ICONIK – DATA PROCESSING AGREEMENT

1. INTRODUCTION AND OBJECTIVE

1.1. The Customer and Supplier have entered into an agreement (the "**Main Agreement**") whereby Supplier shall provide services to the Customer, This Appendix 1 – Data Processing Agreement ("**Processor Agreement**" or "**Data Processor Agreement**") forms part of the Main Agreement and governs the processing of Personal Data in connection with the Main Agreement. Except as may be otherwise required under Data Protection Laws, Customer, on behalf of any other Controller (e.g., where applicable, companies within its company group or other Controllers designated by Customer and as may be agreed by Supplier in writing from time to time), shall serve as a single point of contact for Supplier in all matters under this Data Processor Agreement and shall be responsible for the internal coordination, review and submission of instructions or requests to Supplier as well as the onward distribution of any information, notifications and reports provided by Supplier hereunder.

1.2. Unless stipulated otherwise, the provisions of the Data Processor Agreement shall take precedence over the provisions of the Main Agreement.

1.3. This Data Processor Agreement is entered pursuant to the Data Protection Laws' requirement that there shall be a written agreement on the Processor's Processing of Personal Data on behalf of the Controller. This Data Processor Agreement also governs the technical and organisational measures that the Supplier and its potential Subcontractors are to implement and maintain for the protection of Personal Data.

1.4. This Data Processor Agreement is valid for as long as the Main Agreement is in force between the parties, and thus terminates when the Main Agreement ends unless the parties have agreed otherwise.

2. DEFINITIONS

2.1. "**Customer**" means the entity that has entered into a contract with the Supplier and is defined as the "customer" in the Main Agreement. The Customer shall, for the purpose of this Processor Agreement, include, where applicable, also entities within the Customer´s group of companies.

2.2. "**Controller**" means the party that determines the purposes and means of processing Personal Data, acting alone or with others.

2.3. "**Processor**" means the party that processes personal data on the Controller's behalf.

2.4. "**Data Protection Laws**" means the applicable laws that aim at protecting the fundamental rights and freedoms of individuals, and specifically their privacy. They include the Customer's national legislation and Regulation (EU) 2016/679 of the European Parliament and of the Council ("**GDPR**")").

2.5. "**Data Subject**" means an identified or identifiable natural person, as defined under the Data Protection Laws.

2.6. **"Instruction"** means written instructions for the processing of personal data by the Customer. Such instructions are provided in this Data Processor Agreement but may be updated or modified from time to time by separate written instructions from the Customer.

2.7. "**Personal Data**" means any piece of information that refers to an identified or identifiable natural person, as defined under the Data Protection Laws.

2.8. "**Processing**" means an action or combination of actions concerning personal data, as defined in the Data Protection Laws.

2.9. "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data that is Processed under the Main Agreement.

2.10. "**Subcontractor**" means any third party which the Processor engages to carry out its obligations under the Main Agreement and/or this Data Processor Agreement in accordance with Section 6, and which through this engagement Processes Personal Data for which the Customer is the Controller.

2.11. "**Supplier**" is iconik Media AB (corporate reg. no. 559208-7695), C/O: Cantemo AB, P.O. Box 45001, SE-104 30 Stockholm, Sweden.

2.12. **"Transfer"** means a cross-border transfer of Personal Data to territories outside the EU in accordance with Section 11.

3. PROCESSING OF PERSONAL DATA

3.1. **Purpose and categories of Processing and types of data processed.** The nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects covered under this Data Processor Agreement are specified in Appendix 1.

3.2. **Controller**. Without affecting any of the foregoing, the Customer is the Controller for all information that the Customer shares with the Supplier for the Processing of Personal Data under the Main Agreement and this Processor Agreement. The Customer is responsible for ensuring that the Personal Data is collected legally, and for the accuracy and quality of the Personal Data. The Customer holds all rights to the Customer's Data and the Supplier receives no rights to the Customer's Data.

3.3. **Processor.** The Supplier and its Subcontractors are Processors for the Processing of Personal Data under the Main Agreement and shall only process Personal Data on behalf of the Customer and in accordance with the Customer's Instructions. The Supplier is responsible for ensuring that Subcontractors that it engages only Process Personal Data in accordance with the Data Processor Agreement and the Data Protection Laws.

3.4. **Instructions.** The Customer is responsible for giving the Supplier Instructions for the Processing of Personal Data. The Supplier shall only manage the Customer's Personal Data in accordance with this Data Processor Agreement and Instructions given by the Customer from time to time. If the Supplier deems that an instruction is contrary to the requirements of the Data Protection Laws, the Supplier shall notify the Customer thereof without delay. The Supplier shall for the avoidance of doubt not be obliged to perform a certain measure if it is evident, according to the Supplier´s reasonable assessment, that it would result in a breach of Data Protection Laws. The Supplier shall however not be obliged to perform own investigations or surveys in order to establish whether there is a breach or not, or whether the Instructions comply with applicable laws or not.

