DATA PROTECTION IMPACT ASSESSMENT ("DPIA")

UK MODEL DIVERSITY SURVEY

Submitting controller details

Name of controller	InterLaw Diversity Forum
Subject/title of DPIA	UK Model Diversity Survey DPIA
Name of controller contact	Jonathan Leonhart

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA.

InterLaw Diversity Forum ("**IDF**") was established in 2008, originally as an inter-organisational forum for LGBT+ personnel in the legal sector, and has since expanded its scope to encompass all strands of diversity and inclusion (including race & ethnicity, disability, gender, and social mobility), with a particular focus on cultural change in the workplace and intersectionality. IDF's mission and purpose is to foster inclusion for all diverse, socially mobile, and under-represented talent working in the legal sector, and to promote meritocracy in all sectors by working to 'level the playing field' in order to create environments where the best talent can succeed.

As part of this mission, IDF is rolling out the UK Model Diversity Survey ("**UK MDS**"), a supplier DEI questionnaire which corporate and financial institution signatories ("**client signatories**") ask their panel firms/legal service providers to fill out. The UK MDS has been adapted with kind permission from the 2021 version of the ABA Model Diversity Survey, originally developed and conducted by the American Bar Association ("**ABA**").

The purpose of the UK MDS is to serve as the standard for law firms' reporting of their diversity, equity, and inclusion ("**DEI**") metrics to their clients. The UK MDS can help clients shape their decisions about allocation of legal work to law firms/legal suppliers by creating greater transparency around diversity, equity, inclusion, and culture in law firms.

The UK MDS will also assist law firms in providing thorough, accurate, and uniform information to their corporate and financial institution clients. Further, it will streamline DEI data collection for law firms by allowing firms to provide a single, uniform set of data to multiple clients.

A DPIA is required pursuant to Article 35(1) GDPR where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. **Although IDF does not consider that its data processing is high risk to the rights and freedoms of natural persons**, there is a small chance that special category data could be processed as part of the UK MDS where the survey indicates that there is only "1" person in a particular diversity category in a particular law firm and that person could therefore potentially be identified through publicly available sources. In addition, IDF strives to ensure the highest standards of

privacy in the design of the UK MDS regardless of whether a DPIA is a specific requirement. As such, IDF has decided to carry out this DPIA as part of its ongoing compliance efforts.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? What types of processing identified as likely high risk are involved?

Any law firm with an office location based in the UK will be eligible to submit a response to the UK MDS. Participating law firms will receive a key code once a year giving them one-time access to the online platform in order to enter and submit their anonymous numerical data, which they will have first gathered and completed manually offline. This key code will also serve as a record identifier.

The data submitted by the law firms into the UK MDS platform will be processed only by IDF and its service partner, the Law School Admission Council, Inc. ("**LSAC**"), a Delaware not-for-profit corporation, that provides platform maintenance, support, and training services to IDF. The UK MDS platform runs on a suite of Microsoft tools: Microsoft Dynamics 365 (SaaS), PowerBI (SaaS), and Power Platform (SaaS – where the platform sits) with security managed by Microsoft under contract with LSAC. As an SaaS offering, the physical datacentre, physical network, physical host, operation system, network control, certifications, and applications are all managed by Microsoft. Data is stored in Microsoft's US Azure East data centre.

IDF will use law firms' responses on a confidential basis to generate 'Dashboards' in the UK MDS platform for client signatories. These Dashboards translate the raw anonymous numerical data provided by firms into percentages and IDF provides only this percentage information to the client signatories on the UK MDS platform. Only certain individuals at client signatories will have access to the platform and its Dashboards through secure log-in credentials on a 'need-to-know' basis. UK MDS terms will ensure that client signatories are subject to confidentiality obligations and only able to use the information for the same overall mission purposes set out above.

The Dashboard enables the client signatories to view data in an easy-to-understand visual format and to draw out information and insights which might not be possible when viewing such large amounts of data in a tabular format. Client signatories will be able to make like-for-like comparisons between law firms/legal service providers, as well as to compare data over time and measure their panel firms' progress.

Client signatories will be able to see the law firm's name, the name of its CEO/Managing Partner, and the name and email of the law firm's designated contact for the UK MDS ("**Firm Contact**"). No demographic data is requested for these two individuals. The raw anonymous numerical data which IDF collects about the law firms' lawyers will only be viewable by IDF and LSAC and will not be accessible by any client signatory. Additionally, no law firm participant has any on-going access to the online platform once their

data has been submitted. No law firm has access to any other law firms' data in any form. Law firms may request from IDF a copy of their own data as presented in the Dashboards. The response information will always be aggregated and released to client signatories in a statistical or summary form.

