

PERSONAL DATA PROCESSING AGREEMENT FOR OCLC SERVICES

This Data Processing Agreement (“DPA”) is entered into between OCLC (UK) Ltd., (“OCLC” or “Processor”) and the customer listed below (“Customer” or “Controller”) (jointly “the Parties”) as of the date of last signature below.

Customer

Organization Name	
Mailing Address	
Telephone/Fax	
Email	
Notice Contact	

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorised Affiliates, if and to the extent OCLC processes Personal Data for which such Authorised Affiliates qualify as the Controller. OCLC enters into this DPA on behalf of itself and in the name and on behalf of those OCLC Affiliates that process Personal Data. For the purposes of this DPA only, and except where indicated otherwise, the term; (i) “Customer” or “Controller” shall include Customer and Authorised Affiliates; and (ii) “OCLC” or “Processor” shall mean OCLC or the relevant OCLC Affiliate that is undertaking the processing of the Personal Data concerned. In the course of providing the Covered Services to Customer pursuant to the existing services agreement between the parties (the “Services Agreement”), OCLC may Process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

To ask questions about this DPA, please contact your OCLC contact or email EU_privacy@OCLC.org.

DATA PROCESSING AGREEMENT TERMS

The subject matter of the data processing under this DPA is Personal Data, as defined in Appendix 1, and the purpose and nature of the data processing under this DPA is the provision of the Covered Services initiated by Customer under the Services Agreement. Accordingly, the duration of the data processing under this DPA shall be determined by Customer’s Services Agreement for such Covered Services. This DPA shall terminate or expire on the same date that the Services Agreement terminates or expires, except that this DPA shall continue with respect to Processing that is contemplated to occur after the termination or expiration of the Services Agreement (such as making Personal Data available to Customer for a limited time period prior to deletion), and any extension of the Services Agreement shall also extend the term of this DPA.

For the purposes of the General Data Protection Regulation and Swiss Data Protection Laws (as defined below), for the transfer of personal data to processors established in third countries outside the European Economic Area (“EEA”) and Switzerland that are not recognized by the European Commission or the Swiss Federal Protection and Information Commissioner (as applicable) as ensuring an adequate level of data protection for personal data (“Third Country Recipient”), those entities of Customer who are transferring Personal Data outside of the EEA or Switzerland and those entities of OCLC who are Third Country Recipients hereby agree that the Standard Contractual Clauses (the “Clauses”), linked [here](#) and incorporated into this DPA by reference (as supplemented in the next paragraph below), shall apply to such transfers in order to adduce adequate safeguards with respect to the protection of privacy and

fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

For the sake of clarity, the Clauses apply to Customer and each of its Authorised Affiliates who, for the purposes of the Clauses, each act as 'data exporter' and each OCLC Affiliate (and OCLC, if OCLC is or becomes a Third Country Recipient) as each, for the purposes of the Clauses, may act as 'data importer' under this DPA. Customer acknowledges that Processor established in the EEA, Switzerland or UK may utilize its Affiliates who are Third Country Recipients, and with respect to any such transfer of Personal Data to such Third Country Recipients, such transfer shall be covered by the Clauses and deemed a direct export by Customer to the Third Country Recipient. All relevant terms from Appendices 1 and 2, attached hereto, are hereby incorporated into the Clauses agreed to by the parties (as Appendices 1 and 2 of the Clauses, respectively). In clauses 9 and 11(3) of the Clauses, the governing law is the laws of the country of Customer's establishment. Nothing in this DPA or in the Services Agreement is intended by the parties to be construed as prevailing over the Clauses.