3.5. The Controller's original Instructions to the Processor regarding the object and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of data subjects are listed in this Data Processor Agreement and in Appendix 1.

3.6. **Remuneration.** The Supplier is entitled to remuneration on a time and material basis for any added work caused by new instructions given by the Customer (or additional work otherwise caused) pursuant to section 3.4 or other added work not expressly undertaken by the Supplier herein.

4. SUPPLIER'S PERSONNEL

4.1. **Confidentiality.** The Supplier is responsible for ensuring that Supplier's and its Subcontractors' personnel who Process Personal Data for which the Customer is the Controller shall maintain secrecy, have received suitable training on Personal Data and are bound by non-disclosure agreements. The obligation of confidentiality shall remain in force even after this Data Processor Agreement has otherwise cease to be in force. Otherwise, what is stated in the Main Agreement shall apply to the Supplier's obligation of confidentiality.

4.2. **Restricted access.** The Supplier is responsible for ensuring that only the personnel of the Supplier and the Subcontractor who need the Personal Data to fulfil the Supplier's commitment under the Main Agreement shall have access to the Personal Data.

5. PROTECTION OF PERSONAL DATA

5.1. **Technical and organisational measures.** The Supplier shall take the technical and organisational measures for the protection of the Personal Data that are appropriate with regard to the sensitivity of the Personal Data; the particular risks that exist; existing technical capabilities and the costs of implementing the measures. The Personal Data shall be protected from any type of unauthorised Processing such as change, destruction or unauthorised access and dissemination. The Supplier, accordingly, undertakes to take all the measures stipulated in Article 32 of the GDPR. The Supplier shall be prepared to comply with a competent authority's decision on measures to comply with the Data Protection Laws' security requirements.

5.2. **Rights of the Data Subject.** The Supplier shall notify the Customer without delay if the Supplier receives a request from a Data Subject regarding his or her rights, such as information, correction or deletion of the Data Subject's Personal Data. The Supplier shall not respond to such a request without the Customer's written consent, except for the purpose of notifying the Data Subject that the request has been received and forwarded to the Customer. The Supplier shall assist and help the Customer in managing Data Subjects' inquiries and rights, unless the Supplier is prevented from doing so by law or by official decision.

5.3. The Supplier shall assist the Customer in fulfilling his or her duties as a Controller of Personal Data to respond to requests regarding the registered user's rights

5.4. **Official communications.** The Supplier shall notify the Customer without delay if a government authority contacts the Supplier regarding or pertinent to the Personal Data managed under the Main Agreement, unless bound by law not to provide such a notification. At the Customer's request, the Supplier shall, to a reasonable extent, help the Customer with such an official communication, and otherwise provide information so that the Customer is able to respond to the official communication within a reasonable period of time. The Supplier has no right to respond on the Customer's behalf or act in the Customer's Name.

5.5. **Remuneration.** The Supplier is entitled to remuneration on a time and material basis for any work performed assisting the Customer to fulfil its obligations in relation to Data Subjects and authorities regarding Data Protection.

6. SUBCONTRACTORS

6.1. **Use of Subcontractors.** The Supplier may engage Subcontractors for the Processing of Personal Data under the Main Agreement subject to what is otherwise stipulated in this Section 6, and only for the purposes specified in Appendix 1.

6.2. **Change in Subcontractor.** The Supplier has the right to terminate a Subcontractor or engage other appropriate and reliable Subcontractors, provided that the rules in Section 6 are applied. Before engaging a new Subcontractor, the Supplier shall notify the Customer in writing of the new Subcontractor, and upon receipt of the notice the Customer has a right to object to the new Subcontractor in accordance with Section 6.4.

6.3. **Contractual obligation.** The Supplier is responsible for ensuring that all Processing of Personal Data performed by a Subcontractor is governed by a written agreement with the Subcontractor that corresponds to the requirements of this Data Processor Agreement.

6.4. **Objections.** If Customer has cause to object to any Subcontractor, the Customer shall notify the Supplier of this in writing. If the Customer wishes to exercise its right under Section 6.2 to object to a proposed new Subcontractor, the Customer shall notify the Supplier in writing within ten (10) days of receipt of the Supplier's notice in writing.