IDF, with the support of the ABA, has carefully designed the UK MDS to collect the minimum amount of data possible from law firm participants and only asks for DEI data to be reported in anonymous numerical format to reduce the risk of individuals being identifiable. These numbers are shown in the Dashboards as percentages which have been rounded to the nearest whole number.

As above, if the response to any question in the UK MDS is "1" (meaning one person reported for that DEI metric) then there is a remote chance that this individual could be identified indirectly, though this would only be possible by **a)** knowing the firm's total number of lawyers; **b)** knowing how many of these lawyers qualify to be counted in the UK MDS; **c)** knowing the actual percentage, as opposed to the reported percentage which has been rounded to the nearest whole number, and **d)** using publicly available sources (e.g., the law firm's website or LinkedIn or other communications which may contain photos and other information the firm or individual has published) to try to identify the relevant individual. However, the risk of identification is lower given that the results are reported to client signatories in percentages rather than the actual numbers input into the UK MDS online platform.

To give an example, a law firm has 66 total associates. Of these 66 associates, 60 fulfil the criteria to be counted in the UK MDS. If the law firm reports that one of these associates is a gay male, it is not possible to tell directly from the information in the UK MDS dashboard that this represents only one individual or who this individual is – it is reported as 2% LGBT associates (i.e., 1 out of 60 associates, where 1.6% is rounded up to 2%). (Note that the Dashboard show 2% LGBT associates and not 2% gay male associates. When displaying this information in the Dashboards, IDF combines information on gay men, lesbian/gay women, bi men, bi women, and trans under the single heading "LGBT" to further obscure the raw data.) It may, however, be possible to indirectly identify that individual through multiple steps. First, it would be necessary to know not the total number of firm associates (66), but rather the precise total number of firm associates who qualify to be reported on in the UK MDS (in this case 60) as well as the actual percentage (1.6% and not the reported 2%) in order to translate this 1.6% back into a real number and to determine that this percentage represents one LGBT associate. (Note that even in this case the sex of the individual is unknown). *IDF will never reveal any of these raw data figures (1, 66, or 60) to any party.* Second, it would be necessary to use other publicly available information to determine who this one LGBT associate is – for example if the individual appeared in diversity videos published by the law firm or talked about experiences of being gay (or lesbian or bi or trans) in their LinkedIn profile which also mentions the firm.

Additionally, the UK MDS generally does not report on the intersection of diversity characteristics*. If the associate in the above example is a gay black male with a disability, the UK MDS does not report on the percentage of gay black male associates with disabilities. It gives one percentage for black associates, another percentage for male associates, another percentage for LGBT associates, another for disabled associates, etc. This further protects the individual's privacy.

**In the instances where the UK MDS does report on the intersection of "race/ethnicity + sex", additional steps are taken to obscure the raw data. For example, in these cases the UK MDS does not separately report the percentages of Black male associates, Black female associates, Asian male associates, and Asian female associates in the Dashboards. Rather, these are combined into a single umbrella category and shown as BAME male associates and BAME female associates.*

In the unlikely event that a firm should still have concerns about identifiability, they may always choose not to report on an individual, either by assigning them a value of "0" or by counting them under "X not disclosed to firm", as appropriate. IDF is available to Law Firm Participants in the UK MDS to discuss any areas of potential concern and help identify solutions.

Additionally, every three years IDF will use the aggregate data collected by the UK MDS to publish a written report which analyses the state of diversity, equity, inclusion, and culture in the UK legal sector. While the names of all law firms participating in the UK MDS will be listed in these research findings, all response information will be aggregated and released in a statistical or summary form. IDF will not report results in its research findings in categories small enough to allow any participating law firm or individuals to be identified either directly or indirectly.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The nature and scope of personal data collected for the UK MDS will vary depending on the make-up of the relevant law firm submitting the response.

The UK MDS asks for participating law firms to provide the names, pronouns, email address, and job title of the Firm Contact, and the name of the CEO/Managing Partner.

Law firms are asked to input the total number of UK lawyers that are working only in the UK, and the total number of lawyers globally, and then input the firm's anonymous demographic data for all UK offices as of a certain date.

The survey is split into 'equity partners', 'non-equity partners', 'counsel', 'associates', 'trainees' and 'other lawyers'. For each of the aforementioned categories, the law firm enters the number of individuals who fall into particular diversity categories e.g., "Asian/Asian British + Male", "Black/Black British + Sex Not Disclosed", "White + Female" etc, "Lesbian/Gay women", "Trans/Non-Binary", "Disabled", "Socially Mobile", etc.

