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's online platform who conduct transactions via the Service. Users of Customer's scientific library portal making inquiries for information regarding use of library resources. End users may include (i) Customer administrators who use or support usage of the Services; (ii) Customer 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/business physical address
- Organization/business e-mail address
- Phone number
- Invoicing information
- Company-id
- User-id
- Department
- Division
- Cost center
- 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.

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
[*Include full legal name and address of each recipient entity to whom data will be transferred*]	[*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*]
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
Vega IT, d.o.o. Novosadskog sajma, 2 9th floor, Novi Sad, Serbia	Software development, maintenance	Serbia
Cybersource	Credit card payment processing (transactional purchases only)	Services provided globally

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 October 2024*

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The later of: (i) the most recent date of the DPA accepted by Customer, or (ii) the Effective Date of the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As identified in Annex I of the EU SCCs.	Full legal name: As identified in Annex I of the EU SCCs.
Key Contact	Contact Details as set out in Annex I of the EU SCCs.	Contact Details as set out in Annex I of the EU SCCs.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs to which this Addendum is appended, detailed below, including the Appendix Information as set out in the relevant Appendices thereto.

Table 3: Exhibit Information

"**Exhibit Information**" means the information which must be provided for the selected modules as set out in the relevant Appendices of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As identified in Annex I of the EU SCCs.
Annex 1B: Description of Transfer: As set out in Annex I of the EU SCCs.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in Annex II of the EU SCCs.

Annex III: List of Sub processors (Modules 2 and 3 only): The sub-processors identified in Annex III of the EU SCCs.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	The Parties cannot end the IDTA before the end of the Agreement Term, except as set forth in Clause H of the Agreement.

Part 2: Mandatory Clauses

A. Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in consideration of each other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

B. Interpretation of this Addendum

1. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised as set forth herein.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

2. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
3. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such

amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

4. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
5. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

C. Hierarchy

1. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in this Section C will prevail.
2. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
3. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

D. Incorporation of and changes to the EU SCCs

1. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

   a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

   b. Section C overrides Clause 5 (Hierarchy) of the EU SCCs; and

   c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.

2. Unless the Parties have agreed alternative amendments which meet the requirements of Section D.1 above, the provisions of Section B.4 above will apply.
3. No amendments to the Approved EU SCCs other than to meet the requirements of this Section D may be made.
4. The following amendments to the Addendum EU SCCs are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

E. Amendments to this Addendum

1. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
2. If the Parties wish to change the format of the information included in *Part 1: Tables* of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
3. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

4. If the ICO issues a revised Approved Addendum under Section E.3 above, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the

end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

5. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.