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 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 below. Controller may find a mechanism to subscribe to notifications here https://kollective.com/customer-opt-in for new sub-processors 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 above;
(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
- 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

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- United Kingdom
- Kollective Technology PTE LTD- Singapore
- Kollective Technology Pty Ltd- Australia
- Kollective Technology GK- Japan
- Kollective Technology (KT) GmbH- Germany

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:

- State of the art
- Implementation costs
- The nature, scope, context and purposes of processing
- The likelihood and severity of risks of the processing for data subjects
- 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:

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

B. Overview

1. Pseudonymization and Encryption of Personal Data

- Kollective does not perform pseudonymization.
- 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

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

- Administrative level access is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.
- All access (Administrative & Non-Administrative) is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.
- Kollective Technology administrative and general user account passwords have the following password parameters:
    i. Minimum eight (8) characters in length and require an alphanumeric combination.
    ii. Passwords are set with a 90-day expiration date.
    iii. History: five (5) remembered passwords
    iv. Auto-lockout: 30 minutes
    v. Auto-lockout after five (5) logon attempts
-
- 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.
- All administrative access to servers and network devices must be approved by Operations Management.
- 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.
- Systems are configured to require a separate user ID and password.
- 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.
- 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.).
- Kollective policies require the encryption of sensitive information during transmission over public networks and business data at rest.
- Backup data is encrypted during creation.
- 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

- Weekly full-system and daily incremental backups are performed using an automated system. Issues or anomalies are investigated and resolved to ensure a full backup is successfully achieved.
- Annually a test of restores is performed to ensure that data can be restored from backups if needed.
- 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.
- Operations personnel follow defined protocols for evaluating reported events. Security related events are assigned to the security group for evaluation.
- 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

- 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.

- Emergency changes must be approved by authorized personnel.
- Changes are reviewed at the weekly release management meeting and scheduled for production to migration.
- 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.
- Separate environments are used for development, testing, and production.
- Developers do not have the ability to make changes to software in production.

4. Availability Control

- Processing capacity is monitored on an ongoing basis. Issues or anomalies are investigated and resolved to ensure a predetermined capacity levels are successfully maintained.
- 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.
- Business continuity and disaster recovery plans, including restoration of backups, are updated and tested annually.

5. Confidentiality Controls

- The ISP contains explicit language that does grant Kollective access and use of confidential information in a controlled manner.
- Application code restricts the ability to access, modify, and delete client data to only authorized individuals.
- Policies and procedures are in place to restrict sharing of confidential client information with vendors or other third parties.
- 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.
- 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

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

7. Risk Management and Design and Implementation Controls

- 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.
- On a quarterly basis, management performs a risk assessment to identify and rate key threats and risks.

8. Communications Controls

- 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.
- 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

- Management establishes training plans and requirements for continued training for its employees.
- 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.
- Personnel must pass a criminal background check before they may be hired by Kollective.
- 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

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[(1)] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2**Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[(2)] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9**Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(2) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 daysin advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(a) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(b) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(c) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(d) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data

management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Exhibit 1A: ANNEX I

Annex I to the Standard Contractual Clauses

For purposes of this Annex I, "personal data" shall include Buyer Personal Information.

A. **LIST OF PARTIES**

A-1. Module Selection

Check which option(s) applies	
	MODULE ONE: Transfer controller to controller
X	**MODULE TWO: Transfer controller to processor**
	MODULE THREE: Transfer processor to processor
	MODULE FOUR: Transfer processor to controller

A-2. Data exporter(s):

Company Name	
Company Address	
Company Role (Controller or Processor or Both)	Controller
Contact Person Name	
Contact Person Position/Title	DPO
Contact Person Email and/or Telephone Number	
Description of the activities relevant to the data transferred by this company	Digital content delivery network infrastructure
Name of person signing (does not need to be the contact)	
Title of person signing	DPO
Signature	
Signature date	

A-3. Data importer(s):

Company Name	Kollective Technology, Inc.
Company Address	549 NW York Drive, Suite 260, Bend, OR 97703 USA
Company Role (Controller or Processor or Both)	Processor
Contact Person Name	Brock Beckner
Contact Person Position/Title	Data Processing Officer
Contact Person Email and/or Telephone Number	bbeckner@kollective.com
Description of the activities relevant to the data transferred by this company	Digital content delivery network infrastructure
Name of person signing (does not need to be the contact)	Brock Beckner
Title of person signing	DPO
Signature	
Signature date	

B. **DESCRIPTION OF TRANSFER**

B-1. Categories of data subjects whose personal data is transferred

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

- Controller's employees and contractors

B-2. Categories of personal data transferred

The personal data transferred concern the following categories of data:

- Full name
- Email address
- IP address
- Username

B-3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for

onward transfers or additional security measures.

