EU SCC Transfer Impact Assessment (TIA)

for use under the EU General Data Protection Regulation (GDPR) regarding compliance with the EU Standard Contractual Clauses (EU SCC).

Conducted by:

Technische Informationsbibliothek (TIB), Welfengarten 1B, 30167 Hannover, Germany

Reviewed by:

ORCID Inc., 10411 Motor City Drive, Suite 750, Bethesda, Maryland 20817, USA

for the ORCID DE Consortium

regarding the transfer of personal data described below.

I. Description of the intended transfer

1.	**Data exporter:**	Members of ORCID DE Consortium (all located in the European Union)
2.	**Country of data exporter:**	Countries in the European Union (if member institutions of ORCID DE Consortium update researcher information on ORCID Inc. servers).
3.	**Data importer:**	ORCID Inc. USA
4.	**Country of data importer:**	USA
5.	**Context and purpose of the transfer:**	Updating profile information in personal ORCID records of ORCID record holders affiliated with members of ORCID DE Consortium
6.	**Roles of data importer and exporter**	Regarding data protection, the data exporters always act as as data controllers, whereas the importer acts as a data controller when information is uploaded to the ORCID Member API, or a data processor when information is uploaded to the ORCID member portal.
7.	**Categories of data subjects concerned**	ORCID record holders affiliated with members of ORCID DE Consortium
8.	**Categories of personal data transferred**	- Name (including variations of the data subject's name), email address, online and other social media profiles - Details of grants and funding awarded or applied for by data subjects - Details of researcher papers and other submissions

		(e.g. peer reviewed publications) or works developed or contributed to by data subjects - Details of entities which the data subject is affiliated to or employed by - Details of the data subject's education, qualifications, awards, honors, membership, service and positions (e.g. visiting fellow). For most data fields the source is also included, which will usually be the data subject itself, but may sometimes also be the institution.
9.	**Sensitive personal data**	None
10.	**Technical implementation of the transfer**	Member institutions of ORCID DE Consortium can upload profile information of affiliated ORCID record holders via the ORCID member API, and also transfer affiliation data to the Member Portal. In both cases, information is only added to the data subject's ORCID record with their permission.
11.	**Technical and organizational measures in place within the member institutions of the ORCID DE Consortium and in communication with servers of ORCID Inc.:**	Security measures are described in the SCCs, and in particular Annex II thereto. Security measures described therein include the following: - Security Policies and Procedures; - Event Logging; - Remote Access; - Access Control; - Network Controls; - Malware Controls; - Encryption; - Passwords and Multi-factor Authentication; - Data Back-Ups; - Physical Security Measures; - Data Security and Privacy training; and - Information security incident management.
12.	**Relevant onward transfer(s) of personal data (if any):**	Data which is set to "Public" by the record holder (data subject) may be transferred onwards to any other user of the registry, ORCID APIs or ORCID Public Data File anywhere in the world. This is done with the record holder's explicit consent. Data which is set to "Trusted Parties" may be transferred onwards to any organization the record holder has chosen to designate as a trusted organization.
13.	**Countries of recipients of**	Any country (see above)

	relevant onward transfer(s):	

II. Transfer Tool according to Chapter V GDPR

Art. 45 GDPR	**Adequacy decision of the EU Commission**	There is no adequacy decision for the USA
Art. 46 par. 2 GDPR	**Appropriate Safeguards according to Art. 46 par. 1 GDPR:**	
	Legally binding and enforcable instrument between public bodies or authorities	
	Binding corporate rules in accordance with Article 47 GDPR	
	Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);	**X**
	Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);	
	An **approved code of conduct pursuant to Article 40 together with binding and enforceable commitments** of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects‘ rights	
	An **approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments** of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects‘ rights.	
Art. 46 par. 3 GDPR	**Subject to the authorisation from the competent supervisory authority,** the appropriate safeguards referred to in par. 1 may also be provided for, in particular, by	
	Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in	

	the third country or international organisation	
	Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	
Art. 49 GDPR	**Derogations for specific situations:**	
	n/a	

III. Assessment of efficacy of transfer tool

1.	**Target jurisdiction** for which the TIA is made:	USA
2.	**Legislation in the third country** formally meeting EU standards is manifestly **not applied/complied with in practice;**	n/a
3.	There are **practices incompatible with the commitments of the transfer tool** where relevant legislation in the third country is lacking;	No known practices or cases.
4.	Your transferred data and/or importer fall or **might fall within the scope of problematic legislation** (i.e. impinging on the transfer tool's contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on fundamental rights, necessity and proportionality).	Relevant local laws taken into consideration: The transferred data and/or importer falls or might fall within the scope of **Section 702 FISA, EO 12.333 (and PPD-28)**, which may impinge on the transfer tool's contractual guarantee of an essentially equivalent level of protection and have been judged not to meet EU standards on fundamental rights, necessity and proportionality.

