Data Transfer Agreement

1. Introduction

This Data Transfer Agreement ("Agreement") is between OCLC (UK) Ltd. (as "data exporter") and OCLC, Inc. (as "data importer") (together "the Parties") and is dated on the date of execution.

The data exporter and data importer are members of the same corporate group. The purpose of this Agreement is to ensure that, where personal data are shared by the data exporter with the data importer, the data importer's processing of such personal data is compliant with all applicable data protection laws.

2. Obligations

In consideration of the payment by each Party to the other of the sum of £5.00 (receipt of which is hereby acknowledged), the Parties agree as follows:

2.1 to enter into the Controller-to-Controller Standard Contractual Clauses as published by the UK Information Commissioner's Office and provided at Appendix 1 ("SCCs"); and

2.2 that in light of the Schrems II judgment issued by the Court of Justice of the European Union on 16 July 2020 in regard to transfers of personal data from data exporters based in the UK, to data importers located in a country outside of the UK, the obligations of the Parties warrant the inclusion of supplemental clauses to the SCCs in order to adduce additional safeguards to personal data transferred to the data importer. The Parties hereby agree to the supplemental clauses provided in Appendix 2.

2.3 For the avoidance of doubt, the supplementary clauses contained in Appendix 2 do not vary or modify the SCCs as prohibited by clause VII of the SCCs. Rather, the supplementary clauses add to the protection of personal data in line with UK data protection laws regarding international data transfers.

AGREED FOR AND ON BEHALF OF OCLC (UK) Ltd. on the date set out below:

Date: Jun 9, 2021

Name and Title: H.L.M. (Eric) van Lubeek, Vice President & Managing Director

Signature: Eric van Lubeek
Eric van Lubeek (Jun 9, 2021 11:34 GMT+2)

AND

AGREED FOR AND ON BEHALF OF OCLC, Inc. on the date set out below:

Date: Jun 8, 2021

Name and Title: Barton Murphy, Chief Technology & Information Officer

Signature: Bart Murphy
Bart Murphy (Jun 8, 2021 16:42 EDT)

Appendix 1

Standard Contractual Clauses for international transfers from controller to controller:

Date of contract: Jun 8, 2021

Parties

Name of the data exporting organisation: OCLC (UK) Ltd.
(The sender of the data)

Address and country of establishment: City Gate, 8 St. Mary's Gate, Sheffield S1 4LW, United Kingdom

Telephone: +44 (0)114 267 7500

And

Name of the data importing organisation: OCLC, Inc.
(The receiver of the data)

Address and country of establishment: 6565 Kilgour Pl., Dublin, Ohio 43085

Telephone: 614-764-6000

Definitions

For the purposes of the Clauses:

a) 'personal data', 'special categories of data/sensitive data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in the UK GDPR;
b) 'the data exporter' shall mean the controller who transfers the personal data;
c) 'the data importer' shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018; and
d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

Clause I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.
d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.
e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause 4, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the Information Commissioner. However, the data exporter shall abide by a decision of the Information Commissioner regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the Information Commissioner where required.

Clause II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.
c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the Information Commissioner where required) if it becomes aware of any such laws.
d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses
e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the Information Commissioner concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause 2(e).
f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause 4 (which may include insurance coverage).
g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.
h) It will process the personal data, at its option, in accordance with:

- the data processing principles set forth in Annex A.

Please complete:

Initials of data importer: BM
BM

It will not disclose or transfer the personal data to a third party data controller located outside the United Kingdom (UK) unless it notifies the data exporter about the transfer and

a) the third party data controller processes the personal data in accordance with UK adequacy regulations finding that a third country provides adequate protection, or
b) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by the Information Commissioner, or
c) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.
d) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

Clause III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under the UK GDPR or DPA 2018.
b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses 2(b), 2(d),2(e), 3(a), 3(c), 3(d), 3(e), 3(h), 3(i), 4(a), 6, 7(d) and 8 against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

Clause IV. Law applicable to the clauses

These clauses shall be governed by the law of the UK country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

Clause V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the Information Commissioner concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Information Commissioner. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties

also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the Information Commissioner which is final and against which no further appeal is possible.

Clause VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the United Kingdom rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the Information Commissioner shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if new UK adequacy regulations under Section 17A Data Protection Act 2018 are issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause 8(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

Clause VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the Information Commissioner where required. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding additional commercial clauses where required.

Clause VIII. Description of the transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause

1(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Additional commercial clauses

Priority of standard contractual clauses of standard contractual clauses

The Clauses take priority over any other agreement between the parties, whether entered into before or after the date the Clauses are entered into.

Unless the Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Clauses are entered into, will amend the terms or the effects of the Clauses, or limit any liability under the Clauses, and no term of any such other agreement should be read or interpreted as having that effect.

Please complete:

On behalf of the data exporter: OCLC (UK) Ltd.

