Capture One

Data Processing Agreement

Effective as of January 15, 2024

THIS DATA PROCESSING AGREEMENT has been entered into

By and between

The customer identified in the Main Agreement	and	Capture One A/S Roskildevej 39 2000 Frederiksberg, Denmark Company reg. no.: 17 88 96 99
(the "Customer" or the "data controller")		**(the "Supplier" or the "data processor")**

(collectively referred to as the "Parties" and individually the "Party")

1. BACKGROUND AND PURPOSE OF AGREEMENT

1.1 The Parties have entered into a software license agreement (the "**Main Agreement**") about the Supplier's provision to the Customer of the Capture One desktop and/or mobile software application or service (the "**Software**") incl.

(i) a cloud-based service based on Microsoft Azure integrated into the Software called Capture One Live ("**COL**") enabling photographers to share photos e.g. from a live photo session via the internet;

(ii) a cloud-based service based on Microsoft Azure integrated into the Software called Cloud File Transfer ("**CFT**") that adds certain features to the mobile and the desktop Software, including uploading of images and their adjustments from the mobile Software to the cloud; and importing those images and their adjustments from the cloud into the desktop and/or mobile Software; and

(iii) whitelisting of users by Customer's admin

(collectively the "**Services**").

1.2 When using the Services the Customer will be acting as data controller with respect to any photos that the Customer uploads to the application, including personal data and/or any other personal information the Customer processes as part of using the Services, whereas the Supplier will be acting as data processor in this context.

1.3 Against the above background this data processing agreement (the "Agreement") has been entered into between the Parties as an integral part of the Main Agreement. By signing or accepting the Main Agreement, the Customer also accepts the terms of this Agreement.

2. PROCESSING OF PERSONAL DATA

2.1 As part of the provision of the Software and Services, the Supplier will be processing personal data on behalf of the Customer (the “Personal Data”). A specification of the type of personal data and category of data subjects processed as well as the nature and purpose of the processing specified in Appendix A to this Agreement.

2.2 With this Agreement the Parties wish to establish their respective obligations and rights in relation to the processing of Personal Data.

2.3 The Parties are mutually obliged to comply with EU data protection legislation in force at any time whenever they process personal data; i.e. currently 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 (the "GDPR") as well as any national legislation supplementing the GDPR or otherwise setting out rules on processing of personal data to the extent applicable to the Parties (jointly the ”Data Protection Legislation”).

3. THE CUSTOMER'S INSTRUCTION TO THE SUPPLIER

3.1 The Supplier is the data processor of the Personal Data which the Supplier processes for and on behalf of the Customer.

3.2 The Supplier may only process Personal Data to the extent necessary to provide the Software and Services in accordance with the Main Agreement and Appendix 1 and in accordance with any documented instruction from the Customer (the “Instruction”). The Main Agreement, together with this Agreement with appendices, set out the Instruction at the time of signing.

3.3 The Supplier must notify the Customer immediately if in the Supplier’s opinion the Instruction is in violation of the Data Protection Legislation.

3.4 Changes in or expansions of the Instruction as well as the implementation hereof must in reasonable time before the implementation be discussed by the Parties.

3.5 The Supplier may process the Personal Data beyond the Instruction if required by EU or national law to which the Supplier is subject. In case the processing of Personal Data goes beyond the Instruction, the Supplier must inform the Customer, unless prohibited from doing so by EU or national law.

3.6 The Supplier may – if necessary to document provision of services to the Customer or to defend itself against legal claims – save a copy of the Personal Data processed on behalf of the Customer. In such cases the information may only be processed for the purposes stated in this clause.

4. THE CUSTOMER’S OBLIGATIONS

4.1 The Customer is the data controller in respect of the Supplier when using the Services.

4.2 It is the Customer’s responsibility to ensure that the processing of Personal Data carried out under the Instruction has a legal basis according to the Data Protection Legislation.

4.3 It is the Customer's responsibility to fulfil the data subjects' rights according to the Data Protection Legislation. Should the Supplier receive requests from the persons concerned, the Supplier must immediately inform the Customer hereof.

(i) The Supplier must assist the Customer in fulfilling the Customer's obligations to answer requests on the exercise of the data subjects' rights, including access, rectification, restriction, erasure, objection and data portability.

(ii) The Supplier is entitled to charge the Customer for any such assistance pursuant to the agreed upon hourly rates.