NB Although IDF collects the intersection of "sex + sexual orientation/gender identity" in the UK MDS (for example "gay male" and "bi female"), this granularity of data is only collected for sector-wide research purposes where it will be aggregated with responses from all participating firms. When reporting on a single firm's data in the Dashboards accessed by Client Signatories, IDF does not show the intersection of 'sex + sexual orientation". Rather, IDF aggregates all responses with regards to sexual orientation and gender identity under the single statistic "LGBT".

The law firm is then asked to provide the demographic profile for lawyers in leadership positions, the demographic profiles of the highest and lowest earning partners, and the demographic profile of those holding the top 30 key client partnerships. *No actual financial figures are ever given in the UK MDS.*

There are three questions which may concern non-UK based individuals. To give some more detail, these are: (i) a question on the demographic profile of firm leadership; (ii) a question about the demographic profile of the top 30 key client partners; and (iii) a question on the number of multiples between the highest and lowest earning equity partner. (The question described in (iii) above does not request any actual financial figures, nor does it collect any demographic data.)

As above, special category data (racial or ethnic origin, disability information, and sexual orientation) may be processed only if the response in a particular diversity category is "1" and therefore the individual may potentially be identifiable by first determining that the percentage reported in the UK MDS represents one individual and then by combining this with publicly available information as illustrated in more detail in the example above.

Law firms will never share any names of law firm lawyers with IDF when completing the UK MDS (except the Firm Contact and the CEO/Managing Partner). They simply share number of lawyers that fall into an applicable diversity category.

The intention is that each participating law firm will submit one UK MDS response annually. The geographical area is currently restricted to the UK only.

In relation to client signatories, IDF will have email addresses of the relevant contacts in order to allow them to set up an account with unique log-in credentials (username and password) for the dashboard, in order to access the reports generated by the dashboard from the participating law firms' D&I data.

IDF and LSAC will also have access to platform usage data (e.g., technical data about interactions with the platform) which they will use only for analysis, security, troubleshooting, and system improvement purposes.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme?

The relevant data subjects are 1) the eligible staff of participating law firms and 2) client signatories that have an existing relationship with IDF. The law firms' staff will have provided their diversity information to their employer to use in an employment context and should reasonably expect that statistical diversity data will be given to clients and potential clients on request given that many clients routinely collect similar data from their law firms/legal service providers using their own supplier diversity questionnaires.

IDF will advise firms to inform their staff that the data they collect will be used for the UK MDS and to provide them with information on the relevant data controllers. This can be accomplished, for example, through an update of the firm's privacy notice. IDF will also provide information on best practice around monitoring, which should always include the option 'Prefer not to say'.

Since only anonymous numerical diversity data is input into the UK MDS, it is unlikely that individuals will be identified from the information in practice. However, even if an individual could be identified indirectly by the answer being "1" (as described in the example above), it is likely that the individual will have had control over the other information required to make this identification (for example, any diversity information they have shared on the company website, LinkedIn, or other publicly available sources). Individuals may reasonably expect that any diversity information they have on publicly available sources could be used for D&I purposes, and the risk of any harms arising from the individual being identified is lower given that the information will already be in the public domain.

The UK MDS has been adapted with kind permission from the tried and tested ABA Model Diversity Survey, originally developed and conducted by the American Bar Association ("**ABA**"), which is now in its fifth year. IDF is working with LSAC, which is the same service supplier used by the ABA, to develop the online platform (which is built on the Microsoft Dynamics 365 product which contains the platform) to work with the UK MDS.

It is not novel for law firms to provide statistical D&I information to clients or potential clients, but the UK MDS is more sophisticated than what many clients are currently asking from their law firms. As such, IDF has obtained input from the Solicitors Regulation Authority ("**SRA**"), which is the regulatory body for solicitors in England and Wales, and worked with general counsel, senior in-house lawyers, D&I experts, and law firm representatives with respect to the diversity categories and questions contained in the UK MDS.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The purposes of the processing is to provide client signatories greater transparency around diversity, inclusion, and culture in their panel law firm/legal service providers in case they wish to consider this information when making decisions about allocation of legal work and research on the state and trends around diversity in the legal profession. **More about the purpose and mission of the UK MDS is set out in the introduction to this DPIA.**

As firms and their clients track information over time, the UK MDS can serve as a benchmarking tool and can facilitate regular discussions and better collaboration between clients and their outside counsel on the topics of inclusion and culture.