Name: H.L.M. (Eric) van Lubeek
Position: Vice President & Managing Director
Address: City Gate, 8 St. Mary's Gate, Sheffield S1 4LW, United Kingdom

Signature: Eric van Lubeek
Eric van Lubeek (Jun 9, 2021 11:34 GMT+2)

On behalf of the data importer: OCLC, Inc.

Name: Barton Murphy
Position: Chief Technology & Information Officer
Address: 6565 Kilgour Pl., Dublin, Ohio, 43085, United States

Signature: Bart Murphy
Bart Murphy (Jun 8, 2021 16:42 EDT)

Annex A

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.
8. Automated decisions: For purposes hereof, "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a)(i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   (ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.

Annex B

Data subjects

The personal data transferred concern the following categories of data subjects:

- Staff and related data subjects, including volunteers, agents, temporary and casual workers, Board of Directors and Global Council members, etc.;
- Customers and prospective customers (including their staff, faculty, students, administrators, employees, visitors and alumni of Customer);
- Data subjects whose Personal Data are reflected in Customer's holdings (such as the names of authors);
- Data subjects who are users of free services such as WorldCat.org, WebJunction, and similar services; and
- Suppliers (including their staff).

Purposes of the transfer

The transfer is made for the following purposes:

- Staff administration, including permanent and temporary staff, including appointment or removals, pay, discipline; superannuation, work management, and other personnel matters in relation to the data exporter's staff;

- Advertising, marketing and public relations of the data exporter's own business or activity, goods or services;

- Accounts and records, including:
  - keeping accounts relating to the data exporter's business or activity;
  - deciding whether to accept any person or organisation as a customer;
  - keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;
  - keeping customer records
  - records for making financial or management forecasts; and
  - other general record keeping and information management;

- Advertising, marketing and public relations for others, including public relations work, advertising and marketing, host mailings for other organisations, and list broking;

- Education, including the provision of education or training as a primary function or as a business activity; and

- Other:
  - Storing, retrieving, using, modifying, and deleting Personal Data as necessary to provide Services;
  - Copying and storing Personal Data for development, testing, backup, disaster recovery, sandbox services, and other non-production purposes;
  - Sending communications related to Services to end users;
  - Providing reports to Customers;
  - 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 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 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;

Categories of data

The personal data transferred concern the following categories of data:

- 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), Author-related information, Staff-related usage information, Author-related information, Research activity, General usage information, including connection data, Supplier/vendor information,
- Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details;
- Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records; and
- Employment and similar details, including information relating to the employment and employment history of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

- Charitable and voluntary;
- Education and childcare;
- General business/general public;
- IT, digital, technology and telecoms;
- Legal and professional advisers;
- Regulators; and
- Research.

Sensitive data

The personal data transferred concern the following categories of sensitive data.

- Data relating to health and welfare benefits, such as short and long-term disability, medical and dental care.
- Information about traffic infractions in case of company cars.
- Where necessary and authorized by law, criminal records, information about violations of laws as part of internal investigations, disciplinary or legal proceedings and helpline submissions.
- Biometric data, including voice recordings of meetings, voicemails, etc. when needed for business operations.
- Trade union membership if required to comply with legal obligations.
- Ethnic origin if required to comply with legal obligations.
- Religious beliefs if required to comply with legal obligations.

Contact points for data protection enquiries

Data importer contact details:

OCLC Data Protection Officer
dpo@oclc.org

Data exporter contact details:

OCLC Data Protection Officer
dpo@oclc.org

Footnotes

[1] "Relevant provision means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

Appendix 2

1 SUPPLEMENTARY CLAUSES

1.1 Pursuant to clause I(a) of the SCCs, the data exporter warrants and undertakes that the personal data have been, among other things, transferred in accordance with the laws applicable to the data exporter. The Parties acknowledge that in light of the Schrems II judgment issued by the Court of Justice of the European Union on 16 July 2020 in regard to transfers of personal data from data exporters based in the UK, to data importers located in a country outside of the UK (**"Third Country"**), the obligations of the Parties warrant the inclusion of supplemental clauses to the SCCs in order to adduce additional safeguards to personal data transferred to the data importer. Therefore, the Parties hereby warrant the following:

(a) In the event that the data importer receives a request from any law enforcement authority of a Third Country for disclosure of personal data processed under the SCCs in such Third Country, it will use every reasonable effort to redirect such authority to request data directly from the relevant data exporter.

(b) In the event that the data importer is served with legally binding requests by any law enforcement authority in Third Country for disclosure of personal data in such Third Country, it will notify the relevant data exporter without undue delay. Such notification shall include information available to data importer.

(c) In the event that the data importer in Third Country becomes aware of any direct access by local public authorities regarding such personal data, it will notify the relevant data exporter without undue delay. Such notification shall include information available to the data importer.

