CAPTURE ONE

July 2021

Capture One

Data Processing Agreement

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.: 31 36 43 02
(the "Customer")		**(the "Supplier")**

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

1. BACKGROUND AND PURPOSE OF AGREEMENT

1.1 The Parties have entered into a subscription agreement (the "**Main Agreement**") about the Supplier's provision to the Customer of a cloud-based service called Capture One Live ("**COL**") enabling photographers to share photos e.g. from a live photo session via the internet (the "**Services**").

1.2 When using COL 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 COL, 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 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 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.

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.

4.3.1 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.

4.3.2 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**").

5.3.1 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.

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

5.3.3 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

5.3.4 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.

6.2.1 The audit must be carried out in accordance with recognized auditing

standards in force at the given time by a competent third party.

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

6.2.3 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.

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.

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 until the

termination of the Main Agreement.

10.2 Regardless of Section 10.1, the Agreement stays in effect as long as the Supplier is in possession of any of the Customer's Personal Data.

10.3 In case of termination 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.

10.4 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.

11.2.1 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 PROCESSING ACTIVITIES

The Supplier stores and otherwise processes personal information on behalf of the Customer, typically in the form of the Customer's photos, which the Customer uploads to COL.

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 COL available to the Customer, including the provisioning of remote support and other assistance to the Customer.

2 CATEGORIES OF PERSONAL DATA

The personal data consists of photos taken by the Customer and other information about the Customer's customers.

3 PERSONAL DATA

Types of personal data processed in COL:

- Photos of the Customer's customers

4 SENSITIVE PERSONAL DATA

It is not envisaged that COL should be used for storage or other processing of sensitive personal data. The Customer should therefore refrain from uploading information of this sort to COL.

Sensitive personal data is understood as: Information on race or ethnical origin, political, religious or philosophical beliefs or trade union memberships, health information, information on sexual orientation and information on criminal records, and in the long term also generic and biometric data.

5. MICROSOFT AS DATA PROCESSOR AND TRANSFER TO THIRD COUNTRIES

COL is a cloud-based service based on Microsoft Azure.

As regards the storing and processing of the Customer's personal data on the Microsoft Azure platform, Microsoft Ireland Operations, Ltd ("**Microsoft**") acts as data processor, whereas the Customer will act as data controller

This data processing will therefore be conducted on the basis of Microsoft's standard data processing agreement forming part of Microsoft's online terms. The current version is "Microsoft Online Services Data Protection Addendum" of 9 December 2020" (the "**DPA**"), which may be downloaded via the following link https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=DPA.

The Customer accordingly instructs the Supplier to enter into the DPA with Microsoft on the

Customer's behalf.

Personal data is being transferred to third countries as part of the processing of the Customer's data on the Azure platform as set out in the DPA. The Customer therefore instructs the Supplier to enter into a data transfer agreement on the Customer's behalf with the data importers mentioned in the DPA based on the EU-Commission's Standard Contractual Clauses included in the DPA.

Notwithstanding the fact that Microsoft's processing of the Customer's personal on the Azure platform is a matter between Microsoft and the Customer, any instructions regarding this processing must be given to the Supplier who will then pass these instructions on to Microsoft.

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 which may be downloaded via the following link https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=DPA.

APPENDIX C

Use of sub-data processors:

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

Name	Location	Purpose/scope of processing
N/A		
N/A		

The Supplier may replace or make use of new sub-data processors subject to a prior written notice to the Customer giving the Customer a reasonable time to object.

As regards transfer of personal information to any sub-data 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-data processors on the Customer's behalf.