to manage the impact of those risks.
   b. On a quarterly basis, management performs a risk assessment to identify and rate key threats and risks.

8. **Communications Controls**
   a. Kollective has defined user security commitments that are available to Kollective's internal and external users via intranet. Kollective has also established a Security and Compliance Overview document highlighting Kollective'ss security commitments that is shared with external users at the time of registration.
   b. Kollective's security, availability, and confidentiality commitments and related responsibilities, including management, operational, and technical controls; the incident management process; how to contact Kollective with inquiries, complaints, and disputes; customer responsibilities; and legal requirements, are communicated to customers through contracts, service level agreements, terms of service and other documentation which are communicated to every customer during initial onboarding or are made available on Kollective sites and audit reports.

9. **Organization and Management Controls**
   a. Management establishes training plans and requirements for continued training for its employees.
   b. Personnel are required to read and accept the Employee Handbook which contains the Business Ethics and code of conduct and the statement of confidentiality and privacy practices upon their hire.
   c. Personnel must pass a criminal background check before they may be hired by Kollective.
   d. Employees are required to attend security, availability, and confidentiality training during the onboarding process. They are required to read and accept Kollective's security, availability, and confidentiality commitments upon hire.

Appendix A-2 to GDPR Data Processor Addendum

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organization:	Customer Organization Name (add in signature blocks as well)
Address:	
Tel:	
Email:	
Other information needed to identify the organization	

(the data **exporter**)

and

Name of the data importing organization:	Kollective Technology, Inc.
Address: 549 NW York Drive, Suite 260, Bend, OR 97703 USA	
Tel: +1 (541) 371-2661	
Email: dpo@kollective.com	
Other information needed to identify the organization	

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub processor'* means any processor engaged by the data importer or by any other sub processor of the data importer who agrees to receive from the data importer or from any other sub processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organizational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by

operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third- party liability of the sub processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation; that it will ensure compliance with the security measures

(e) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(f) to forward any notification received from the data importer or any sub processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(g) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(h) that, in the event of sub processing, the processing activity is carried out in accordance with Clause 11 by a sub processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(i) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its Instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the Instructions and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorized access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request and expense of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information,

with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub processor will be carried out in accordance with Clause 11; to send promptly a copy of any sub processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub processor agrees that the data subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub processor preventing the conduct of an audit of the data importer, or any sub processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub processing

1. Controller grants Processor general authorization to engage other processor(s) (i.e. sub-processor(s)). Controller authorizes and consents to the use of those sub-processors already engaged by Processor, specifically those listed in Appendix A-1; provided, however, that Processor shall comply with the requirements of Section 3. Controller may find a current list of sub-processors on Processor's website here https://kollective.com/privacy-policy/ as well as a mechanism to subscribe to notifications of new sub-processors, to which Controller may subscribe, and if Controller subscribes, Processor 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. Controller may object to Processor's use of a new sub-processor by notifying Processor promptly in writing within thirty (30) days after receipt of Processor's notice at dpo@Processor.com. In the event Controller objects to a new sub-processor, as permitted in the preceding sentence, Processor will use reasonable efforts to make available to Controller a change in the services or recommend a commercially reasonable change to Controller's configuration or use of the services to avoid Processing of personal data by the objected-to new sub-processor without unreasonably burdening Controller. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Controller may terminate the applicable order form(s) with respect only to those services which cannot be provided by Processor without the use of the objected-to new sub-processor by providing written notice to Processor.

2. Where Processor engages another processor for carrying out specific processing activities on behalf of Controller, the same data protection obligations as set out in the Agreement and herein shall be imposed on that other processor by way of a contract, and, such contract will provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR and other applicable law. Where that other processor fails to fulfil its data protection obligations, Processor shall remain fully liable to Controller for the performance of that other processor's obligations.

3. The prior written contract between the data importer and the sub processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third- party liability of the sub processor shall be limited to its own processing operations under the Clauses.