5. SECURITY OF PROCESSING

5.1 The Supplier shall implement appropriate technical and organisational measures to protect the Personal Data against a) accidental or unlawful destruction, loss or alteration, b) unauthorized disclosure of, access to, misuse of, or c) other unlawful processing. The Supplier guarantees to implement the appropriate technical and organisational measures in a manner that ensures that the processing meets the requirements of the Data Protection Legislation.

5.2 At the time of signing, the Supplier has implemented the technical and organisational security measures described in Appendix B.

5.3 The Supplier must without undue delay inform the Customer of any breach of security that could potentially lead to accidental or unlawful destruction, loss, alteration, unauthorized transmission of or access to the Personal Data processed on behalf of the Customer ("Security Breach").

(i) The information must include a description of i) the nature of the Security Breach, including where possible the categories and approximate number of data subjects concerned as well as the categories of and approximate number of personal data records concerned, ii) the likely consequences of the Security Breach, and iii) the measures taken or proposed to be taken by the Supplier to alleviate the Security Breach, including if relevant measures to minimize the potential harm.

(ii) The Supplier must upon request assist the Customer in fulfilling its obligations to notify and inform the competent supervisory authority and/or data subjects.

(iii) The Supplier must, to a necessary extent and upon the Customer's request, assist the Customer in carrying out an impact assessments and prior consultation with the supervisory authority.

(iv) In case any of the activities mentioned are not, in whole or in part, caused by a breach of the Agreement by the Supplier, the Supplier may charge the Customer for such activities applying the agreed upon hourly rates.

6. DEMONSTRATION OF COMPLIANCE

6.1 The Supplier must upon the Customer's request provide the Customer with the necessary documentation enabling the Customer to ensure that the Supplier fulfils i) it's obligations according to this Agreement, and ii) the provisions of the Data Protection Legislation in force at any given time, insofar as it concerns the Personal Data processed by the Supplier on behalf of the Customer.

6.2 The Supplier must allow for the Customer's performance of an audit of the Supplier's data processing and data protection measures via a third party subject to customary confidentiality undertakings and at the Customer's cost.

(i) The audit must be carried out in accordance with recognized auditing standards in force at the given time by a competent third party.

(ii) The Supplier must grant the auditor access to the Supplier's premises and facilities to the extent necessary to perform the audit.

(iii) If the audit reveals insufficient security measures or other breaches of Data Protection Legislation on the part of the Supplier, the Supplier must take necessary steps to cure such breaches without undue delay and without any remuneration.

7. USE OF SUB-PROCESSORS

7.1 If at the time of signing the Agreement the Supplier uses sub-processors, this is specified in Appendix C. The Customer has approved that the use of these sub-processors is included in the Instruction.

7.2 The Supplier will notify the Customer of any planned additions to or replacements of any sub-processors and grant the Customer a reasonable amount of time to object to any such alterations. Updated list of sub-processors will always be available at https://www.captureone.com/en/terms-conditions/sub-processors-list and Supplier will be considered to have provided a notification on adding a new sub-processor to Customer by publishing the sub-processor's name on the said link. Customer may also opt to receive notifications of new sub-processors on the said link and if the Customer contact subscribes, the Supplier shall provide the subscriber with notification of new sub-processor(s).

7.3 If the Supplier uses a sub-processor in connection with specific processing activities on behalf of the Customer, data protection responsibilities corresponding to those stated in this Agreement must be imposed on the sub-processor, either by contract or another legal act guaranteeing in particular that the sub-processor will implement appropriate and technical measures to ensure that the processing fulfils the requirements of the Data Protection Legislation.

7.4 The Supplier remains fully responsible to the Customer for the fulfilment of the sub-processors' obligations.

8. TRANSFERS TO THIRD COUNTRIES

8.1 The Supplier may not cause or allow the transfer of Personal Data to countries outside the European Economic Area (EEA) unless such transfer is included in the Instruction or the Customer has given its prior written consent to such a transfer.

8.2 Insofar as the Customer has allowed a transfer in accordance with Section 8.1, the Supplier must ensure that there is a legal basis for the transfer according to the Data Protection Legislation.

8.3 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C of this Agreement.

8.4 If the data controller is established in a non-EEA country which has not been deemed by the EU Commission to provide adequate protection of personal data

through an adequacy decision, the parties by virtue of accepting this Data Processing Agreement agree to be bound by the Standard Contractual Clauses (SCC's) for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council – module 4 (P2C) (COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021) as attached in Appendix D of this Agreement.

