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**" 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, 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 contradiction between the Standard Contractual Clauses (as defined below, as applicable) and the provisions of the Main Agreement and/or this Data Processor Agreement, the Standard Contractual Clauses shall prevail.

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 and attached hereto according to the template model 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 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 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 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, 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.

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: 111 Charlotte Dr. Novi, MI 48377 United States[1] iconik.io	United States	United States	See Appendix 1, 1-5.
Iconik Media AB Address: Kivra: 559208-7695, SE-106 31 Stockholm, Sweden[1] iconik.io	Sweden	Sweden	See Appendix 1, 1-5.
Google Ireland Limited Address: Gordon House, Barrow Street, Dublin 4, Ireland google.com	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 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 sentry.io	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 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 rev.com	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 zoho.com	United States	United States	All 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 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 segment.io	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 aws.amazon.com	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 Plaform, AWS may also be used to spin up temporary instances of iconik.

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 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 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.

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 and 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.

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 30 November 2021

APPENDIX 3 – Transfer of Personal Data to Subcontractors established outside the EEA pursuant to Clause 11.2 d) in the Data Processing Agreement

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) 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)

(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)

(*omitted*)

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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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)

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. 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.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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.

(d) 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.

(e) 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)

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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.

MODULE THREE: Transfer processor to processor

(a) 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.

(b) 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.

(c) 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.

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

(e) 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)

MODULE THREE: Transfer processor to processor

(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)

MODULE THREE: Transfer processor to processor

(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.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these

Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

(Local laws and practices affecting compliance with the Clauses)

MODULE THREE: Transfer processor to processor

(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;

(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). 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, 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 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)

MODULE THREE: Transfer processor to processor

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 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.

The data exporter shall forward the notification to the controller.

(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.). The data exporter shall forward the information to the controller.

(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. 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 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) 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.] 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.

(d) 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Sweden or another Member State agreed between the Supplier and the individual Subcontractor.

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 Sweden or another Member State agreed between the Supplier and the individual Subcontractor.

(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.

_____

ANNEX I – TO THE STANDARD CONTRACTUAL CLAUSES

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 Supplier's 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, and party to the Standard Contract Clauses with the individual Subcontractor.

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

The Supplier's contact details are as follows:

Please refer to contact details for the iconik company identified as the Supplier in the Main Agreement.

On behalf of Data exporter

Signature: please see the above
Name: please see the above .....

Tel: please see the above
Email: please see the above

Data importer(s): For the purposes of the Standard Contract Clauses, and subject to the terms of the Data Processor Agreement, the Supplier's individual Subcontractor acting as a subprocessor is defined as Data importer.

The individual Data importer(s) and the activities relevant to the data transferred to the individual Data importer is set out in section 5 in Appendix I to the Data Processor Agreement.

Notwithstanding the foregoing, the identify and contact details of each individual Data importer, including any contact person(s) with responsibility for data protection, is set out in the individualized Standard Contract Clauses with the relevant Subcontractor.

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). For the purposes of the Standard Contract Clauses, and subject to the terms of the Data Processor Agreement, the categories of data subjects whose personal data is transferred to the individual Data importer is defined and specified in the individualized Standard Contract Clauses with the relevant Subcontractor.

Categories of personal data transferred is set out in Appendix I to the Data Processing Agreement between the Customer (Data Controller) and the Supplier (Data Processor). For the purposes of the Standard Contract Clauses, and subject to the terms of the Data Processor Agreement, the categories of data subjects whose personal data is transferred to the individual Data importer is defined and specified in the individualized Standard Contract Clauses with the relevant Subcontractor.

Unless otherwise instructed by the Customer, the Supplier (acting as Data exporter) confirms that no sensitive data, within the meaning of the Data Protection Laws, is transferred to Subcontractors (acting as Data importer).

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 our 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 datacenter 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 the individualized Standard Contract Clauses between the Supplier and the concerned Subcontractor.

_____

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

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

See the individualized Standard Contract Clauses with the relevant Subcontractor for details on their respective technical and organizational measures.

_____

ANNEX III – LIST OF SUB-PROCESSORS

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

- Subprocessors to the Supplier: See Appendix 1 to the Data Processor Agreement.
- Subprocessors to the Subcontractor: see the individualized Standard Contract Clauses with the relevant Subcontractor.

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

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