APPENDIX A

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name:	Customer
Address:	As set forth in the Agreement
Contact person's name, position and contact details:	As set forth in the Agreement
Activities relevant to the data transferred under these Clauses:	As set forth in Annex I.B
Role (controller/processor):	Controller

Data importer(s):

Name:	Copyright Clearance Center, Inc.
Address:	222 Rosewood Drive Danvers, MA 01923, USA
Contact person's name, position and contact details:	Richard A. Ruf, VP & Chief Financial Officer privacy@copyright.com
Activities relevant to the data transferred:	Authorized officer of Data importer
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

End users of the Data Importer's online platform who conduct transactions via the Service. End users may include (i) authors of manuscripts, related to use of the Services; (ii) organization administrators who use or support usage of the Services; (iii) data exporter users of the Services whose information is used to support the Services

……..

Categories of personal data transferred

- Name
- Job title/Position
- Professional license/certification information

- Organization physical address
- Email address
- VAT country and ID
- Phone number
- Invoicing information
- Credit Information (Invoicing and billing information related to transactions)
- Organization and/or Institution affiliation
- Author identifiers (e.g. ORCID, ISNI)
- Data relating to usage of the Service.
- Publication identifiers (e.g., DOI, manuscript identifiers)

……..

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.

None.

……..

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

- Continuous, as described in the Agreement.

……

Nature of the processing

As described in the Agreement.

……

Purpose(s) of the data transfer and further processing

As described in the Agreement.

……..

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

Data will be retained for the term of the Agreement and may be retained thereafter to allow for resumption of the Services and/or for the Processor to fulfill ongoing business obligations. At any point, the Data Importer will provide the Data Exporter with the ability to delete Personal Data.

……..

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

See Annex III attached.

……..

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

……..

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

CCC is ISO/IEC27001:2013 certified and is audited annually under AICPA SOC II Type 2. Copies of CCC's ISO Certificate and SOC II Type 2 report will be provided on request.

Specifically, the Processor shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment as long as the personal data transferred by the data controller are processed.

Category 1 – Access to data processing equipment

The Processor shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment as long as the personal data transferred by the data controller are processed.

This shall be accomplished by:

- Establishing access authorizations for employees and third parties, including the respective documentation;
- Code card passes;
- Restrictions on keys;
- Best practices and guidance for third parties;
- Regulations on key codes;
- Identification of the persons having access authority;
- Security alarm system or other appropriate security measures including after working hours;
- Securing the decentralized data processing equipment and company issued computers;
- Protection and restriction of access path; and
- Other measures.

Category 2 - Access control to personal data

The Processor commits that the persons entitled to use the data processing system will only be able to access the personal data within the scope and to the extent covered by the respective access permission (authorization).

This shall be accomplished by:

- Locking of terminals;
- Allocation of individual terminals and/or terminal user and identification characteristics exclusive to specific functions; Single use dump terminals are not employed.
- Functional and/or time restricted use of terminals and/or terminal users and identification characteristics; Single use dump terminals are not employed.

- Regulations for user authorization;
- Obligation to comply with confidentiality provisions;
- User codes for personal data and programs;
- Coding routine for files;
- Differentiated access regulations (e.g. partial blocking);
- Regulations for the organization of files;
- Logging and analysis of use of the files;
- Controlled destruction of data media;
- Work instructions for templates for the registration of personal data;
- Checking, adjustment and controlling systems;
- Processes for the checking and release of programs; and
- Other measures.

Category 3 - User Control

The Processor shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment. In addition, the Processor shall implement suitable measures to prevent unauthorized reading, copying, alteration or removal of the data media, unauthorized input into memory, reading, alteration or deletion of the stored personal data.

This shall be accomplished by:

- Authorization design;
- Terminal with access user key;
- Identification of the terminal and / or the terminal user within the system of the Processor;
- Automatic turn-off of the user ID when several erroneous passwords are entered;
- Log file of events (monitoring of break-in attempts);
- Issuing and safeguarding the identification codes;
- Dedication of individual terminals and/or terminal users;
- Identification characteristics exclusive to specific functions;
- Authentication of the authorized personnel;
- Protective measures for the data input into memory as well as for the reading, blocking and deletion of stored personal data;
- Use of encryption for critical security files;
- Specific access rules for procedures, control cards, process control methods, program cataloguing authorization;
- Guidelines for data file organization;
- Keeping records of data file use;
- Separation of production and test environments for libraries and data files;
- Providing that entries to data processing facilities (rooms, housing, computer hardware and related equipment) are capable of being locked;
- Automatic log-off of user IDs that have not been used for a substantial period of time;

- Designating the areas in which data media may / must be located;
- Designating the persons in such areas for authorized removal of data media;
- Controlling the removal of data media;
- Securing the areas in which data media are located;
- Release of data media only to authorized persons;
- Control of files, controlled and documented destruction of data media;
- Policies controlling the production of backup copies; and
- Other measures.