4. The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

5. The data exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

- The data exporter is a customer of Kollective Technology, Inc. ("Kollective") for the purposes of acquiring content and data delivery services pursuant to a services agreement between data exporter and Kollective.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

- The data importer is Kollective for the purposes of providing content and data delivery services to Customer pursuant to a services agreement between data exporter and Kollective.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- Employees and contractors of the data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

- Full name
- Email address
- IP address
- Digital image
- Username

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- Not Applicable. No special categories of personal data are processed by Kollective Technology, Inc.

Processing operations

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

- Full name- Setting up user accounts
- Email address- Setting up user accounts
- Username- Setting up user accounts
- IP address- Used by Kollective application to build peering network
- Digital image- Provide video streaming or live event services

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

A. Purpose and Scope

In developing the technical and organizational measures implemented by Kollective to ensure secure processing in accordance with Art. 32 GDPR, Kollective has taken into account the following key factors:

1. State of the art
2. Implementation costs
3. The nature, scope, context and purposes of processing
4. The likelihood and severity of risks of the processing for data subjects
5. The organizational measures taken to ensure that the level of protection for the processing of personal data is adequate

Kollective shall take appropriate technical and organizational measures in accordance with Art. 32 GDPR such as:

1. Encryption of personal data
2. Confidentiality, integrity, availability and resilience of processing systems and services
3. The ability to restore the availability and access to personal data
4. A process for the regular review of the technical and organizational measures

B. Overview

1. Pseudonymization and Encryption of Personal Data

a. Kollective does not perform pseudonymisation
b. Kollective policies require the encryption of sensitive information during transmission over public networks and business data at rest.

2. Effectiveness of the Implemented Technical and Organizational Measures

Kollective has established a procedure for the regular review of the effectiveness of the technical and organizational measures in order to ensure the security of the processing of personal data (Art. 32 (1) GDPR).

3. Information Security Policy

There is an organizational information security policy (ISP), in which essential behaviors regarding IT security and data protection are described. Employees are contractually obliged to

observe and comply with the ISP. Furthermore, upon the start of employment, employees are required to read and sign the ISP and renew their acknowledgment annually. Training courses on information security are distributed annually and are compulsory for continued employment.

C. Controls

1. Logical and Physical Access Controls

a. Remote access to the hosted environment through the corporate network is restricted to the VPN which also employs WIKID two-factor authentication. Accounts are reviewed and approved according to the Kollective Least Privilege policy.

b. Administrative level access is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.

c. All access (Administrative & Non-Administrative) is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.

d. Kollective administrative and general user account passwords have the following password parameters:

- Minimum eight (8) characters in length and require an alphanumeric combination.
- Passwords are set with a 90-day expiration date.
- History: five (5) remembered passwords
- Auto-lockout: 30 minutes
- Auto-lockout after five (5) logon attempts

e. Kollective IT performs periodic network testing using penetration and vulnerability assessment tools (e.g. Qualys.). The results of these reviews are summarized in a report by Kollective IT and presented to management.

f. All administrative access to servers and network devices must be approved by Operations Management.

g. HR provides termination notices to IT. Upon receipt of this notification, IT terminates the account on the date of termination or within one day of receipt of the notice.

h. Systems are configured to require a separate user ID and password.

i. Kollective's employees are required by policy to periodically change their passwords and select passwords that are at least 8 characters and include a combination of alphabetic and non-alphabetic characters.

j. Access to the Equinix data centers is only accessible to authorized Operations personnel.

k. Data transmission between the user organizations and Kollective is protected against disclosure to third parties utilizing appropriate security protocols (e.g. SSL, TLS, etc.).

l. Kollective policies require the encryption of sensitive information during transmission over public networks and business data at rest.

m. Backup data is encrypted during creation.

n. McAfee virus protection receives automatic virus definition updates. Uploaded content is

scanned during the upload process via a command line scanner before the content can be stored on the Linux server. Nightly, content servers are scanned for viruses. Scan vendor may differ based on environment.

o. Incidents are followed up on by Security Response Team as needed and documented in an email with the appropriate parties being notified.

