Data Processing Agreement governing Customer use of KeyShot Software as specified in the Order.

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Customers to

Keyshot's services as specified in the Agreement.

Company registration number: hereinafter "The Controller"

and

KeyShot A/S
Rymarken 2
8210 Aarhus DK

Company registration number: 25499522 hereinafter "The Processor"

each a "Party"; together the "Parties"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

This is version 4, last updated 07.09.2026 14:46.

1. Content

2. Preamble

2.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the Controller and the Processor, when processing personal data on behalf of the Controller.

2.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (GDPR).

2.3 In the context of the provision of KeyShot Software as specified in the Order., the Processor will process personal data on behalf of the Controller in accordance with the Clauses.

2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7 Appendix B contains the Controller's conditions for the Processor's use of subprocessors and a list of sub-processors authorised by the Controller.

2.8 Appendix C contains the Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Processor and how audits of the Processor and any sub-processors are to be performed.

2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.11 The Clauses shall not exempt the Processor from obligations to which the Processor is subject pursuant to the General Data Protection Regulation (GDPR) or other legislation.

3. The rights and obligations of the Controller

3.1 The Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

3.2 The Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3 The Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Processor is instructed to perform, has a legal basis.

4. The Processor acts according to instructions

4.1 The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2 The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1 The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2 The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1 GDPR, Article 32, stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

6.1.1 Pseudonymisation and encryption of personal data;

6.1.2 the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

6.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 According to GDPR, Article 32, the Processor shall also – independently from the Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Controller shall provide the Processor with all information necessary to identify and evaluate such risks.

6.3 Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to GDPR, Article 32, by inter alia providing the Controller with information concerning the technical and organisational measures already implemented by the Processor pursuant to GDPR, Article 32, along with all other information necessary for the Controller to comply with the Controller's obligation under GDPR, Article 32.

If subsequently – in the assessment of the Controller – mitigation of the identified risks require further measures to be implemented by the Processor, than those already implemented by the Processor pursuant to GDPR, Article 32, the Controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1 The Processor shall meet the requirements specified in GDPR, Article 28(2) and (4) in order to engage another processor (a sub-processor).

7.2 The Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the Controller.

7.3 The Processor has the Controller's general authorisation for the engagement of subprocessors. The Processor shall inform in writing the Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the Controller can be found in Appendix B.

7.4 Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and GDPR.

The processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Processor is subject pursuant to the Clauses and GDPR.

7.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the Controller's request – be submitted to the Controller, thereby giving the Controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Controller.

7.6 If the sub-processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in GDPR, Articles 79 and 82 – against the Controller and the Processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1 Any transfer of personal data to third countries or international organisations by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.

8.2 In case transfers to third countries or international organisations, which the Processor has not been instructed to perform by the Controller, is required under EU or Member State law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3 Without documented instructions from the Controller, the Processor therefore cannot within the framework of the Clauses:

8.3.1 transfer personal data to a controller or a processor in a third country or in an international organization

8.3.2 transfer the processing of personal data to a sub-processor in a third country

8.3.3 have the personal data processed by the Processor in a third country

8.4 The 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.6.

9. Assistance to The Controller

9.1 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the Processor shall, insofar as this is possible, assist the Data Controller in the Controller's compliance with:

9.1.1 the right to be informed when collecting personal data from the data subject

9.1.2 the right to be informed when personal data have not been obtained from the data subject

9.1.3 the right of access by the data subject

9.1.4 the right to rectification

9.1.5 the right to erasure ('the right t to be forgotten')

9.1.6 the right to restriction of processing

9.1.7 notification obligation regarding rectification or erasure of personal data or restriction of processing

9.1.8 the right to data portability

9.1.9 the right to object

9.1.10 the right not to be subject to a decision based solely on automated processing, including profiling

9.2 In addition to the Processor's obligation to assist the Controller pursuant to Clause 6.3, the Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:

9.2.1 The Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent data protection agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

9.2.2 The Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

9.2.3 The Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

9.2.4 The Controller's obligation to consult the competent data protection agency, prior to processing where a data protection impact assessment indicates that

the processing would result in a high risk in the absence of measures taken by The Controller to mitigate the risk.

