UK MODEL DIVERSITY SURVEY

InterLaw Diversity Forum

Apollo Leadership Institute

TRANSFER IMPACT ASSESSMENT

FOR TRANSFERS FROM INTERLAW DIVERSITY FORUM TO LAW SCHOOL ADMISSION COUNCIL, INC.

1 Introduction

A Transfer Impact Assessment ("**TIA**") is a mandatory assessment that must be carried out for each new processing activity that involves a data transfer to non-EEA/UK countries not deemed adequate by the European Commission or UK's Information Commissioner. It clarifies the risks for transferring data to countries without adequacy under the GDPR and ensures that the data subjects continue to have a level of protection essentially equivalent to that under the UK/EU data protection regime.

2 Background information

Person(s) conducting assessment	Jonathan Leonhart, InterLaw Diversity Forum, with input from external legal counsel.
Date of assessment	21 October 2021

3 Parties to the data transfer

Who is the data exporter?	InterLaw Diversity Forum, a company incorporated in England and Wales and operating as a not-for-profit, having its principal place of business at 7 Bell Yard, London, WC2A 2JR, United Kingdom ("**InterLaw**").
Who is the data being transferred to (data recipient)?	Law School Admission Council, Inc., a Delaware not-for-profit corporation, having its principal place of business at 662 Penn Street, Newtown, Pennsylvania 18940, USA ("**LSAC**").
What type of organisation is the data recipient (including the economic sector in which it operates)?	Not-for-profit organisation – LSAC's mission is to advance law and justice by encouraging diverse, talented individuals to study law and by supporting their enrolment and learning journeys from prelaw through practice. LSAC administers the Law School Admissions Test ("LSAC") in the United States. LSAC provides platform maintenance, support, and training services to InterLaw.

Will the recipient share the data with any other parties, e.g. sub-processors?	Yes. LSAC uses the hosting services of Microsoft and contracts directly with Microsoft ensuring that appropriate contractual protections are in place. Microsoft stores data in its US Azure East data centre. LSAC may otherwise only subcontract its processing operations with the prior written consent of InterLaw.

4 Details of proposed or actual transfer

What are the specific circumstances of the transfer?	The transfer of data is necessary given that InterLaw operates in the UK and LSAC operates in the US. The parties need to share data between these territories in order to facilitate LSAC's provision of the services to InterLaw. There is a Master Services Agreement ("**Agreement**") in place to govern the transfers of personal data between InterLaw and LSAC, with appropriate data processing provisions, technical and security measures, and standard contractual clauses for international data transfers. Given transfers are from the UK, the old standard contractual clauses are currently relied on but the parties are well aware that these will need to be updated once the ICO has published and approved its final version. In the meantime the parties are following ICO guidance on transfers and appropriate safeguards.
What are the intended onward transfers?	None.
For what purpose is the data being transferred and processed?	LSAC's provision of the Services to InterLaw under the Agreement, which includes carrying out a UK Model Diversity Survey to enable measuring of diversity, equity and inclusion data across law firms (the "**UK MDS**"). The main purpose of the overall processing is for InterLaw to provide client signatories greater transparency around diversity, inclusion, and culture in their panel law firm/legal service providers.
What type of personal data will be transferred? Is any of this special category or criminal offence data?	Personal data included within the InterLaw Diversity Forum Data, including contact details, portal usage data and UK MDS input data. The personal data transferred relating to law firms may include (without limitation): • Names, pronouns, email address, and job title of the Firm Contact, and the name of the CEO/Managing Partner. • Number of individuals who fall into particular diversity categories. • Demographic profiles for lawyers in leadership positions. • Demographic profiles of the highest and lowest earning partners. • Demographic profiles of those holding the top 30 key client partnerships.

	Transfers of special category/criminal offence data relating to law firms may include (without limitation): • Racial or ethnic origin. • Disability information. • Sexual orientation. The personal data transferred relating to client signatories may include (without limitation): • Names and email address. As set out in InterLaw's DPIA in relation to this project, personal data is already heavily minimised, and it is only in remote situations where law firms have low diversity numbers that it may technically be possible to identify an individual, but even then not directly from data supplied in the UK MDS but only with other publicly available information.
What volume of personal data will be transferred?	The volume of personal data will vary depending on the number of platform users InterLaw has at any given time and on the make-up of the relevant law firm submitting the response.
Who are the data subjects?	Staff of participating law firms and client signatories.
Will the data be stored in the recipient country or is it intended to provide remote access only to data stored within the UK/EU?	The data will be stored on the UK MDS online platform (which is built on Microsoft Dynamics 365, Power Platform and PowerBI) in the United States, as administered by LSAC subcontracting Microsoft. Data may be accessed remotely by LSAC located in the US (Delaware) and stored by Microsoft in its Azure East platform. LSAC will delete the data (instructing Microsoft to do so) as soon as it is no longer needed for LSAC to provide InterLaw with the Services.
In what format will data be transferred / what are the transmission channels used?	Data on the UK MDS online platform may be accessed by LSAC located in the US (Delaware) remotely through the internet and then hosted by Microsoft as per above.