Category 4 - Transmission control

The Processor shall be obliged to enable the verification and tracing of the locations/destinations to which the data subject's personal data are transferred by the utilization of the Processor's data communication equipment/devices.

This shall be accomplished by:

- Authentication of the authorized personnel;
- In-house verification requirements; Change control processes
- Designating the areas in which data media may / must be located;
- Controlling the removal of data media;
- Designating the persons in such areas who are authorized to remove data media;
- Control of files;
- Locking of confidential data media;
- Security lockers;
- Policies and procedures for access control within the secure area;
- Control of destruction of data media;
- Policies controlling the production of backup copies;
- Documentation of the transfer programs;
- Documentation of the retrieval and transmission programs;
- Documentation of the remote locations/destinations to which a transmission is intended and the transmissions path (logical path);
- Authorization policy;
- Encryption of the data for online transmission (i.e., encryption in transit) or transport by means of data carriers (tapes and cartridges);
- Monitoring of the completeness and correctness of the transfer of data (end to end check);
- Courier services, personal pickup, accomplishing of the transport;
- Control of plausibility;
- Control of completeness and correctness; and
- Other measures.

Category 5 - Input Control

The Processor shall provide for the retroactive ability to review and determine the time and the point of the data subject's personal data entry into the Processor's data processing system.

This shall be accomplished by:

- Proof of Processor's organization of the input authorization;
- Electronic recording of entries;
- Electronic recording of data processing, in particular usage of data; andOther measures.

Category 6 - Organization Control

The Processor shall maintain its internal organization in a manner that meets the requirements of this Agreement.

This shall be accomplished by:

- Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the personal data transferred by the data controller;
- Formulation of a data security concept;
- Industry standard system and program examination;
- Formulation of an emergency plan (backup contingency plan); and
- Other measures.

Category 7 - Instructional Control

The data transferred by the data controller to the Processor may only be processed in accordance with the instructions of the data controller.

This shall be accomplished by:

- Policies and procedures for the Processor's employees;
- Other measures.

Category 8 - Control of Separation of Personal Data

The Processor shall implement suitable measures to allow the separate processing of personal data that has been collected for different purposes.

This shall be accomplished by:

- Authorization policy (logical separation)

ANNEX III
LIST OF SUB-PROCESSORS

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

Company name of Authorized Subprocessor	**Details of the Point of Contact**	**Details of the processing**	**Service location**	**Additional safeguards (only in case of data transfer outside the EEA)**
[*Include full legal name and address of each recipient entity to whom data will be transferred*]	[*Include contact person's name, position and contact details*]	[*Include details of the processing to be undertaken by the entity*]	[*Include the location of where the services will be provided, including those within the EEA and outside of the EEA*]	[*If the recipient is located outside the EEA, specify the additional safeguards that are agreed on between Processor and Authorised Subprocessor and implemented, e.g. signed Model Clauses]*
Amazon Web Services, Inc.	410 Terry Ave. North, Seattle, WA 98109-5210,	Passive storage, excludes payment data	US East	Standard Contractual Clauses See section 1.14.4: https://aws.amazon.com/service-terms/
5CA International B.V., Catharijnesingel 30E, 3511 GB Utrecht, The Netherlands	Internal contact for CCC is Tom Ogier, Director of Customer Service. We cannot share this PII for vendor.	Customer Service as initiated by the Data Subject	Services provided globally	Contractual agreement and annual review of security and privacy practices per Company's ISO/IEC27001:2013 and SOC 2 Type 2 audits.
EPAM Systems, Inc., 41 University Drive, Suite 2020, Newtown Pennsylvania, USA, 18940	Internal contact for CCC is Michael Farrar, VP Engineering. We cannot share this PII for vendor.	Response to technical service inquiries as initiated by the Data Subject	Services provided from within EEA and United States	Contractual agreement and annual review of security and privacy practices per Company's ISO/IEC27001:2013 and SOC 2 Type 2 audits.

Cybersource Corporation	900 Metro Center Blvd Foster City, CA 94404	Credit card transaction processing	Services provided globally	Data processing agreement & SCCs (see: https://www.cybersource.com/en-us/about/dpa.html) ; annual review of security and privacy practices per Company's ISO/IEC27001:2013 and SOC 2 Type 2 audits.
Avalara, Inc. 255 South King St., Ste. 1800 Seattle, WA 98104		Sales tax exemption verification	Services provided within EEA and United States	Data Protection Addendum, including EU Standard Contractual Clauses and UK Addendum