2. Systems Operations Controls

a. Full backups of the KDMS database are done on a daily basis. IT monitors the backup completion. Issues or anomalies are investigated and resolved to ensure a full backup is successfully achieved.

b. Annually a test of restores is performed to ensure that data can be restored from backups if needed.

c. Kollective IT performs periodic network testing using penetration and vulnerability assessment tools (e.g. Qualys.). The results of these reviews are summarized in a report by Kollective IT and presented to management.

d. Operations personnel follow defined protocols for evaluating reported events. Security related events are assigned to the security group for evaluation.

e. For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.

3. Change Management Controls

a. Management performs a review of operating system software, network configuration and database software to ensure configuration settings and patch levels are in compliance with the Corporate minimum security baselines and that out-of- compliance configurations are corrected appropriately.

b. Emergency changes must obtain Operational Certification and reviewed by operations management.

c. Changes are reviewed at the weekly release management meeting and scheduled for production to migration.

d. The appropriate requestor, business owners, or project sponsor reviews and approves changes prior to introduction into the production environment. Approvals for release into production are based upon Quality Assurance (QA) certification and are also captured in the weekly release management meeting.

e. Separate environments are used for development, testing, and production.

f. Developers do not have the ability to make changes to software in production.

4. Availability Control

a. Processing capacity is monitored on an ongoing basis. Issues or anomalies are investigated and resolved to ensure a predetermined capacity levels are successfully maintained.

b. Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available.

c. Business continuity and disaster recovery plans, including restoration of backups, are updated and tested annually.

5. **Confidentiality Controls**
   - **a.** Information Security Policy contains explicit language that does grant Kollective access and use of confidential information in a controlled manner.
   - **b.** Application code restricts the ability to access, modify, and delete client data to only authorized individuals.
   - **c.** Policies and procedures are in place to restrict sharing of confidential client information with vendors or other third parties.
   - **d.** Management is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to users, related parties, and vendors.
   - **e.** Kollective has a documented data retention policy and has automated processes in place to retain and dispose of information in accordance with those policies.

6. **Monitoring of Controls**
   - **a.** Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.

7. **Rick Management and Design and Implementation Controls**
   - **a.** Kollective has a defined risk acceptance policy that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Identified risks are rated using a risk ranking, and Kollective develops risk mitigation strategies to manage the impact of those risks.
   - **b.** On a quarterly basis, management performs a risk assessment to identify and rate key threats and risks.

8. **Communications Controls**
   - **a.** Kollective has defined user security commitments that are available to Kollective's internal and external users via intranet. Kollective has also established a Security and Compliance Overview document highlighting Kollective's security commitments that is shared with external users at the time of registration.
   - **b.** Kollective's security, availability, and confidentiality commitments and related responsibilities, including management, operational, and technical controls; the incident management process; how to contact the Company with inquiries, complaints, and disputes; customer responsibilities; and legal requirements, are communicated to customers through contracts, service level agreements, terms of service and other documentation which are communicated to every customer during initial onboarding or are made available on Kollective sites and audit reports.

9. **Organization and Management Controls**
   - **a.** Management establishes training plans and requirements for continued training for its employees.
   - **b.** Personnel are required to read and accept the Employee Handbook which contains the Business Ethics and code of conduct and the statement of confidentiality and privacy practices upon their hire.
   - **c.** Personnel must pass a criminal background check before they may be hired by Kollective.

d. Employees are required to attend security, availability, and confidentiality training during the onboarding process. They are required to read and accept the Kollective's security, availability, and confidentiality commitments upon hire.

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2, on behalf of the data importer:

Signature:

Brock Beckner
Data Protection Officer