9.3 The Parties shall define in Appendix C the appropriate technical and organisational measures by which The Processor is required to assist the controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1 and 9.2.

10. Notification of personal data breach

10.1 In case of any personal data breach, the Processor shall, without undue delay after having become aware of it, notify the Controller of the personal data breach.

10.2 The Processor's notification to the Controller shall, if possible, take place within immediately and no later than 36 hours after the processor has become aware of the breach of the personal data security after the Processor has become aware of the personal data breach to enable the Controller to comply with the Controller's obligation to notify the personal data breach to the data protection agency, cf. GDPR, Article 33.

10.3 In accordance with Clause 9.2.1, the Processor shall assist The Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to GDPR, Article 33(3), shall be stated in the Controller's notification to the competent data protection authority:

10.3.1 The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

10.3.2 the likely consequences of the personal data breach;

10.3.3 the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4 The parties shall define in Appendix C all the elements to be provided by the Processor when assisting the Controller in the notification of a personal data breach to the competent data protection agency.

11. Erasure and return of data

11.1 On termination of the provision of personal data processing services, the Processor shall be under obligation to delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

12.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in GDPR, Article 28, and the Clauses and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

12.2 Procedures applicable to the Controller's audits, including inspections, of the Processor and sub-processors are specified in C.7 .

12.3 The Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

13.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13.2 Security scanning and investigation of Customer Files. When the Controller uses the Processor's products and services, the Controller may upload, submit or process files, including 3D scenes, CAD data, textures, materials, scripts, plug-ins, project archives and support attachments ("Customer Files"). The Processor's software generates diagnostic data such as crash reports, memory dumps, telemetry and application logs.

13.3 The Processor does not routinely read or review the content of Customer Files. The Processor may, however, access, scan, analyze and investigate Customer Files and the associated diagnostic data where:

13.3.1 the Processor's security endpoint detection, file-scanning, sandboxing or other security and logging systems raise an alert, or flag a file as malicious or suspicious;

13.3.2 the Processor's software or a hosted service crash, hangs, produces corrupted output or terminates abnormally while processing a Customer File, and diagnosis requires examination of the file or of the diagnostic data derived from it;

13.3.3 the Processor suspects malware, unlawful or prohibited content, fraud, piracy, license circumvention or other misuse of the Processor's products, services or IT systems;

13.3.4 the Processor is investigating an actual or suspected security incident affecting its infrastructure, its supply chain or other customers;

13.3.5 the Processor is required to act by applicable law, by a binding court order or by a lawful request from a competent authority.

13.3.6 the Controller asks the Processor to examine a file, for example in connection with a support case or the reproduction of a defect.

13.4 Analysis is automated by default and comprises hash and reputation lookup, anti-malware scanning, inspection of file structure metadata, and execution in an isolated sandbox, with no person reading the content of the Controller's files.

13.5 Where automated analysis cannot resolve the alert or the malfunction, authorised security, engineering or support personnel may inspect the file, limited to the parts relevant to the event, on a need-to-know basis, subject to confidentiality obligations and with all access logged.

13.6 Where content is confirmed to be malicious, unlawful or in breach of the Agreement, the Processor may quarantine, block or delete it and suspend the affected job, session, account or license. The Processor shall inform the Controller without undue delay unless prevented from doing so by law or by an ongoing investigation.

13.7 The Processor uses the data referred to in Clauses 13.2 to 13.6 solely for security, diagnostic, support, abuse-prevention and legal-compliance purposes, and not for product development, marketing, profiling or the training of artificial intelligence or machine learning models.

13.8 The legal bases are the Processor's legitimate interest in ensuring the security, integrity and availability of its systems, products and services and in protecting its other customers and its intellectual property rights.

14. Commencement and termination

14.1 The Clauses are binding upon the Parties.

14.2 Both Parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the Parties.

14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Controller pursuant to Clause 11.1 and Appendix C.4, the Clauses may be terminated by written notice by either Party.

15. The controller and the processor contacts/contact points

15.1 The Parties may contact each other using the following contacts/contact points

15.2 The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Contact information for The Controller:

Contacts as per Order or Agreement.

