ICONIK – DATA PROCESSING AGREEMENT

1. INTRODUCTION AND OBJECTIVE

1.1. The Customer and the 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**", "**Data Processor Agreement**" or "**Data Processing 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, the Customer, on behalf of any other Controller (e.g., where applicable, companies within its company group or other Controllers designated by the Customer and as may be agreed by the Supplier in writing from time to time), shall serve as a single point of contact for the 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 the Supplier as well as the onward distribution of any information, notifications and reports provided by the Supplier hereunder.

1.2. Unless stipulated otherwise, the provisions of the Data Processor Agreement shall take precedence over the provisions of the Main Agreement. In the event of a conflict between the Standard Contractual Clauses (as defined below, as applicable) and the UK GDPR Addendum (as defined below, as applicable) on the one hand and the provisions of the Main Agreement and/or this Data Processor Agreement on the other hand, the SCCs and the UK GDPR Addendum shall prevail. In the event of conflicting terms between the UK GDPR Addendum and the SCCs, then the UK GDPR Addendum shall prevail, with respect to its scope of application.

1.3. This Data Processor Agreement is entered pursuant to the GDPRs 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. "**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, where applicable, and Regulation (EU) 2016/679 of the European Parliament and of the Council ("**GDPR**")").

2.4. “**Data Subject**” means an identified or identifiable natural person, as defined under the Data Protection Laws.

2.5. **“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.

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

2.7. “**Processing**” means an action or combination of actions concerning Personal Data, as defined in the Data Protection Laws.

2.8. “**Processor**” means the party that processes personal data on the Controller’s behalf.

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. “**Standard Contractual Clauses**” **or** “**SCCs**” means the standard contractual clauses based on the European Commission Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) or any subsequent version or amendment thereof released by the Commission (which shall automatically apply), including their Annexes, as individualised hereto in Appendix 3.

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

2.12. “**Supplier**” is the iconik company identified as such in the Main Agreement.

2.13. “**Transfer**” means a cross-border transfer of Personal Data to territories outside the EEA in accordance with Section 11.

2.14. “**UK GDPR Addendum**” means the template Addendum issued by the Information Commissioner and laid before Parliament in accordance with S119A of the Data Protection Act 2018 on 2 February 2022, as may be revised from time to time, and as individualized hereto in Appendix 3.

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 Personal Data that the Customer shares with the Supplier or which is otherwise Processed by the Processor under 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 its duties as a Controller of Personal Data to respond to requests regarding the registered user's rights pursuant to administrative procedures and measures adopted by the Supplier. The Supplier shall further render assistance to the Customer, and perform measures, as required under Article 28 (3) (a)-(h) of the GDPR.

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, unless otherwise provided under Data Protection Laws.

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 shall endeavor, where this is possible, to provide such notice not less than fourteen (14) days prior to the engagement in question. Upon receipt of such 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 a 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, then the Customer shall notify the Supplier in writing within ten (10) days of receipt of the Supplier's notice.

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. 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.** Subject to its adopted administrative procedures and quality management system, 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, upon the Customer's request, return all Personal Data that the Supplier Processed under the Data Processor Agreement.

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, either directly or via onward Transfer by the Supplier, acting itself and/or through permitted Subcontractors being non-EEA entities. The Customer (for its own part and on behalf of other Controllers referenced herein being established in the EEA) gives its general written 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, framework or other 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 Standard Contractual Clauses together with; as the case may be, as appropriate;

e) Appropriate measures having been adopted in conformity with applicable EU recommendations or guidelines (including those issued by European Data Protection Board; EDPB).

11.3. Subject to Clause 11.2 d) above and starting 27 September 2021, the Supplier will rely on the SCCs for Transfers of Personal Data to Subcontractors established in a country outside the EEA. By incorporating model contract clauses in Appendix 3 (including its Annexes I – III) into this Data Processing Agreement established between the parties, Personal Data processed by the Supplier (or its Subcontractors) is considered adequately protected when Transferred outside the EEA or to countries which are not covered by an adequacy decision pursuant to Clause 11.2 a) above. For transfers of Personal Data outside of the UK, the parties will, for adequate protection, in addition, rely on the UK Addendum, as also set out in Appendix 3.

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 or metadata.