6.5. **Resolution of objections.** In the event that the Customer has objected to a Subcontractor in accordance with Section 6.4 above, the parties shall discuss various activities to resolve the reason for the Customer's objection together. If the parties cannot agree on any solution within a reasonable period of time, which shall not exceed thirty (30) days, the Customer may terminate the Main Agreement and this Processor Agreement by notifying the Supplier in writing. The Supplier is under no obligation to refund any payments made in advance for the agreed services under the Main Agreement.

6.6. **Supplier's responsibility.** The Supplier is responsible for the Subcontractor's Processing of Personal Data under the Main Agreement and is fully responsible for Subcontractors who do not fulfil their obligations according to the Data Processor Agreement.

6.7. **List of Subcontractors.** The Supplier shall maintain a list of all Subcontractors who process Personal Data in connection with the Main Agreement and shall send a copy of the list upon the Customer's request. The Subcontractors currently appointed are listed in Appendix 1.

7. AUDITS

7.1. **Customer's right to perform an audit.** The Supplier shall provide the Customer and Customer's independent auditors with access to such information and Supplier's premises as may reasonably be necessary for the Customer to be able to verify that the Supplier is fulfilling its obligations according to this Data Processor Agreement.

The Customer shall, within a reasonable period of time (at least thirty (30) days), notify the Supplier before such an audit unless otherwise required by a government authority, or the Customer has reason to suspect that the Supplier or a Subcontractor is not fulfilling its obligations according to the Data Processor Agreement. The Customer and any persons conducting an audit, must enter into adequate confidentiality undertakings prior to such audit and must furthermore adhere to the Supplier´s security requirements at the site where the audit shall be conducted. The audit must furthermore, in so far as possible, be conducted so as not to disturb the Supplier´s business operations or jeopardise the security of information belonging to other customers. Notwithstanding the foregoing, the Customer will primarily rely on applicable existing audit reports or other available verification, if any, to confirm the Supplier's compliance hereunder and to avoid unnecessary repetitive audits; unless required by Data Protection Laws, audits will not be made more than once in any twelve-month period. An audit shall not grant the Customer access to trade secrets or proprietary information unless required to comply with Data Protection Laws (and the Supplier will never be obliged, with regard to any information request or audit, to provide access to any price or other commercial information.

7.2. **Audit results.** If an audit has shown that the Supplier or a Subcontractor has not fulfilled its obligations according to the Data Processor Agreement, the Supplier shall promptly

manage and correct this. Such corrective action does not affect the Customer's other possible claims and rights under the Data Processor Agreement.

7.3. **Remuneration.** The Supplier is entitled to remuneration on a time and material basis for any work performed assisting the Customer in performing an audit.

8. INCIDENTS AND NOTIFICATION OF SECURITY BREACHES

8.1. **Incident management.** The Supplier shall evaluate and act upon events suspected of possibly resulting in unauthorised access or Processing of Personal Data ("**Incidents**"). If there is a risk that the Incident may lead to unplanned or illegal deletion, loss, alteration or release to unauthorised persons, the Supplier shall promptly notify the Customer of the Incident and provide all relevant information related to the Incident. The Supplier shall develop appropriate steps to manage the Incident and cooperate with the Customer when appropriate to protect the Personal Data, with the aim of restoring the confidentiality, privacy and availability of the Personal Data.

8.2. **Security Breach.** The Supplier shall promptly notify the Customer and confirm that the notification was received as soon as a Security breach is discovered that could pose or could have posed a risk to the Personal Data Processed under this Data Processor Agreement. The Supplier shall promptly investigate the Security Breach and take measures to reduce the damage, identify the basic problem and prevent it from happening again. The Customer shall be updated with relevant information related to the Security Breach and the Supplier's work on the breach while the work is proceeding, and the Supplier shall cooperate with the Customer when appropriate to reduce the damage and protect the privacy of the Data Subjects.

9. RETURN AND DELETION OF PERSONAL DATA

9.1. **Return and deletion.** Within thirty (30) days of expiration of the Main Agreement, the Supplier shall delete all Personal Data that the Supplier Processed under this Data Processor Agreement, including Personal Data managed in backups and the like. Before deletion, the Supplier shall return all Personal Data that the Supplier Processed under the Data Processor Agreement upon the Customer's request.

10. LIABILITY AND LIMITATION OF LIABILITY

10.1. **Damages and penalties.** The Supplier is only liable for claims and damages from a Data Subject or a third party and administrative penalties from an authority targeting the Customer or otherwise, where the Supplier or a Subcontractor fails to fulfil its obligations according to the Data Processor Agreement and relevant Data Protection Laws.

The Customer shall indemnify the Supplier with respect to any claims and damages from a Data Subject or a third party and administrative penalties from an authority caused by the Customer.