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

None

B-4. The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

The frequency will be on an as-needed basis to support the work under the Agreement.

B-5. Nature of the processing

The nature of the Services being provided are set forth in the Agreement and any Statement of Work executed pursuant to, or Order issued under, the Agreement. The data importer will only process personal data for the purpose of providing those Services.

B-6. Purpose(s) of the data transfer and further processing

The data importers are service providers for customer. They will Process the data only to provide the Services under the Agreement.

B-7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data shall be retained only so long as required to perform the Services under the Agreement and/or any Statement of Work executed pursuant to, or Order issued under, the Agreement.

B-8. For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

Any transfers to sub-processors will be consistent with the terms of the Standard Contractual Clauses, the Section of the Terms and Conditions entitled "Data Privacy", and this Annex I.

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13:

Member State in which the relevant data exporter is established, which for the purposes of the Agreement will be considered the law of establishment of the relevant data controller.

Exhibit 1B: ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer undertakes to institute and maintain physical, technical, and organizational security measures in order to maintain and to protect the security of personal data created, collected, received, or otherwise obtained in connection with the Agreement, and the processing operations provided thereunder, which measures are required for the processing of personal data in accordance with the relevant data protection laws in the European Union.

The technical and organisational security measures of the data importer shall include, as a minimum, the following (as may be updated from time to time).

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:

- State of the art
- Implementation costs
- The nature, scope, context and purposes of processing
- The likelihood and severity of risks of the processing for data subjects
- 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:

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

B. Overview

1. Pseudonymization and Encryption of Personal Data

- Kollective does not perform pseudonymization.
- 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

- Remote access to the hosted environment through the corporate network is restricted to the VPN which also employs Pulse multi-factor authentication. Accounts are reviewed and approved according to the Kollective Least Privilege policy.
- Administrative level access is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.
- All access (Administrative & Non-Administrative) is reviewed at the quarterly meeting to determine whether access remains commensurate with job responsibilities.
- Kollective Technology administrative and general user account passwords have the following password parameters:
    i. Minimum eight (8) characters in length and require an alphanumeric combination.
    ii. Passwords are set with a 90-day expiration date.
    iii. History: five (5) remembered passwords
    iv. Auto-lockout: 30 minutes
    v. Auto-lockout after five (5) logon attempts
-
- 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.
- All administrative access to servers and network devices must be approved by Operations Management.
- 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.
- Systems are configured to require a separate user ID and password.
- 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.
- 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.).
- Kollective policies require the encryption of sensitive information during transmission over public networks and business data at rest.
- Backup data is encrypted during creation.
- 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

- Weekly full-system and daily incremental backups are performed using an automated system. Issues or anomalies are investigated and resolved to ensure a full backup is successfully achieved.
- Annually a test of restores is performed to ensure that data can be restored from

backups if needed.

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

- 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.
- Emergency changes must be approved by authorized personnel.
- Changes are reviewed at the weekly release management meeting and scheduled for production to migration.
- 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.
- Separate environments are used for development, testing, and production.
- Developers do not have the ability to make changes to software in production.

4. Availability Control

- Processing capacity is monitored on an ongoing basis. Issues or anomalies are investigated and resolved to ensure a predetermined capacity levels are successfully maintained.
- 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.
- Business continuity and disaster recovery plans, including restoration of backups, are updated and tested annually.

5. Confidentiality Controls

- The ISP contains explicit language that does grant Kollective access and use of confidential information in a controlled manner.
- Application code restricts the ability to access, modify, and delete client data to only authorized individuals.
- Policies and procedures are in place to restrict sharing of confidential client information with vendors or other third parties.
- 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.
- 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

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

7. Risk Management and Design and Implementation Controls

- 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.
- On a quarterly basis, management performs a risk assessment to identify and rate key threats and risks.

8. Communications Controls

- 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.
- 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

- Management establishes training plans and requirements for continued training for its employees.
- 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.
- Personnel must pass a criminal background check before they may be hired by Kollective.
- 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.

Exhibit 1C: ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorization of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following 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

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2, on behalf of the Data Importer:

Signature:

Brock Beckner

Data Protection Officer