ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. 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:	As set forth in the Agreement
Address:	As set forth in the Agreement
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 who conduct transactions directly via the Service. End users may include (i) employees of organizations requesting reprints, e-prints, and permission to use copyrighted works; (ii) organization administrators who use or support usage of the Services; (iii) third party individuals who, under industry-specific regulations, may be required to report purchases of reprints, e-prints and requests for permission to use copyrighted works

……..

Categories of personal data transferred

- Name
- Job title/Position
- Professional license/certification information
- Organization/business physical address
- Organization/business e-mail address
- Phone number
- Invoicing information
- Company-id
- User-id
- Department
- Division

- Cost center
- PSP-element
- VAT & Tax ID
- Credit Information (only for specific document orders)
- Organization and/or Institution affiliation
- Data relating to usage of the Service.

……...

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

The subject matter and duration of the Processing of Personal Data shall be consistent with the Agreement and the DPA.

……...

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.

Copyright Clearance Center (Provider or Provider's ultimate parent, as applicable) is ISO/IEC27001:2013 certified and is audited annually under AICPA SOC II Type 2. Copies of the most current ISO Certificate and SOC II Type 2 report will be provided on request, provided that the parties have entered into written confidentiality obligations.

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 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;
- Policies 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.
- Policies for user authorization;
- Obligation to comply with confidentiality provisions;
- User codes for personal data and programs;

- 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 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.

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 processing	Service location
Copyright Clearance Center, Inc. (if Provider is an affiliate of Copyright Clearance Center)	Full back office support for the Services, including storage of Personal Data	United States
Amazon Web Services, Inc.	Passive storage, excludes payment data	United States
5CA International B.V., Catharijnesingel 30E, 3511 GB Utrecht, The Netherlands	Customer Service as initiated by the Data Subject	Services provided globally
EPAM Systems, Inc., 41 University Drive, Suite 2020, Newtown Pennsylvania, USA, 18940	Response to technical service inquiries as initiated by the Data Subject	Services provided from within EEA and United States
JP Morgan Paymentech	Credit card payment processing (transactional purchases only)	United States
FlyWire	Credit card payment processing (transactional purchases only, where contact is initiated through Provider customer service)	Services provided globally

**Last updated 10 June 2024*