2. CATEGORIES OF PROCESSED DATA

- Web browser User-Agent string
- User email
- User id (UUID)
- User first name
- User last name (Optional)
- User phone number (Optional)
- User photo (Optional)
- User group membership
- User type in iconik (Power, Standard, Browse, or Admin user type)
- Video, sound, images and other personal data pertaining to identifiable persons in Customer´s media files or metadata
- 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. We comply with regulations for safeguarding any transfers of personal data outside of the EU.

5. List of sub-contractors

Subcontractor	Country of Jurisdiction	Processing Jurisdiction	Brief description of processing
Iconik, Inc. Address: 450 Bedford Street, Suite 2200, Lexington, MA 02420 United States[1] privacy@iconik.io	United States	United States	See Appendix 1, 1-5.
Iconik Media AB Address: Kivra: 559208-7695, SE-106 31 Stockholm, Sweden[1] privacy@iconik.io	Sweden	Sweden	See Appendix 1, 1-5.
Google Ireland Limited Address: Gordon House, Barrow Street, Dublin 4, Ireland https://support.google.com/cloud/contact/dpo	Ireland	European Union and United States	Google Cloud Platform is where the core Service is hosted. Data is replicated between Europe and USA in real time. We use encryption and pseudonymisation to protect personal data. Google Analytics is used to track web analytics. Data is pseudonymised. Google Video Intelligence (GVI) is the default image and video analytics service in iconik. GVI is only used when a user requests analysis of a specific video file. GVI gets access to the video file but no other information about the Data Subject.
Twilio, Inc. Address: 101 Spear St Fl 1, San Francisco, CA, 94105-1580 United States support@twilio.com	United States	United States	SendGrid is used to send emails on various Service notifications to users. These notifications can contain the name of the user performing an action as well as the name and the email address of the user receiving the notification.
Functional Software, Inc. Address: 132 Hawthorne St San Francisco, CA 94107-1308 United States https://sentry.io/contact/enterprise/	United States	European Union	Sentry is used for monitoring and error tracking. All PII is removed before data is sent to Sentry.

[1] When not acting as Supplier/Processor under the Main Agreement.

Stripe Payments Europe, Ltd. Address: c/o A&L Goodbody Ifsc North Wall Quay Dublin D01 H104 Ireland dpo@stripe.com	Ireland	European Union	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. Address: 222 Kearny St, 8 Fl San Francisco, CA 94108 United States support@rev.ai	United States	United States	The default transcription service in iconik. Rev is only used when a user requests a transcription of a specific video or audio file. Rev gets access to the media file but no other information.
Zoho Corp. Address: 4141 Hacienda Drive Pleasanton, CA 94588, United States privacy@zohocorp.com	United States	United States	Customer support is done through Zoho. The information sent to Zoho includes: Customer Name, Name and email of main customer contact, Name and email of any user who contacts iconik Support, including content of any correspondence.
Mixpanel, inc. US. Address: One Front Street, 28th Floor San Francisco, CA 94111 United States compliance@mixpanel.com	United States	European Union	Product usage analytics. Information sent to Mixpanel includes: pseudonymised user id, details and timing of certain actions users take within the system, such as logging in, opening an asset or writing a comment. The purpose of this information is to help us track which features of the product are being used to be able to focus our development in those areas.
segment.io, inc. Address: Att: Data Protection Officer Segment.Io, Inc. 101 Spear Street, Fl 1 San Francisco, CA 94105 United States support@twilio.com	United States	European Union	Product usage, data processing and streaming. Segment.io is part of the same data pipeline as Mixpanel above and shares the same rationale for its use.
Amazon Web Services, Inc. Address: 410 Terry Avenue North Seattle, WA 98109-5210 Attn: AWS Legal https://aws.amazon.com/contact-us/compliance-support/	United States	European Union and United States	AWS is used to store encrypted backups of the iconik database. In case of a major and lasting outage of Google Cloud Platform, AWS may also be used to spin up temporary instances of iconik.