IV. Define the TIA parameters

1.	**Starting date** of the transfer	01. Jan 22
2.	**Assessment period in years**	5 - once we approach the end of the period, we will re-assess the situation.
3.	**Ending date** of the assessment based on the above	31. Dec 26

V. Description of current level of protection:

1.	Is the **personal data at issue transmitted to the target jurisdiction in clear text** (i.e. there is no appropriate encryption in-transit)?	All traffic over the internet is protected by state-of-the-art line encryption.
2.	Is the **personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party** (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Access is to the data in clear text is technically possible by the data importer and is necessary for the correct operation of ORCID's services. Access to the data in clear text may be possible by the US authorities under Section 702 FISA, EO 12.333 (and PPD-28), even though a state-of-the-art encryption is in place. Most data held in the ORCID registry is publicly accessible by choice of the data subject, although they often choose not to make their email addresses public.

VI. Define the safeguards in place

1.	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	No. The service of ORCID Inc. is located in the USA, there is no alternative to data storage with ORCID Inc. in the USA for the ORCID DE Consortium.
2.	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes. ORCID Inc. has in place EU SCCs for Controller to Processor and Controller to Controller and we have no reason to believe that ORCID Inc. will not comply with them, to the extent that US law permits so.
2.	Ensure that the mechanism remains in place and is complied with.	ORCID has made public commitments to uphold the privacy of user data, and these commitments may only be made by a binding vote of its Board of Directors, which in turn is elected by member organizations.

		ORCID enters into legally binding agreements with its members to adhere to privacy guidelines and requires all users of its services to abide by legally binding terms and conditions.

VII. Risk assessment of prohibited lawful access in the target jurisdiction

Assess the probability that during the assessment period, the following legal arguments will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the relevant local laws as identified in

Considering that

- ORCID Inc. holds personal data of researchers and other scholars of ORCID DE member institutions on its servers,
- The researchers and other scholars of member institutions of the ORCID DE Consortium are generally not US citizens (US persons) and not located in the US, and thus not protected by mechanisms which prevent the targeting of communications to persons located in the United States or US persons by US authorities under the relevant laws.
- The data importer/recipient has possession, custody or control over the personal data at issue in clear text and could be (successfully) ordered to provide or search it in clear text under the relevant laws which will not be prevented by the applicability of European data protection law or any other applicable legal regulations,

It is possible that access to the personal data of the data subjects of the importer would be requested of ORCID Inc. on the basis of **Section 702 FISA, EO 12.333 (and PPD-28).**

However, given that:

- **T**he data importer is **contractually required to defend the personal data at issue** against lawful access attempts under the EU SCCs entered into with ORCID Inc.,
- The **data importer/recipient is not an "Electronic Communications Service Provider"** with regard to the processing of the personal data at issue but offers services to the scholarly community and is thus out of scope of the relevant laws and contains no communication data between data subjects,
- The profile data of the researchers and other scholars held by ORCID is generally publicly available on the internet and generally the **non-public personal data of relevance and in scope of the relevant laws is the contact information of the data subjects** and the probability that this may be of interest is not very high,
- To the best of the knowledge of the current senior management, a request for access to personal data on this basis has so far not been made to ORCID Inc by US authorities

The probability that during the assessment period the data is regarded as content that is the subject of lawful access requests at issue under the relevant local laws, based on past experience

and

the probability that during the assessment period, the data importer will search the data in plain text for selectors on an ongoing basis (i.e. search terms such as certain recipients or senders of electronic communications) without the data exporter's permission as part of the lawful access requests at issue under the relevant local laws

is rated as low

as this is not the target of data gathering under Section 702 FISA or EO 12.333.

This is confirmed by a report of the Privacy and Civil Liberty Oversight Board (PCLOB) (https://irp.fas.org/offdocs/pclob-702.pdf) and the decisions of the Foreign Intelligence Surveillance Court (FISC) granting accesses in such cases (2019: https://bit.ly/3heBYQB). These sources contain no indication that such data has ever been the target of searches under Section 702 FISA or EO 12.333. Also, Section 702 FISA is only about communications services provided to the targets of the searches, and not to others or applications such as the present one. Therefore, we believe that the probability that the provider has or will receive a surveillance order with respect to our data during the period under consideration is very low

Thus the ORCID DE Consortium has no reason to believe that **Section 702 FISA, EO 12.333 (and PPD-28)** will be applied to the transferred data or importer.

In addition, it has been agreed upon that the importer will regularly report on its experience with lawful access requests during the assessment period and will inform the data exporter if the circumstances taken into account in the above assessments are no longer valid.

Place, Date	Place, Date
_____	_____
Signature TIB (on behalf of ORCID DE Consortium)	Signature ORCID Inc.