9. OBLIGATION OF CONFIDENTIALITY

9.1 The Supplier must process Personal Data in confidence. The Supplier must ensure that the persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9.2 The Supplier undertakes to limit its employees' access to the Personal Data to employees for whom it is necessary to process the Personal Data in order to fulfil the Supplier's obligations.

9.3 The Supplier's responsibilities under Section 9 are not limited by nor contingent upon the Parties' continued or discontinued cooperation.

10. DURATION AND TERMINATION

10.1 This Agreement comes into effect upon the Parties' signing and is effective for the term of the Main Agreement plus the period from termination of the Main Agreement until the Supplier ceases to process Personal Data on behalf of the Customer.

10.2 In case of termination or expiration of this Agreement, regardless of the reason, the Supplier must, at the Customer's sole discretion, either delete or return to the Customer all Personal Data and delete any existing copies, unless the Data Protection Legislation prescribes storing of the Personal Data.

10.3 The Supplier is not entitled to exercise a lien in Personal Data for claims, such as payment of invoices etc., which the Supplier may have in relation to the Customer.

11. LIABILITY

11.1 The Parties are liable under the common regulations of Danish law with the limitations specified in this Section.

11.2 The Parties are not liable for indirect losses and derived damage, including operating losses that may arise in association to this Agreement. Further, the Parties' mutual liability for breach of this Agreement or any other financial claims is limited as set out in the Main Agreement. The limited responsibility in this Section 11.2 does not include losses resulting from the other Party's gross or intentional negligence.

11.3 Regardless of the above, one Party must indemnify the other Party against any claim for remuneration or compensation from third parties arising from the first mentioned Party's violation of this Agreement.

12. PRECEDENCE

12.1 In case of conflict between the Main Agreement and this Agreement's provisions on processing of Personal Data, the latter has precedence.

13. ACCEPTANCE

13.1 This Agreement is accepted as part of the entering into of the Main Agreement.

APPENDIX A

---

1. NATURE AND PURPOSE OF PROCESSING

The Supplier stores and otherwise processes personal information on behalf of the Customer, typically in the form of the Customer's images, which the Customer uploads to the Services, incl. information used to manage the Customer's License and access to the Software and Services.

The Supplier processes personal information on behalf of the Customer in order to send email invitations to Customer's customers, Customer's collaborators, and/or any person Customer decides to invite to the live session.

The Supplier processes personal information on behalf of the Customer in order to (i) whitelist Customer's employees, contractors, students and/or any other person selected by the Customer; (ii) send email invitations to Customer's employees, contractors, students and/or any other person Customer decides to whitelist in order to grant them access to the Software; (iii) inform the Customer of email addresses of Customer's employees, contractors, students and/or any other person selected by the Customer that the Supplier was not able to whitelist.

The storage and processing of the said information is done exclusively on behalf of the Customer and according to the Customer's instructions as part of making the Software and Services available to the Customer, including the provisioning of remote support and other assistance to the Customer.

2. CATEGORIES OF DATA SUBJECTS

The data subjects whose personal data is processed will depend on which files the data controller instructs Capture One to process.

The data controller may include:

- any data subject whose personal data may be included in the images, which the data controller in its own discretion chooses to disclose to the data processor or upload to the platform,
- any data subject invited by the Customer to the live session,
- any data subject that the Customer wishes to whitelist in order to grant them access to the Software,
- any data subject invited to create a Capture One account in order to be whitelisted.

3. CATEGORIES OF PERSONAL DATA

Types of personal data processed in Software and Services:

The personal data consists of photos taken by the Customer and other information about the Customer's customers, collaborators and/or any other person invited by the Customer to the live session, as well as information used to manage the Customer's License and access to the Software and Services. The personal data processed in the Services will depend on the images, the data controller edits and uploads to the Services. Types of personal data processed in connection with the provision of the services may include any personal data included in the images and other content which the data controller in its own discretion chooses to disclose to

Capture One or upload to the platform/Services. As such the personal data may include ordinary as well as special categories of data of any nature.

COL may process names, e-mail addresses, comments and/or interactions of Customer's customers, collaborators and/or any other person invited by the Customer to the live session.

Supplier may process e-mail addresses of Customer's employees, contractors, students, and/or any other person that the Customer decides to whitelist in order to grant them access to the Software.

The frequency of transferring Personal data depends on the Customer's use of the Software and Services and can be transferred both on a one-off and on a continuous basis.

4. DURATION OF PROCESSING

Supplier may process Customer data for the duration of the Agreement, unless otherwise agreed by the Parties.

The period for which Personal Data is retained depends on the Customer's use of the Software and Services.