Crowdstrike, Inc. Address: 150 Mathilda Place, 3rd Floor Sunnyvale, CA 94086 legal@crowdstrike.com	United States	European Union and United States (all processing is done in the iconik datacenters)	Crowdstrike provides security services for iconik including real-time monitoring of our infrastructure. Crowdstrike does not process any customer data as part of its services.
Orca Security, Inc. Address: 2175 NW Raleigh St, Suite 110, Portland, OR 97210 privacy@orca.security	United States	European Union and United States (all processing is done in the same region as the iconik data)	Orca Security provides automated risk analysis and vulnerability scanning of the iconik infrastructure. Orca Security does not process any customer data as part of its service.
SFDC Ireland, Ltd. Legal Department - Level 1, Block A, Nova Atria North, Sandyford Business District, Dublin 18, Ireland privacy@salesforce.com	England	United States	Salesforce is used for sales and marketing related activities. Salesforce is given access to contact information, including name and email address for prospective and current customers.
Hubspot, Inc. Address: 25 First Street, 2nd Floor, Cambridge, MA 02141, USA https://preferences.hubspot.com/privacy	United States	United States	Hubspot is used for marketing related activities. Contact information entered into the iconik website is managed through Hubspot.
Zendesk 989 Market Street, San Francisco, California 94103 U.S.A. Attn: Legal Department legalnotice@zendesk.com	United States	United States	Customer support is done through Zendesk. The information sent to Zendesk includes: Customer Name, Name and email of main customer contact, Name and email of any user who contacts iconik Support, including content of any correspondence.

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, System 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 unencrypted 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 use 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 data in iconik 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 and geographic locations.

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 removed after 30 days.

System logs

System 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.

Role based Access Control

Every access to APIs and the User Interface 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 and data 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. We also contract with Orca Security to perform vulnerability and risk analysis of our infrastructure and Crowdstrike to perform malware and intrusion detection and prevention.

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 fully separated from the main production environments by accounts, location, access control and network connectivity.

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. Audit logs are stored for 12 months to be able to investigate security related issues.

External Auditing

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

For details on our security measures see https://app.iconik.io/help/pages/security/

This text was last updated 15 February 2023

APPENDIX 3 – Transfer of Personal Data outside the EEA and/or the UK pursuant to Clause 11.2 d) in the Data Processing Agreement

This Appendix 3 incorporates by reference the SCCs (PART A) and the UK GDPR Addendum (PART B). The SCCs and the UK GDPR Addendum have been pre-signed by iconik as the data importer. The parties agree that the SCCs and the UK GDPR Addendum shall govern any Transfers (out of the EEA) of Personal Data protected by the GDPR and/or transfers out of the UK of Personal Data protected by the UK GDPR, as and when applicable.

PART A

STANDARD CONTRACTUAL CLAUSES ("SCCs"/"EU SCCs")

The parties acknowledge and agree that the following provisions will apply with respect to Transfers of Personal Data protected by the GDPR.

COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

STANDARD CONTRACTUAL CLAUSES – Module 2: MODULE TWO:

Transfer controller to processor. The full text of the Module 2: Transfers Controller to Processor is available at: https://eurlex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en

Completed and individualised SCCs, as well as Annexes I-III to the SCCs, are provided below.

In relation to Personal Data protected by the GDPR, the SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause shall not apply;

(iii) in Clause 9, Option 2 "General Authorisation" will apply, and the time period for prior notice of sub-processor changes shall be 14 days. The Subcontractors currently appointed are listed in Appendix 1.

(iv) in Clause 11 a), the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the SCCs will be governed by Swedish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Sweden;

(vii) Annex I of the SCCs shall be deemed completed with the information set out in Annex I below; and

(viii) Annex II of the SCCs shall be deemed completed with the information set out in Annex II below.

ANNEX I TO THE SCCs

A. LIST OF PARTIES

Data Controller: For the purposes of the Standard Contract Clauses, and subject to the terms of the Data Processor Agreement, the Customer is identified as Data Controller, as defined in Data Protection Laws.

Data Processor: For the purposes of the Standard Contract Clauses, and subject to the terms of the Data Processor Agreement, the Supplier is identified as Data Processor, as defined in Data Protection Laws.

Data exporter(s): For the purposes of the Standard Contract Clauses, and subject to the terms of the Data Processor Agreement, the Customer is Data exporter. The activities relevant to the data transferred under these Clauses are set out in Appendix 1 to the Data Processor Agreement.

The Customer's / Data exporter's contact details, key contact person and signature are specified in the Main Agreement.