Contact information for The Processor: Privacy@keyshot.com

Appendix A Information about the processing

1. **The purpose of the Processor's processing of personal data on behalf of the Controller is:**

1.1 The following purposes form the basis of the Processor's processing of personal data on behalf of the Controller:

KeyShot A/S stores and process Customer Data entered or uploaded to KeyShot Cloudbased Software (SaaS).

2. **The Processor's processing of personal data on behalf of the Controller shall mainly pertain to (the nature of the processing):**

2.1 Operation of KeyShot Cloud-based Software, Support, Onboarding Services and Service Requests delivered to Customer and it's Users.

2.2 Development of apps and customer portals and provision of services in relation hereto:

a) The processor provides services in relation hereto, including IT-architecture and development resources

b) The processor develops and provides apps, web-shops and customer portals

3. **The processing includes the following types of personal data about data subjects:**

3.1 **User information** containing: "Name, e-mail address, title" **User uploaded files** containing: "Customer Data" e.g. pictures, video, documents, 3D models, renderings with images of faces. **User entered data** containing: "Customer Data" e.g. metadata for search, file descriptions with personal information on employees, customers or suppliers.

4. **Processing includes the following categories of data subject**

4.1 Customer Users, Customer Data which may include data subjects like Employees, Customers, Suppliers.

5. **The Processor's processing of personal data on behalf of the Controller may be performed when the Clauses commence. The processing has the following duration:**

5.1 The processing of personal data shall be performed until the Processor's services has been terminated, after which the personal data is either returned or erased in accordance with Clause 11. The Processor's processing of personal data is performed as long as the underlying commercial agreement(s) consists.

Appendix B Authorised Sub-processors

1. Approved sub-processors

1.1 On commencement of the Clauses, the Controller authorises the engagement of the following sub-processors:

Name: MICROSOFT IRELAND OPERATIONS LIMITED

Company registration no/VAT: IE 8256796

Address: ONE MICROSOFT PLACE, SOUTH COUNTY BUSINESS PARK, LEOPARDSTOWN,

DUBLIN 18

Description of processing: Cloud hosting

Description of processing: Not specified.

Name: Amazon Web Services (AWS)

Address: 38 Avenue John F. Kennedy, Luxembourg, Luxembourg

Description of processing: Cloud hosting and computing infrastructure.

Name: Arrow ECS

Address: Not specified (Data location: Not specified)

Description of processing: Not specified.

Name: Chargebee

Address: 909 Rose Avenue, Suite 950, North Bethesda, United States of America

Description of processing: Subscription billing software.

Name: Cylynt LTD

Address: 50 City Quay, Dublin, Ireland

Description of processing: Anti-piracy monitoring software.

Name: Google

Address: 70 Sir John Rogerson's Quay, Dublin, Ireland

Description of processing: Analytics, advertising and workspace collaboration tools (Google Analytics, Google Ads, Google Workspace).

Name: HubSpot

Address: 25 First Street, 2nd Floor, Cambridge, MA, United States of America

Description of processing: CRM and marketing platform.

Name: Influitive

Address: 240 Richmond St West, Toronto, Canada

Description of processing: User community platform.

Name: Salesforce

Address: Salesforce Tower, 415 Mission Street, San Francisco, United States of America

Description of processing: CRM services (incl. Slack, Sales Cloud, Mulesoft, Tableau).

Name: TinyFrog Technologies

Address: 4455 Murphy Canyon Road #100, San Diego, United States of America

Description of processing: KeyShot website (WordPress) and hosting.

Name: WP Engine

Address: Collingham House, 6-12 Gladstone Road, Wimbledon, London, United Kingdom

Description of processing: Website hosting.

Name: Honeycomb

Address: 548 Market Street, Suite 24362

San Francisco, CA 94104

United States

Description of processing: Application monitoring and observability.

Name: DataDog

Address: 620 8th Avenue, 45th Floor

New York, NY 10018

United States

Description of processing: Infrastructure, application, and security monitoring.

Name: Zapier

Address: 548 Market St. #62411

San Francisco, CA 94104-5401

United States

Description of processing: Workflow automation and system integrations.