10.2. **Limitation of liability.** The Supplier's aggregate liability under this Data Processor Agreement shall under no circumstances exceed fifty (50) per cent of the remuneration received under the Main Agreement during a period of twelve (12) months immediately preceding the occurrence of the event upon which liability is based.

11. TRANSFER OF PERSONAL DATA

11.1. The Processing activities (including storage) shall take place as set out herein (including by Subcontractors as set out in Appendix 1). It is acknowledged that the Supplier, either itself or using Subcontractors, as part of the services, need to perform services from locations in countries and territories outside the EEA. In case of such performance, then the Customer (for its own part and on behalf of other Controllers referenced herein being established in the EEA) will give its specific written consent, mandate, authorization and instruction to the Supplier for the purposes of conducting transfers outside EEA when providing the services under the Main Agreement from locations outside the EEA, as set forth below.

11.2. The Supplier or its Subcontractors may Process Personal Data outside the EU/EEA only if:

a) The recipient has been deemed by the EU Commission to guarantee an adequate level of protection of the Personal Data (e.g. through certification under the Privacy Shield arrangement, or any such subsequent framework or arrangement), or;

b) The Supplier or its Subcontractor has provided appropriate safeguards pursuant to article 46 of the GDPR, or;

c) The transfer and rights and freedoms of the data subjects are protected through approved Binding Corporate Rules pursuant to Article 47 of the GDPR, or;

d) The transfer and rights and freedoms of the data subjects are protected through the Commission's Standard Contractual Clauses.

APPENDIX 1

1. DATA SUBJECTS

The processing of personal data under the Data Processor Agreement applies to the following categories of data subjects:

- The authorised users of the Customer who access the service.
- Identifiable persons in Video, Images or other media files.

2. CATEGORIES OF PROCESSED DATA

- Users email
- Users first name
- Users last name (Optional)
- Users phone number (Optional)
- Users photo (Optional)
- Users group membership
- Video, sound, images and other personal data pertaining to identifiable persons in Customer´s media files
- IP addresses

3. PURPOSE, NATURE, OBJECTIVE AND DURATION OF THE PROCESSING

The Customer is the party that decides on the purpose of the Processing of Personal Data under the Main Agreement. The purpose of the Processing of Personal Data by the Supplier is limited to

a) Providing the agreed services such as the provision of software services, consulting services, maintenance, support and other services in accordance with the Main Agreement;

b) Implementing, managing and monitoring any underlying infrastructure required to provide services under the Main Agreement and to fulfil the stipulated technical and organisational requirements for the protection of Personal Data;

c) Communicating with the Customer and Customer's personnel;

d) Implement the Customer's Instructions in accordance with Section 3.4; and

e) Handling service problems, Incidents or Security Breaches.

f) The Supplier is entitled to use information about the use of the services for business development purposes or for example, but not limited to, providing benchmarking information or other value adding features that can be included in the services. However, the Supplier is bound to only show aggregated, unidentifiable information that can't be attributed to an individual Customer or individual User. The Customer is entitled to not include their data in such value adding features but will then not be able to use such functions.

The duration of the Processing is limited to the duration of the Main Agreement.

4. TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

We operate a global infrastructure and process data in both EU and US-based servers certified under Privacy Shield. We comply with regulations for safeguarding any transfers of personal data outside of the EU.

5. LIST OF SUB-CONTRACTORS

SUBCONTRACTOR	COUNTRY OF JURISDICTION	BRIEF DESCRIPTION OF PROCESSING
GOOGLE IRELAND LIMITED	Ireland	Google Cloud Platform is where the core Service is hosted. Google Analytics is used to track web analytics. Google Video Intelligence is the default image and video analytics service in iconik.
TWILIO, INC.	United States	SendGrid (sendgrid.com) is used to send emails on various Service notifications to users
FUNCTIONAL SOFTWARE, INC.	United States	Sentry (sentry.io) is used for monitoring and error tracking
STRIPE PAYMENTS EUROPE, LTD.	Ireland	Stripe is used to provide services for managing billing, credit card information, and invoicing. No credit card information is stored in the iconik service.
REV.COM, INC.	United States	The default transcription service in iconik.
ZOHO CORP.	United States	All customer support is done through Zoho.

APPENDIX 2 – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. TECHNICAL AND ORGANISATIONAL MEASURES - GENERAL; ENCRYPTION

Supplier shall take the technical and organisational measures for the protection of the personal data that are appropriate with regard to the sensitivity of the personal data; the particular risks that exist; existing technical capabilities and the costs of implementing the measures. The personal data shall be protected from any type of unauthorized processing such as change, destruction or unauthorised access and dissemination. Supplier, accordingly, undertakes to take all measures stipulated in Article 32 of the GDPR. The technical and organisational measures we have implemented are summarized below.