Images and Personal Data contained therein stored in COL may be retained for up to a maximum of 30 days after the live session was initiated.

Upon termination or expiry of the Main Agreement, the Customer's account will be deleted, images and Personal Data contained therein may be retained for a period of up to 90 days, after which it will be inaccessible.

Deletion of emails sent via SendGrid services will be guided by Sendgrid's retention policy available at: Data Retention and Deletion in Twilio Products.

APPENDIX B

---

1. INTRODUCTION

This Appendix B describes security measure made by Capture One to the physical, technical and organizational security in connection with the delivery of services under the Main Agreement.

2. PHYSICAL SAFETY

2.1 Fire, power failure, flooding etc.

All production services are cloud-based or in external professional datacenter and no customer faced services will stop working if our own physical locations are hit by fire, power failure, flooding etc.

The Supplier's primary customer faced services are hosted in Microsoft Azure infrastructure with Geo Redundant Backup Plans to cover disaster recovery scenarios etc.

3. ACCESS CONTROL

All access to the Supplier's office is controlled with strictly personal digital access keys (fobs) which are also controlling burglar alarm system.

4. TECHNICAL SAFETY

4.1 Firewalls and antivirus

All the Supplier's computers have Antivirus installed to protect against virus, phishing etc.

All on-prem servers are hosted in a professional datacenter behind firewall and can only be accessed via MFA controlled VPN or from inside our corporate network.

All cloud-based infrastructure, i.e. the Supplier's Microsoft Azure tenant, are only accessible with MFA authentication integrated with our corporate authentication setup.

The Supplier's office network is based on Cisco Meraki technology and Wifi is same and integrated with corporate authentication Microsoft Azure Active Directly.

5. ENCRYPTION

All web systems handling personal data are using HTTPS encrypted protocol to transfer data between client and the Supplier's backend systems.

All internal access to customer data, i.e. customer support, tech support etc. can only happen via encrypted channels like HTTPS, VPN etc.

6. STORING OF DATA AND BACKUP

All customer data are stored in Microsoft Azure infrastructure, FastSpring payment platform and Zendesk support platform. Databases in Azure infrastructure are configured with both geo

redundancy and 30 days retention for optimal data safety.

7. ORGANISATIONAL SAFETY

7.1 Access rights

All access to the Supplier's own systems are controlled with personal logins only. No generic logins are allowed. Microsoft MFA is forced on all personal logins to our corporate systems including VPN connections. Microsoft extended security plans are activated to protect the data from phishing etc.

Access to 3rd party systems are controlled by IT and only personal logins are allowed for proper tracking of user activity.

8. CONFIDENTIALITY

All employees with access to the Supplier's IT systems are under a legal contract including confidentiality agreement regarding all company and customer data.

9. LOGGING

All employee logins are logged within the Supplier's Microsoft Azure Active Directory tenant.

10. DELETION AND DISCARDING

10.1 Storing media

All client computers and portable storage systems are formatted when no longer in use or user stops working with the Supplier.

All server-side storage and backup sets are deleted permanently when no longer in production.

11. MICROSOFT AZURE

The security measures in place on the Microsoft Azure platform are specified in the DPA with Microsoft Ireland Operations, Ltd ("**Microsoft**") which may be downloaded via the following link https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA. More information on Microsoft Azure security measures can be found via the following link https://learn.microsoft.com/en-us/azure/security/fundamentals/overview.

12. SENDGRID

The security measures in place with Sendgrid are specified in the DPA with Twilio, Inc. which may be downloaded via the following link https://www.twilio.com/en-us/legal/data-protection-addendum. More information on Sendgrid security measures can be found via the following link https://www.twilio.com/en-us/legal/security-overview.

APPENDIX C

Use of sub-processors:

At the time of entering this Agreement, the Supplier makes use of the following sub-processors:

Name	**Location**	**Purpose/scope of processing**
Microsoft Azure	*Europe and USA*	*Cloud infrastructure provider, data storage, user login analytics, application analytics and performance analytics*
MaxMind	*USA*	*Customer Identity and Access Management*
Twilio - SendGrid	*USA*	*Sending* - *service emails, invitations of collaborators/customers to Capture One Live session;* - *invitations to Customer's employees, contractors, students and/or any other person Customer decides to whitelist in order to grant them access to the Software;* - *service emails to Customer with a list of email addresses of Customer's employees, contractors, students and/or any other person selected by the Customer that the Supplier was not able to whitelist on behalf of the Customer.*

The Supplier may replace or make use of new sub-processors subject to a prior written notice to the Customer giving the Customer a reasonable time to object. Updated list of sub-processors will always be available at https://www.captureone.com/en/terms-conditions/sub-processors-list and Supplier will be considered to have provided a notification on adding a new sub-processor to Customer by publishing the sub-processor's name on the said link. Customer may also opt to receive notifications of new sub-processors on the said link.

