

Addendum

to Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

INTRODUCTION

This Addendum ("**Addendum**") is dated on the date of execution and supplements the Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers) (the "**SCCs**"). The Parties agree to:

- (i) supplement the SCCs with additional safeguards to data transfers to countries that are not deemed as offering an adequate level of data protection by the EU Commission. These safeguards are outlined at clause 1 of this Addendum.
- (ii) amend the role of OCLC (UK) Ltd. from a data exporter to a data importer, as outlined at clause 2 of this Addendum, in the event that the European Commission does not grant the UK an adequacy decision by 1 July 2021, i.e. the end of the interim regime set forth by the EU-UK Trade and Cooperation Agreement.

Any defined words and expressions used in this Addendum shall, unless otherwise provided for, have the same meanings as provided for in the SCCs.

The additions and amendments which are to be made to the SCCs are as follows:

1 SUPPLEMENTARY CLAUSES

1.1 Pursuant to clause I(a) of the SCCs, the data exporter warrants 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 EEA/Switzerland, to data importers located in a country outside of these locations ("**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 reasonable efforts 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 competent supervisory authority 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 Countries 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 Appendix 1 to this Addendum. 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 competent supervisory authority to do so, in which case data exporter shall be entitled to terminate the SCCs.

2 AMENDMENT

- 2.1 The Parties agree that in the event that the European Commission does not grant the UK an adequacy decision by 1 July 2021, i.e. the end of the interim regime set forth by the EU-UK Trade and Cooperation Agreement, the role of OCLC (UK) Ltd. under the SCCs will, through this Addendum, change from a data exporter to a data importer, with effect on the day following the end of such interim regime.

3 GENERAL

- 3.1 Each of the Parties acknowledge and agree that with effect from the date of execution of this Addendum, the SCCs shall be deemed complemented in accordance with any procedure for the agreement of changes as provided for under the SCCs regardless of whether or not this Addendum has been agreed by the Parties in strict compliance with such procedure.
- 3.2 For the avoidance of doubt, the supplementary clauses do not vary or modify the SCCs as prohibited by clause VII of SCCs. Rather, the supplementary clauses add to the protection of personal data in line with EU data protection laws regarding international data transfers.
- 3.3 The provisions of the SCCs, as supplemented by this Addendum, shall continue in full force and effect, and shall be read and construed as one document with this Supplementary Agreement, as of the effective date of this Addendum.
- 3.4 OCLC EMEA B.V., Paris office, OCLC S.r.l., OCLC GmbH, OCLC BV, OCLC AG, and OCLC (UK) Ltd. shall sign the Addendum for and on behalf of all data exporters indicated in the SCCs, including OCLC (UK) Ltd. OCLC, Inc. shall sign the Addendum on behalf of the data importer.

Signatures follow on next page

AGREED FOR AND ON BEHALF OF THE PARTIES SET OUT AS DATA EXPORTERS IN THE SCCs by:

OCLC EMEA B.V., Paris office
58-60 avenue de la Grande Armée
75017 Paris, France

OCLC S.r.l.
Viale dei Mille, 164
50131 Florence, Italy

OCLC GmbH
Grünwalder Weg 28g
82041 Oberhaching, Germany

OCLC BV
Schipholweg 99
2316 XA Leiden, Netherlands

OCLC AG
Münchensteinerstrasse 220
4053 Basel, Switzerland

OCLC (UK) Ltd.
City Gate
8 St. Mary's Gate
Sheffield S1 4LW, United Kingdom

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 (Jun 9, 2021 11:35 GMT+2)

AND

AGREED FOR AND ON BEHALF OF THE PARTY SET OUT AS DATA IMPORTER IN THE SCCs by: OCLC, Inc.

on the date set out below:

Date: Jun 8, 2021

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

Signature: 
Bart Murphy (Jun 8, 2021 16:35 EDT)

Appendix 1 Questionnaire

Following up on our obligations under the EU General Data Protection Regulation (“**GDPR**”) in regard to the transfer of EEA and Swiss 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 - Addendum to existing SCCs 060721 Final

Final Audit Report

2021-06-09

Created:	2021-06-08
By:	Anne Utendorf (utendora@oclc.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA5M0mFBbUg8N4fvxs3ouQH2aclFsYy-LP

"OCLC - Addendum to existing SCCs 060721 Final" History

-  Document created by Anne Utendorf (utendora@oclc.org)
2021-06-08 - 8:31:59 PM GMT- IP address: 75.118.6.201
-  Document emailed to Eric van Lubeek (eric.vanlubeek@oclc.org) for signature
2021-06-08 - 8:34:05 PM GMT
-  Document emailed to Bart Murphy (murphyba@oclc.org) for signature
2021-06-08 - 8:34:05 PM GMT
-  Email viewed by Bart Murphy (murphyba@oclc.org)
2021-06-08 - 8:34:47 PM GMT- IP address: 98.31.39.209
-  Document e-signed by Bart Murphy (murphyba@oclc.org)
Signature Date: 2021-06-08 - 8:35:20 PM GMT - Time Source: server- IP address: 98.31.39.209
-  Email viewed by Eric van Lubeek (eric.vanlubeek@oclc.org)
2021-06-09 - 7:38:46 AM GMT- IP address: 132.174.171.2
-  Document e-signed by Eric van Lubeek (eric.vanlubeek@oclc.org)
Signature Date: 2021-06-09 - 9:35:43 AM GMT - Time Source: server- IP address: 80.115.137.20
-  Agreement completed.
2021-06-09 - 9:35:43 AM GMT