Data importer(s): For the purposes of the Standard Contract Clauses, and subject to the terms of the Data Processor Agreement, the Supplier is defined as Data importer. The activities relevant to the data transferred are set out in Appendix 1 to the Data Processor Agreement.

The Supplier's / Data importer's contact details, key contact person and signature are set out in the Main Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred is set out in Appendix 1 to the Data Processing Agreement between the Customer (Data Controller) and the Supplier (Data Processor).

Categories of personal data transferred is set out in Appendix 1 to the Data Processing Agreement between the Customer (Data Controller) and the Supplier (Data Processor).

No sensitive data, within the meaning of the Data Protection Laws, is known to be transferred.

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

Data is continually transferred in real-time between iconik´s data centers in EU and US.

Nature of the processing

See Appendix 1, Section 3

Purpose(s) of the data transfer and further processing

Data is transferred between EU and US in order to provide data replication and protection from natural disasters, as well as making sure the data is as close to the user as possible. Users are directed to the closest data center using our Geo-based global load-balancers.

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

Data is retained as long as the Customer has an active account and has not instructed the Supplier to delete the data via the relevant user interface or API interactions. Once data has been deleted the Supplier maintains backup copies of data for 30 days until the backup copies are automatically purged.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing: See Appendix 1, Section 5

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: the Swedish Authority for Privacy Protection (www.imy.se), unless another Member State's competent supervisory authority is identified in accordance with Clause 13.

ANNEX II TO THE SCCs - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

iconik's technical and organizational measures are set out in Appendix 2 to the Data Processing Agreement.

ANNEX III TO THE SCCs – LIST OF SUB-PROCESSORS

The Controller has authorised the use of the following sub-processors:

- Sub-processors to the Supplier: please see Appendix 1 to the Data Processor Agreement.
- Sub-processors to the Subcontractor: please refer to Appendix 1 and/or relevant sub-processor contract.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: please see Appendix 1.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing: please see Appendix 1.

PART B

UK GDPR ADDENDUM

This Addendum forms part of a Main Agreement and a Data Processing Agreement, including the Addendum EU SCCs, entered into between iconik and Customer. The Addendum applies with regard to UK GDPR (as applicable).

The Addendum conforms to the international data transfer addendum issued by the UK ICO for parties making Restricted Transfers (as defined below) and is aimed to provide Appropriate Safeguards (as also defined below) for Restricted Transfers. The Addendum is incorporated in the Data Processing Agreement and the Main Agreement. In the event of conflicting provisions among documents, the terms of the Addendum shall - subject to Part 2, clause 10, below - prevail with respect to its area of application.

Part 1: Tables

Table 1: Parties

Start date	*the effective date of the Data Processing Agreement.*	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	The parties' (Data exporter and Data importer) contact details are specified in the Main Agreement.	
Key Contact	The parties' (Data exporter and Data importer) key contact persons are specified in the Main Agreement.	
Signature (if required for the purposes of Section 2)	The parties' (Data exporter and Data importer) signatures are set out in the Main Agreement.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: The EU SCCs to which this Addendum is appended to are contained in PART A of Appendix 3 to the Data Processing Agreement. ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	*Module 2*	*Omitted*	*The optional language will not apply*	*General authorisation*	*14 days*	*Yes*
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: List of parties as set out in Annex 1A to the Approved EU SCCs.

Annex 1B: Description of Transfer: Description of transfer as set out in Annex 1B to the Approved EU SCCs.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: as set out in Annex II to the Approved EU SCCs.

Annex III: List of Sub processors (Modules 2 and 3 only): as set out in Annex III and Appendix 1 to the Data Processing Agreement.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

> “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

> “These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

> “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

The SCCs and the UK GDPR Addendum set out in this Appendix 3 will become legally binding between the parties upon entering into of the Main Agreement and the Data Processing Agreement and, in any event, Supplier’s continued Processing of the Personal Data shall constitute acceptance of the terms contained herein.

On behalf of the Customer: as per the Main Agreement
Name (written out in full): as per the Main Agreement
Position: as per the Main Agreement
Signature: as per the Main Agreement

On behalf of iconik: as per the Main Agreement
Name (written out in full): as per the Main Agreement
Position: as per the Main Agreement
Signature: as per the Main Agreement