Name: ChurnZero

Address: 717 D Street NW, 2nd Floor

Washington, DC 20004

United States

Description of processing: Customer success management and usage analytics.

1.2 The Processor has the Controller's general authorisation for the engagement of subprocessor(s) from the above list. The Processor shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the subprocessor(s). The Processor shall provide the Controller with the information necessary to enable the data exporter to exercise its right to object.

Appendix C Instruction pertaining to the use of personal data

1. The subject of/instruction for the processing

1.1 The Processor processes personal data on behalf of the Controller in order to enable The Controller to use KeyShot Software owned and managed by the Processor. The Controller will use the Software in accordance with the Agreement.

2. Security of processing

2.1 The level of security shall take into account:

Taking into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the Processor must implement an appropriate level of security.

The Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Controller:

Physical security

The Processor shall implement the following physical security measures:

a) Reception is staffed 24/7 or there is a security company outside of office hours.
b) The processor and visitors etc. are identified by the use of identification cards.
c) The processor has tested the contingency and evacuation plan for emergencies.
d) The processor uses a verification process or verification system to control the identity of visitors.
e) The processor uses alarm systems to detect and prevent burglary.
f) The processor uses fire alarms and smoke detectors to detect and prevent fires.
g) The processor uses key management, i.e. provide keys to the relevant and necessary employees, etc.
h) The processor's devices (including PCs, servers, etc.) are secured behind locked doors.
i) The processor's employees are required to carry identity cards.
j) The processor's office space can be locked.

Organizational security

The Processor shall implement the following organizational security measures:

a) All employees of the processor are subject to confidentiality obligations that apply to all processing of personal data.
b) The employee access to personal data is limited, so that only the relevant employees have access to the necessary personal data.
c) The processing of personal data done by the employees of the processor is logged and can be checked as required.
d) The processor has an IT security policy.

e) The processor has documentable process descriptions for breaches of the personal data security, which are reviewed at least annually.
f) The processor has established procedures that ensure proper deletion or continuous confidentiality when the hardware is repaired, serviced, or disposed.
g) The processor has the opportunity to respond to employees' breaches of the processor's data security or breach of instructions on the processing of personal data according to employment law.
h) The processor's employees regularly document and report breaches of personal data security or risks thereof.

Technical security: Access to and protection of it systems

The Processor shall implement the following technical security measures regarding access to and protection of it systems:

a) The processor has policies for password composition, including minimum requirements.
b) The processor logs and controls unauthorized or repeated failed login attempts.
c) The processor requires employees to use individual passwords.
d) The processor uses antivirus programs that are updated regularly.
e) The processor uses logical access control with username and password or other unique authorization.
f) The processor's computers have automatic access protection during inactivity, ie. locked screen saver.
g) There are procedures for granting authorizations to IT systems when hiring new employees.
h) There are procedures for revoking permissions when an employee stops or switches department.

Technical security: Access to personal data

The Processor shall implement the following technical security measures regarding access to personal data:

a) The processor grants authorizations to individuals or groups of users to access, change and delete processed personal data.
b) The processor has procedure(s) to restore data from backup.
c) The processor has traceability of access, modification and erasure of data by individual users.
d) The processor logs and controls unauthorized or repeated failed attempts to access data.
e) The processor logs and controls unauthorized or repeated failed attempts to erase data.
f) The processor regularly reviews system controls.
g) The processor regularly reviews and verifies user authorizations for specific systems.

Technical security: Encryption

The Processor shall implement the following technical security measures regarding encryption:

a) Content on external hard drives and USB keys, etc. is encrypted when such media contain personal or sensitive personal information.
b) Passwords stored on the processor's computers, etc. are encrypted.
c) The network is encrypted.

d) The processor encrypts personal data in systems and/or on devices.

e) The processor encrypts sensitive personal data in systems and/or on devices.

f) The processor's computers have encrypted hard drives.

g) The processor's websites and web forms uses SSL certificates/HTTPS (Hyper Text Transfer Protocol Secure).