Encryption

Encryption is a major component to help ensure the authenticity, integrity, and privacy of data at rest (Assets, Data, Logs) and in transit (Access, Assets, Email). iconik will comply with the following requirements:

Access

iconik forces using HTTPS, HTTP2 or WSS. No authenticated connection is allowed via HTTP or WS protocols.

iconik only uses TLS or QUIC.

All external network communication is encrypted.

We have audited the details such as the certificates we use and their effectiveness and that they conform to the latest standards and that we use TLS 1.2 or better.

Assets

All assets that are stored in iconik provided storage are secured and encrypted using AES-256 and are transferred using either HTTPS or QUIC Protocol.

When viewing or transferring assets iconik used time limited signed URLS which are created on request, making sure the requestor is authenticated, has the correct roles and permissions to access or upload the file being requested.

iconik's internal access to assets is authenticated internally and uses TLS.

Data

All personal data is stored with Encryption at Rest. Our internal databases and search services are backed with SSD drives with AES-256 with integrity and replicated across multiple devices.

We do not store credit card or sensitive billing information internally, instead using Stripe to perform these services.

All data stored in the iconik-managed domain is backed up to separate geographical locations and stored on encrypted storage. We backup the database, Elasticsearch, and all media (originals, proxies, and keyframes) stored in the iconik-managed storages. All backups are remove after 30 days.

Logs

Logs are stored and secured in buckets with AES-256 encryption. Logs are anonymised and stored for 30 days to be able to detect any anomalies.

Email

All outbound email from iconik is sent securely to a third-party email service using HTTPS. When sharing assets to external parties, an email will be sent which contains a limited access key
which gives the sharing recipient access to that asset or collection of assets. Due to the nature of email this key can be sent in clear-text when the email is passed between email servers. This is outside of iconik's control.

Bring your own bucket

When you add your own Storage bucket to iconik it is your responsibility to make sure that the storage meets your security needs. To make your storage more secure we recommend following the security guidelines in our knowledge base.

2. SECURITY CONTROLS

iconik will comply with the following requirements to provide control over your media, by whom it's accessed and how it's accessed.

Roles

Every access to APIs and the GUI is enabled by Roles enabled on User Groups. You can define exactly what actions different groups are allowed to perform and this is enforced both on the Web-GUI level and via the APIs that the Web-GUI and third-parties can use.

ACLS

All content and collection of content is controlled by Access Control Lists defining exactly which users and groups of users are allowed access to what assets, and what access level they are allowed.

External Sharing

Users with the role to share out content can define what is shared, how long it is shared for and what access the external user has when sharing. External Sharing can be disabled for iconik with Admin Settings.

Support Access

By default, iconik support personnel can access your system domain on your behalf in order to provide support. You can enable and disable iconik support's access to your iconik account giving us access when needed to identify problems.

API

All API requests are authenticated using App-ID and Token pairs which allows each API client to use a separate set of authentication tokens.

3. HYBRID SECURITY

In Hybrid Cloud models, the iconik Storage Gateway (ISG) is deployed onto on premise networks.

ISG is responsible for managing files and storage for iconik. No communication or control can be instigated from iconik to ISG and all communication is instigated from the ISG up to iconik. This means that ISG does not have to be open from the outside world whilst living on your network.

Firewalling

The ISG can be firewalled so that no incoming connection can be established. It only needs outbound HTTPS port 443 open for communicating with the iconik Cloud Service.

VPNs

No VPNs are needed in the standard security model for iconik.

4. NETWORK SECURITY

iconik operates its network in a secure manner on top of Global Cloud leaders such as Amazon AWS and Google Cloud building upon their best practices. This provides it with Denial of Service Protection, and best in class operational and physical security.

Intrusion Detection

The iconik network is built upon sophisticated intrusion detection from our cloud suppliers that use Machine Intelligence and proactive support for monitoring and responding to intrusion attempts.

Secure Access

We limit all access to iconik production environments internally to the engineers that need access from a secure environment using two-factor authentication, access controls and secure accounts using application level access management. The internal networks at the iconik office have no access to any iconik production environments.

iconik testing environments and other environments are separated from the main production environments by accounts, location and access control and network configuration.

Logging

iconik logs all API calls and all operations performed on iconik for internal auditing processes into secured logging environments. The same Encryption at Rest is applied to log files as other files and data on iconik.

Auditing

iconik uses the services of a third-party company to perform tests to independently audit its security.

This text was last updated 29 June 2020