5 Jurisdiction

Where is the data being transferred to?	The data will be transferred to LSAC in the US and stored as explained in 3 above.

Where are the headquarters of the data recipient?	US (Delaware).

6 Lawful ground for processing

What is your lawful ground for processing the personal data (by transferring it) under GDPR?	Legitimate Interests, which includes processing in order to receive the Service from LSAC. Substantial Public Interests (for special category data). InterLaw relies on the lawful bases set out in Schedule 1, Part 2, Data Protection Act 2018 relating to the equality of opportunity or treatment, and/or racial and ethnic diversity at senior levels. Participating law firms (as independent data controllers) will be separately responsible for determining their own lawful basis for the processing of personal data by them and sharing such data with InterLaw.

7 Alternatives to international data transfer

Can you anonymise the data?	For some data, this is not possible because LSAC will need personal data to fulfil the purposes of processing (set out above) and there is no alternative method for InterLaw to achieve this objective. Only non-directly identifying numerical diversity data is input into the UK MDS.
Can you achieve your purposes without transferring the personal data at all?	No, this is not possible because LSAC need to access the data from the US for operational reasons. LSAC configures and manages the American Bar Association's Model Diversity Survey, from which the UK MDS has been adapted. As such they are best positioned to configure and manage the UK MDS.

8 Relying on an adequacy decision

Is there an adequacy decision you can rely on?	No. There is no UK adequacy decision in respect of the US at the current time.

9 Relying on standard contractual clauses (SCCs)

9.1 Transfer mechanism

Which transfer mechanism do you propose to rely on?	Standard contractual clauses, which are set out in the DPA (Exhibit D to the Agreement).

9.2 Level of protection provided in the third country – US

When relying on SCCs, you must be satisfied that there is no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the Data Importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under the SCCs. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, are not in contradiction with the SCCs.

Question	Response
What are the laws and practices of the country in which the Data Importer operates?	The US has several sector-specific and medium-specific national privacy or data security laws, as well as state-specific laws such as the California Consumer Privacy Act and the Delaware Online Privacy and Protection Act. Violations of US privacy laws and rules are generally enforced by the FTC, state attorneys general, or the regulator for the industry sector in question. Individuals may bring private rights of action (and class actions) for certain privacy or security violations.
Are there laws requiring the disclosure of data to public authorities or authorising access by public authorities? Are such laws relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards?	InterLaw has considered the following U.S. national security and surveillance laws: • s702 of Foreign Intelligence Surveillance Act ("FISA") • Executive Order (EO) 12333 ("EO 12333") • U.S. Judicial Redress Act of 2015 • Official Reports on foreign intelligence to aid Congressional and Judicial oversight of intelligence agencies' use of information collected under s702 FISA ("FISA Amendments Reauthorization Act of 2017") Personal data transferred to, or accessed by, LSAC in the US is not subject to FISA or EO 12333, and is unlikely to be subject to other US surveillance laws.

Question	Response
	FISA applies to "electronic communications service providers". These include both "providers of electronic communications services" and "providers of remote computing services." LSAC is not a provider of electronic communications services or remote computing services, and the type of data collected not does constitute "communications" sought by FISA s702. Further, the personal data processed by LSAC will not constitute intelligence information and therefore EO 12333 is not relevant.
Has the data recipient received any request from public authorities to disclose data, in the past 12 months, two years and five years? If so, provide details.	No.

9.3 Supplementary measures

What are the relevant contractual, technical or organisational safeguards in place to supplement the SCCs, including measures applied during transmission and to the processing of the personal data in the country of destination?

9.3.1 Are additional Supplemental Measures required following the assessment set out above?

[X] No. Reason:

InterLaw is satisfied that there is no reason to believe that the laws and practices to which LSAC is subject, including any requirements to disclose personal data or measures authorising access by public authorities, prevent LSAC from fulfilling its obligations under the SCCs. LSAC and InterLaw already have appropriate technical and organisational measures in place (for example, access controls, encryption, physical security and information security policies) to protect the personal data.

10 Assessment conclusion

Are you satisfied that there is no reason to believe that the laws and practices in the third country of destination applicable to the	Yes. InterLaw is satisfied that there is no reason to believe that the laws and practices in the US, including any requirements to disclose personal data or measures authorising access by public authorities, prevent LSAC from fulfilling its obligations under the SCCs.

processing of the personal data by the Data Importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under the SCCs, taking into account all of the factors outlined in this transfer impact assessment?	

11 Sign-off

Assessment approved by	Jonathan Leonhart Head of Operations
Date of approval	30 October 2022
Comments or recommendations	