1. DEFINITIONS

- 1.1. "**Authorised Affiliate**" means Customer's Affiliates that (a) are subject to the data protection laws and regulations of the EU, the EEA and/or their member states, Switzerland and/or the United Kingdom; (b) are permitted to use the Covered Services pursuant to the Services Agreement between Customer and OCLC; and (c) have not signed their own Services Agreement with OCLC.
- 1.2. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by or is under common control with a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- 1.3. "**Covered Services**" means the OCLC services that are ordered by the Customer from OCLC involving the Processing of Personal Data on behalf of the Customer, as set forth in the applicable Services Agreement.
- 1.4. "**Data Protection Laws and Regulations**" means all applicable laws that govern the use of data relating to Data Subjects, including the European Union ("EU") General Data Protection Regulation ("GDPR"), as amended or replaced from time to time, and any other foreign or domestic laws to the extent that they are applicable to a party in the course of the performance of the Services Agreement.
- 1.5. "**Personal Data**" means any personal data, as defined in the GDPR, which is provided by or on behalf of Customer and Processed by the Processor pursuant to the Services Agreement. An overview of the categories of Personal Data and purposes for which the Personal Data are being Processed is provided in Appendix 1.
- 1.6. "**Regulator**" means any supervisory authority with authority under Data Protection Laws and Regulations over all or any part of the provision or receipt of the Covered Services or the Processing of Personal Data.
- 1.7. "**Sensitive Data**" means the special categories of Personal Data as described in Article 9 of the GDPR, and Personal Data relating to criminal convictions and offences as described in Article 10 of the GDPR.
- 1.8. "**Standard Contractual Clauses**" means European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU.
- 1.9. "**Subprocessor**" means any data Processor engaged to Process Personal Data on behalf of OCLC and/or its Affiliates. For the avoidance of doubt, OCLC's colocation data centre facilities are not considered Subprocessors under this DPA.

- 1.10. **“Swiss Data Protection Laws”** means all applicable data protection and privacy laws in force from time to time in Switzerland, including the Swiss Federal Data Protection Act 1992, as amended or replaced from time to time.
- 1.11. Terms such as “Data Subject”, “Personal Data Breach”, “Processing”, “Controller”, “Processor” and “Supervisory Authority” shall have the meaning ascribed to them in the Data Protection Laws and Regulations.

2. SERVICES AGREEMENT

- 2.1. This DPA supplements and is incorporated into the Services Agreement, and in the event of any conflict between the terms of this DPA and the terms of the Services Agreement, the terms of this DPA shall prevail and control, but only with respect to the subject matter of this DPA.

3. OBLIGATIONS OF THE CUSTOMER

- 3.1. **Instructions.** This DPA and the Services Agreement are Customer’s complete and final instructions, at the time of signature of the DPA, to OCLC for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon mutually by the Parties in writing, unless such instructions are required by law. Customer warrants that the instructions it provides to OCLC pursuant to this DPA comply with Data Protection Laws and Regulations.
- 3.2. **Data Subject and Supervisory Authority Requests.** Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under Data Protection Laws and Regulations and all communications from any Regulator(s) that relate to the Personal Data, in accordance with Data Protection Laws and Regulations.
- 3.3. **Notice, Consent, and Other Authorisations.** Customer is responsible for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired the Personal Data that it provides to OCLC for Processing under the Services Agreement. Customer is responsible for providing any notice to the Data Subjects and for obtaining and demonstrating evidence that it has obtained any necessary consents, authorisations, and permissions from the Data Subjects in a valid manner for OCLC to perform the Covered Services. Customer will provide OCLC with such evidence of this as OCLC may reasonably request if OCLC needs this information to comply with Data Protection Laws or the request of any Regulator. Customer understands that custom fields and other free text fields in the software provided as a part of the Covered Services (such as “notes” fields) are not designed for the Processing of Sensitive Data and warrants that it will not enter Sensitive Data in such fields or otherwise when using the Covered Services.