Technical security: Protection of personal data during transmission

The Processor shall implement the following technical security measures regarding protection of personal data during transmission:

a) The processor has guidelines for the use of work emails, including use for private use, appropriate use, encryption, secure use, etc.

b) The processor uses and has guidelines for secure email.

3. Assistance to the Controller

3.1 The Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Controller in accordance with Clause 9.1 and 9.2 by implementing the following technical and organisational measures:

3.1.1 If the Controller receives a request for the exercise of one of the rights of the data subjects in accordance with applicable data protection law, and a proper reply to the request requires assistance from the Processor, the Processor shall assist the Controller with the necessary and relevant information and documentation as well as appropriate technical and organizational security measures.

3.1.2 If the Controller needs the Processor's assistance in order to reply to a request from a data subject, the Controller must send a written request for assistance to the Processor and the Processor shall in response provide the necessary help or documentation as soon as possible and no later than 7 calendar days after

receiving the request.

3.1.3 If the Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Controller, and the request concerns personal data processed on behalf of the Controller, the Processor shall without undue delay forward the request to The Controller.

4. Storage period/erasure procedures

4.1 Upon termination of the provision of personal data processing services, the Processor shall either delete or return the personal data in accordance with Clause 11.1 unless the Controller – after the signature of the contract – has modified the Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

5. Processing location

5.1 Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Controller's prior written authorisation:

The processing location is KeyShot office and employees working from home in EU and North America.

Data Center is in either USA or EU depending on Customer location.

6. Instruction on the transfer of personal data to third countries

6.1 Personal data is only being processed by the Processor on the locations specified in clause C.5. Transfers to the United States occur on the basis of the data importer's certification under the EU-U.S. Data Privacy Framework (see certified organizations here.) The Data Processor transfers personal data to the following countries not subject to an adequacy decision on the basis of Article 45 of Regulation (EU) 2016/679 in order to fulfill the Main Agreement: USA.

6.2 If the Controller does not provide a documented instruction in these Clauses or subsequently with regards to the transfer of personal data to a third country, the Processor is not entitled to carry out such transfers within the scope of these Clauses.

6.3 Transfer of personal data can in all cases only be done in accordance with these Clauses, on the instructions of The Controller and to the extent permitted by the applicable data protection law.

6.4 Where, in accordance with these clauses, The Processor transfers personal data to sub-data processors in third countries outside the EU / EEA, the Processor must independently secure a legal basis for the transfer in accordance with Chapter 5 of GDPR.

6.5 If the transfer of personal data to third countries outside the EU/EEA is carried out in connection with the Processor's transfer to sub-processors, the Processor is by the provisions of the agreement authorized to enter into the standard contractual provisions adopted by the European Commission with the Processor's sub-processors on behalf of the Controller, provided that all the applicable rules regarding transmission and other processing of personal data are otherwise complied with. If the data controller itself is the processor, and the data processor is a sub-data processor of the data in relation to the data controller's ultimate contractual partner(s), the Controller must obtain authorization from the ultimate contracting party of the Processor in the standard contract terms.

7. Procedures for the Controller's audits, including inspections, of the processing of personal data being performed by the Processor

7.1 The Processor shall, upon the Controller's written request, document to the Controller that the Processor

7.1.1 is complying with his obligations under these Clauses and the Instruction, and

7.1.2 with the relevant articles in the GDPR in regards to the personal data being processed on behalf of the Controller.

7.2 According to Clause C.7.1 The Processor's documentation shall be sent to the Controller within a reasonable time after receiving the request.

7.3 The Processor shall not make available self-audit reports to the Controller in accordance with the principles of the ISAE 3000 Statement of Assurance as part of the Processors' documentation for compliance with these Clauses. The Processor is not obligated to initiate and undertake external audits of its compliance with the Clauses on its own initiative.

7.4 Regardless of Clause C.7.3, The Processor shall furthermore provide for and contribute to audits and inspections, performed by auditors appointed by the Controller, the public authorities in the competent jurisdiction, to the extent necessary to verify the Processor's compliance with these Clauses and the applicable data protection law. The auditor in question must be subject to

confidentiality under law or agreement. The Controller must notify the audits in writing with 30 calendar days.