(d) If the data importer is prohibited from notifying the relevant data exporter, it agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicate to the relevant data exporter as much information and as soon as possible. The data importer agrees to document its best efforts in order to demonstrate them upon request of the relevant data exporter.

(e) To the extent permissible under the local laws of the relevant Third Country, the data importer will provide to data exporter, in regular intervals for the duration of the SCCs, the greatest possible amount of relevant information on the requests received, if any (in particular, number of requests, type of personal data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.).

(f) The data importer will preserve the information pursuant to points (a) to (e) above for the duration of the SCCs and make it available to the Information Commissioner's Office upon request.

(g) In case of any legally binding request as referred to in point (b) above, the data importer will review the legality of the request for disclosure under laws of the relevant Third Country, notably whether such request remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if it concludes that there are grounds under such laws to do so. When challenging a request, the data importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. The data importer shall not disclose the personal data

requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of data importer under the SCCs.

(h) In any case, the data importer will provide the minimum amount of personal data permissible if responding to a request for disclosure, based on a reasonable interpretation of the request.

(i) Each data importer processing personal data in Third Country has provided to data exporters information necessary to evaluate risks associated with the processing of personal data in Third Countries, in particular any such information as indicated in Annex 1. Each data importer shall further respond to requests for relevant additional information from any respective data exporter, and provide such information without undue delay.

(j) The data importer will promptly notify the relevant data exporter if, after having committed to these supplementary safeguards and having completed the assessment under point (i) above, and for the duration of the SCCs, the data importer has a reason to believe that the data importer has become subject to new/amended Third Country laws or national enforcement practices of Third Country have changed in a way that do not allow the data importer to meet its obligations under the SCCs.

(k) Following the notification pursuant to point (j) above, the data importer will seek to accommodate any relevant instruction from the data exporter that the data importer can reasonably implement. Such instructions may be for instance of technical or organizational nature. The data exporter may also decide to suspend the transfer of personal data to the data importer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the Information Commissioner to do so, in which case data exporter shall be entitled to terminate the SCCs.

Annex 1
Questionnaire

Following up on our obligations under the UK data protection laws in regard to the transfer of UK personal data from data exporter's entities acting as data exporters to data importers located in Third Countries and in light of the Schrems II, data exporters request your prompt response to the following questions. These aim to assess whether the adequate level of protection that SCCs guarantee, can be maintained by the data exporter as a Party thereto.

(1) For the purposes of 50 U.S.C. § 1881(4) or similar provision in the country where your company is located, is your company classified as a "electronic communication service provider" or otherwise directly subject to 50 U.S.C. § 1881a ("FISA § 702") or provision with a similar effect in your country of residence?

(2) Has your company ever cooperated with your local authorities, conducting surveillance of communications under EO 12333 (or similar provisions under local laws), with regard to the data of any of its clients or employees (including clients' employees), be it on voluntary or mandatory basis?

(3) Has your company ever been the subject of a FISA § 702 warrant (or similar warrant under local laws) with regard to a request for disclosure of any customer or employee data that it stores or otherwise processes for other companies? If possible, please approximate the number of such instances or at least a percentage when compared to client/employee data not subject to such warrants.

(4) Has your company established a team whose responsibility includes responding to FISA § 702 warrants (or similar warrant under local laws) or cooperation with national security agencies under EO 12333 (or similar provisions under local laws)?

OCLC - UK SCC + Schrems II clauses 060721 Final

Final Audit Report 2021-06-09

Created:	2021-06-08
By:	Anne Utendorf (utendora@oclc.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA86_bqJ02IL5iy-delbYO1aiSUfzSMg7w

"OCLC - UK SCC + Schrems II clauses 060721 Final" History

Document created by Anne Utendorf (utendora@oclc.org)
2021-06-08 - 8:34:34 PM GMT- IP address: 75.118.6.201

Document emailed to Eric van Lubeek (eric.vanlubeek@oclc.org) for signature
2021-06-08 - 8:38:13 PM GMT

Document emailed to Bart Murphy (murphyba@oclc.org) for signature
2021-06-08 - 8:38:14 PM GMT

Email viewed by Bart Murphy (murphyba@oclc.org)
2021-06-08 - 8:41:58 PM GMT- IP address: 98.31.39.209

Document e-signed by Bart Murphy (murphyba@oclc.org)
Signature Date: 2021-06-08 - 8:42:41 PM GMT - Time Source: server- IP address: 98.31.39.209

Email viewed by Eric van Lubeek (eric.vanlubeek@oclc.org)
2021-06-09 - 7:38:58 AM GMT- IP address: 132.174.171.2

Document e-signed by Eric van Lubeek (eric.vanlubeek@oclc.org)
Signature Date: 2021-06-09 - 9:34:24 AM GMT - Time Source: server- IP address: 80.115.137.20

Agreement completed.
2021-06-09 - 9:34:24 AM GMT