4. OBLIGATIONS OF THE PROCESSOR

- 4.1. **Scope of Processing.** OCLC will Process the Personal Data on documented instructions from Customer given in accordance with this DPA, including with regard to transfers of Personal Data to a third country or an international organisation, and in such manner as is necessary for the provision of Covered Services under the Services Agreement, except as required to comply with a legal obligation to which OCLC is subject. OCLC shall inform Customer if, in its opinion, the execution of an instruction relating to the Processing of Personal Data could infringe on any Data Protection Laws and Regulations. In the event that OCLC must Process Personal Data for the purpose of complying with a legal obligation, OCLC will inform the Customer of that legal requirement before Processing, unless notification is prohibited by the law.
- 4.2. **Data Subject Requests.** Taking into account the nature of the processing, OCLC has established appropriate technical and organizational measures to assist Customer in its fulfillment of its obligation to respond to requests for exercising the data subject rights laid down in Chapter III of the GDPR, including processes for receiving and responding to requests from Data Subjects. In particular, if OCLC receives a request from a Data Subject made under the GDPR and determines that OCLC is not the controller and that the controller is Customer, OCLC will assist Customer by referring the Data Subject to Customer (either specifically or generally) as the entity to whom a request should be made. At Customer’s request, and provided that

Customer is unable to fulfill a request through functionality of the Covered Services themselves or otherwise, OCLC will provide additional, reasonable assistance (taking into account the nature of the processing) to Customer to assist Customer in fulfilling its obligations related to Data Subject rights under Chapter III of GDPR.

- 4.3. **Regulator Requests.** With respect to its role as a processor of Customer, OCLC will provide reasonable assistance to Customer to address any communications and advice or orders from any Regulator relating to the Personal Data.
- 4.4. **Retention.** OCLC will retain Personal Data only for as long as Customer deems it necessary for the permitted purpose as determined by configuration options made available by OCLC and selected by Customer for Covered Services from time to time, or as required by applicable laws. At the termination of the Services Agreement, OCLC will either, at the choice of Customer, destroy or return the Personal Data to Customer, unless legal obligations require OCLC to retain Personal Data, in accordance with OCLC's then-existing procedures for the destruction or return of Personal Data.
- 4.5. **Disclosure to Third Parties.** OCLC will not disclose the Personal Data to third parties except as permitted by this DPA or the Services Agreement or as otherwise directed by Customer or as contemplated by the Covered Services (such as making limited Personal Data available to another library to facilitate an inter-library loan request), unless OCLC is required to disclose the Personal Data by applicable laws, in which case OCLC shall (to the extent permitted by law) notify Customer in writing and liaise with Customer before complying with such disclosure request. The foregoing shall not apply to Personal Data reflected in Customer's holdings (such as the names of authors).
- 4.6. **Confidentiality.** OCLC will treat all Personal Data as strictly confidential and will inform all of its employees, agents, and approved Subprocessors engaged in Processing the Personal Data, of the confidential nature of such information. OCLC will ensure that personnel authorised to Process the Personal Data are subject to appropriate confidentiality obligations.
- 4.7. **Security.** OCLC will implement and maintain administrative, physical, technical and organisational safeguards for the security, confidentiality and integrity of Personal Data as detailed in Appendix 2 (including protections against accidental or unlawful loss, destruction, alteration, damage, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed). OCLC will have a procedure for the regular testing, inspection, assessment and evaluation of the effectiveness of the technical and organisational measures in order to ensure the security of the processing.
- 4.8. **GDPR Articles 32-36.** Taking into account the nature of the Processing and the information available to OCLC, OCLC will provide reasonable assistance to Customer in complying with its obligations under GDPR Articles 32-36 (inclusive) (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation).

5. AUDIT

- 5.1. **Process.** Processor will provide to Customer, upon request, any then-existing, third-party certification(s) pertinent to Processor's compliance with its obligations under this DPA (for example, ISO certification). To the extent that such third-party certifications or other information provided by Processor are deemed inadequate by Customer to demonstrate compliance to Article 28, Customer may have a reputable, independent third party or auditor with expertise in data security (the "Auditor") inspect Processor's policies and records relating to the Processing of Personal Data by Processor to ensure Processor's compliance with Article 28 of the GDPR, provided that such Auditor is reasonably acceptable to Processor.