The Customer acknowledges that personal data is being transferred to third countries as part of the processing of the Customer's data by the sub-processors. As regards transfer of personal information to any sub-processors located outside of the EU/EEA, this will be based on the Commission's Standard Contractual Clauses which the Customer therefore instructs the Supplier to enter into with any such sub-processors on the Customer's behalf.

Supplier uses additional processors when processing personal data as an independent controller. For more information about such processing, which is outside the scope of the Agreement, see the Supplier's Privacy Policy here: https://www.captureone.com/en/terms-conditions/privacy-policy.

APPENDIX D

STANDARD CONTRACTUAL CLAUSES (MODULE 4 - PROCESSOR TO CONTROLLER)

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 8.1 (b) and Clause 8.3(b);

(iii) [*Intentionally left blank*];

(iv) [*Intentionally left blank*];

(v) Clause 13;

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

(vii) Clause 16(e); and

(viii) Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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 of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

[*Intentionally left blank*].

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

Clause 12

Liability

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

Clause 13

Supervision

[*Intentionally left blank*].

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

Clause 14

Local laws and practices affecting compliance with the Clauses

[*Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU*]

Clause 15

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

[*Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU*]

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Denmark.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: Capture One A/S

Address: Roskildevej 39, 2000 Frederiksberg, Denmark

Contact person's name, position and contact details: Adriana Sefcikova, Legal & Compliance Specialist, legal@captureone.com

Data protection officer (if any) name, position and contact details:

EU representative (if any) name, position and contact details:

Activities relevant to the data transferred under these Clauses: Provision of picture editing services of pictures provided the by data importer and returning and storing of edited files to the data importer.

Signature and date:

_____

Role (controller/processor): Processor

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: Capture One's (data exporter's) customer as identified by the customer itself in the Main Agreement.

Address: -

Contact person's name, position and contact details:-

Activities relevant to the data transferred under these Clauses: Access to the data exporter's services, usage of the services of the platform and return of the edited pictures.

Signature and date:

_____

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects whose personal data is processed will depend on which files the data controller (data importer) instructs Capture One (data exporter) to process. The data subject may include any data subject whose personal data may be included in images and other content which the data controller (data importer) in its own discretion chooses to disclose to the data processor or upload to the platform.

The data subjects may include any data subject whose email address was returned to the data controller (data importer) via email as not whitelisted, thereby encompassing a broader category of data subjects whose personal data is processed through email communications between the data controller (data importer) and data processor (data exporter).

Categories of personal data transferred

The personal data processed will depend on the images, the data controller (data importer) instructs Capture One (data exporter) to process. Types of personal data processed in connection with the provision of the Services may include any personal data included in images and other content, which the data controller (data importer) in its own discretion chooses to disclose to Capture One (data exporter) or upload to the platform. As such the personal data may include ordinary as well as special categories of data of any nature.

Data processor (data exporter) may process e-mail addresses of data controller's (data importer's) employees, contractors, students, and/or any other person that the data controller (data importer) decides to whitelist in order to grant them access to the Software.

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

We refer to point above, "Categories of personal data transferred".

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

Continuous access to the data importers own images in the Services and one-off transfer (return) of the returned images; and/or email addresses of data subjects that could not be whitelisted.

Nature of the processing

Collection, storage, editing, return, and deletion.

Purpose(s) of the data transfer and further processing

The data exporter will transfer (return) to the data importer stored, processed, or otherwise edited versions of images and/or email addresses originally provided by the data importer to the data exporter.

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

Data exporter may process data importer data for the duration of the Agreement, unless otherwise agreed by the parties.

The period for which personal data is retained depends on the data importer's use of the Software and Services and can be transferred both on a one-off and on a continuous basis.

Images and personal data contained therein stored in COL may be retained for up to maximum of 30 days after the live session was initiated.

Upon termination or expiry of the Main Agreement, the data importer's account will be deleted, images and personal data contained therein may be retained for a period of up to 90 days, after which it will be inaccessible.

Deletion of emails sent via SendGrid services will be guided by Sendgrid's retention policy available at: Data Retention and Deletion in Twilio Products.

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

N/A