- 5.2. **Timing and Costs.** Customer will provide Processor with at least one (1) month's written notice of any audit. Prior to the start of an audit, the Parties will agree to reasonable time, duration, place, manner, and conditions for the audit. Customer shall bear the cost of any audit requested pursuant to this Section 5. Unless otherwise required by a Regulator (or if the audit reveals a material breach of this DPA), no more than one audit may be undertaken in any 12-month period.
- 5.3. **Disclosure.** Prior to any such inspection, the Auditor must sign a non-disclosure agreement which shall be provided to Auditor by Processor. The results of the inspection and all information reviewed during such inspection will be deemed Processor's confidential information and shall be protected by Auditor in accordance with the terms of the non-disclosure agreement to be executed between Auditor and Processor. Notwithstanding any other terms, the Auditor may only disclose to Customer specific violations of Article 28, if any, and the basis for such findings in accordance with the terms of this DPA and shall not disclose any of the records or information reviewed during the inspection.

6. CONTRACTING WITH SUBPROCESSORS

- 6.1. **Customer Consent.** Customer consents, on its own behalf and on behalf of its Authorised Affiliates, to the use of Subprocessors for the Processing of Personal Data in relation to the Services Agreement. A listing of Subprocessors is found [here](#) and may be revised from time to time.

Processor will inform Customer of the addition or replacement of any Subprocessors by posting an updated list of Subprocessors at the link above ("New Subprocessor Notice"). If there is no objection by Customer within fifteen (15) days after posting of a New Subprocessor Notice, this will be deemed acceptance by Customer to the use of the proposed new Subprocessor.

If Customer has a reasonable basis to object to the use of a new Subprocessor, Customer will notify Processor promptly in writing within fifteen (15) days after the posting of a New Subprocessor Notice. If Customer reasonably objects in accordance with this clause, OCLC will use commercially reasonable efforts to make available to Customer a change in the affected Covered Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Covered Services to avoid processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If OCLC is unable to make available such a change within a reasonable period of time, which will not exceed thirty (30) days, Customer may terminate the Services Agreement and this DPA and the Clauses by providing written notice to Processor. Upon termination of the Services Agreement pursuant to this Section, OCLC will refund the pro rata portion of the fees for the remainder of the annual subscription period after the termination date of the Services Agreement.

- 6.2. **Liability.** Processor shall ensure that the Subprocessor is bound by written contract or other legal act to the same data protection obligations of Processor under this DPA and the Data Protection Laws and Regulations. Processor will be liable for the acts and omissions of its Subprocessors to the same extent Processor would be liable if performing the services of each of those Subprocessors directly under the terms of this DPA.

7. INFORMATION OBLIGATIONS AND INCIDENT MANAGEMENT

- 7.1. **Notification.** OCLC maintains security incident management policies and procedures specified in Appendix 2, and shall notify Customer without undue delay after OCLC becomes aware of a Personal Data Breach involving OCLC or its applicable Subprocessors that impacts Personal Data provided to OCLC pursuant to this DPA. Such notification may be by any means OCLC has established for such notification, including notification by email. Notifications of Covered Services unavailability may be by [OCLC's System Status](#).
- 7.2. **Coordination.** The Parties agree to coordinate in good faith on developing the content of any related public statements and any required notices to the affected data subjects and/or the relevant Regulator(s) in

connection with a Personal Data Breach involving OCLC or its applicable Subprocessors, provided that nothing in this section shall prevent either party from complying with its obligations under Data Protection Laws and Regulations.

8. MISCELLANEOUS

- 8.1. **Liability and Indemnity.** Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Services Agreement. For avoidance of doubt, any such limitation of liability applied from the Services Agreement shall apply in the aggregate to all OCLC entities taken together, even if such entities are not referred to specifically in the Services Agreement.
- 8.2. **Informal Dispute Resolution.** In the event of a dispute between Customer and OCLC, such dispute shall be referred to the individuals responsible for data protection issues for each organization, who shall endeavour to resolve the dispute within thirty (30) days.
- 8.3. **Obligations Post-Termination.** Termination or expiration of this DPA shall not discharge either party from its obligations meant to survive the termination or expiration of this DPA.
- 8.4. **Changes in Data Protection Laws and Regulations.** The Parties agree to negotiate modifications to this DPA if changes are required to continue to comply with the Data Protection Laws and Regulations or the legal interpretation of the Data Protection Laws and Regulations, including but not limited to (a) replace the Standard Contractual Clauses if they are invalidated, or (b) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.
- 8.5. **Severability.** If any provisions of this DPA shall be found by any court of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect the other provisions of this DPA. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

The parties' authorized signatories have duly executed this DPA on behalf of the party and, where relevant, their Affiliates.

Customer

OCLC (UK) Ltd.

Signature	_____	Signature	<u>I. Singh</u>
Printed Name	_____	Printed Name	<u>Indar Singh</u>
Title	_____	Title	<u>Executive Director Finance, EMEA</u>
Date	_____	Date	<u>October 21, 2019</u>

APPENDIX 1

DATA EXPORTER

The data exporter is Customer.

DATA IMPORTER

The data importer is OCLC, Inc. or its Affiliate who is a Third Country Recipient.

CATEGORIES OF DATA SUBJECT

The categories shall be determined by the Customer and may include, without limitation, patrons, staff, faculty, students, administrators, employees, visitors and alumni of Customer, and data subjects whose personal data are reflected in Customer's holdings (such as the names of authors).

TYPE OF PERSONAL DATA

Types of Personal Data shall be consistent with the provision of the Covered Services and may include, but is not limited to:

- Names
- Job titles
- Contact information (including physical addresses, telephone number(s), fax number(s), email address(es), etc.)
- Unique identifiers, whether assigned by Customer or Processor (e.g., patron ID numbers and barcodes, employee ID numbers, etc.)
- Usernames and passwords
- Personal attributes (e.g., dates of birth, gender, department, patron type, etc.)
- Photographs (via URL)
- Staff-related usage information
- Research activity
- General usage information, including connection data
- Supplier/vendor information

SPECIAL CATEGORIES OF DATA

The personal data transferred will not include special categories of data.

PROCESSING OPERATIONS

Personal Data will be processed for the purpose of providing the Covered Services described in the Service Agreement, thus facilitating the administration, operations, maintenance, and patron use of the Customer library and access to its resources. This includes, without limitation, the following processing activities:

- Storing, retrieving, using, modifying, and deleting Personal Data as necessary to provide the Covered Services;
- Copying and storing Personal Data for development, testing, backup, disaster recovery, sandbox services, and other non-production purposes;
- Sending communications related to the Covered Services to end users;
- Providing reports to Customer;
- Modifying, deleting, copying, or transferring Personal Data as necessary to meet the requests of individual Data Subjects;
- Logging user activity on the system for troubleshooting, auditing, and other purposes;
- Processing that is necessary to troubleshoot, debug, and improve the Covered Services;
- Processing necessary to provide customer support services to Customer and its employees;
- Patching, upgrading, troubleshooting, administering, configuring, and otherwise maintaining information technology systems and databases used to provide the Services;
- Monitoring the performance of the Covered Services and troubleshooting and remediating any causes of downtime or inaccessibility of the Covered Services;
- Security monitoring, network-based intrusion detection support, penetration testing, and other similar monitoring and testing;

- Assistance with backup and restoration of the Covered Services
- Processing that is necessary to meet legal obligations, such as compliance with a valid court order, and record retention requirements that are imposed by law;
- Any other lawful and agreed upon processing necessary to carry out the written instructions of Customer.

DURATION OF THE PROCESSING

The duration of the processing shall be the term of the Services Agreement and a reasonable and limited period of time following expiration or other termination.

APPENDIX 2

OCLC's Technical and Organizational Security Measures can be found [here](#). Security measures may be updated from time-to-time; however, changes will not result in any reduction in the level of protection provided.