There is no commercial or other purpose for the processing.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

As part of the development of the UK MDS, IDF assembled a working group of general counsel, senior in-house lawyers, D&I experts, and law firm representatives to consult on the project. IDF consulted and coordinated with the SRA to ensure its diversity and social mobility categories are the same as those the SRA requires law firms to report on as part of its own compulsory diversity collection exercise which is conducted every two years.

As part of IDF's ongoing compliance efforts, it has included a number of external teams to assist in this joint effort, including having engaged external legal counsel in the UK specialising in data protection matters and who have provided input on this DPIA.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

IDF relies on the following lawful bases for its own processing of personal data:

- Processing is necessary for IDF's and the client signatories' legitimate interests (GDPR Article 6(1)(f)) which are not outweighed by the rights and freedoms of individuals. Such legitimate interests include processing in order to: (i) operate the UK MDS and generate reports for client signatories; and (ii) ensure network information, security, and the efficient running of the dashboard.
- For special category data (to the extent processed at all), processing is necessary for reasons of substantial public interest (GDPR Article 9(2)(g)). IDF 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.

IDF has a **Privacy Policy** on the UK MDS to inform individuals about how their data will be used and their data subject rights. Any specific individual rights requests received will be considered by IDF at the time in accordance with its obligations under data protection laws.

Participating law firms will be separately responsible for determining their own lawful basis for the processing of personal data by them and sharing such data with IDF. As separate and independent controllers of the personal data being input into the UK MDS, the law firms will be responsible for informing staff that their data will be shared with IDF for the purposes of the UK MDS and explaining how individuals can exercise their rights under data protection laws. Whilst the UK MDS has been designed to only present percentage information to client signatories, to the extent that there remains a very remote risk of individuals being identifiable (e.g., if a law firm has low numbers of diverse individuals and when combined with knowledge of a firm's total number of lawyers eligible to be counted in the UK MDS as well as with other publicly available information) client signatories will also be separate independent controllers of any such personal data.

The processing directly achieves the purposes for processing and there is no alternative method for IDF to achieve this objective. Basing it off the 2021 version of the ABA's MDS, IDF has designed the UK MDS with privacy at the front of mind, ensuring that the personal data collection is minimised to the extent possible, and is proportionate to and necessary for the purposes for which it is collected.

It will be clear to client signatories that the data is accurate as of the 31st of December of the previous year, but the participating law firms will be expected to complete the survey annually so that the information remains as accurate as possible.

Data may be accessed by LSAC located in the US (Delaware) which is a data processor and is responsible for the maintenance and support of the UK MDS. IDF and LSAC have a contract in place with appropriate data processing provisions and standard contractual clauses for international data transfers.

Both IDF and LSAC have appropriate technical and organisational security measures in place to protect personal data, including only allowing access to the UK MDS to individuals on a need-to-know basis using secure log-in details.

LSAC has appropriate technical and security measures in place to protect the personal data it processes on IDF's behalf, for example access controls, encryption, physical security, and information security policies.

The UK MDS platform runs on a suite of Microsoft tools: Microsoft Dynamics 365 (SaaS), PowerBI (SaaS), and Power Platform (SaaS – where the platform sits) with security managed by Microsoft. As Saas, the physical datacentre, physical network, physical host, operation system, network control, certifications, and applications are all managed by Microsoft. Data is stored in Microsoft's US Azure East data centre.

IDF will delete the data after six years post-participation (to align with UK statutory limitation periods), and LSAC will delete the data as soon as it's no longer needed for LSAC to provide IDF with maintenance or support services.

A transfer impact assessment has been put in place.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Example	*Remote, possible, or probable*	*Minimal, significant, or severe*	*Low, medium, or high*
1. There is a remote potential risk that an individual could be identified from the information input into the UK MDS (e.g.,	*Remote*	*Minimal*	*Low*

where the law firm's response to a question is "1" individual falling into the category of "Black/Black British + Male" on the "Associates" chart, the relevant individual could potentially be identified if **a)** the total number of firm associates eligible to be counted in the UK MDS is known; and if **b)** the actual percentage (rather than the reported percentage, which is rounded to the nearest whole number) is known so that this percentage can be reverse calculated to show that it represents one individual; and if **c)** the individual's profile is public on the law firm's website or LinkedIn and identifies both the firm and position of the individual as well as the individual's relevant diversity characteristic.			
2. UK MDS data may be the subject of a data breach (including unauthorised access).	*Possible*	*Minimal*	*Low*
3. Risk that personal data is kept for longer than is necessary for the purpose collected.	*Possible*	*Minimal*	*Low*
4. Risk that the personal data is inaccurate.	*Possible*	*Minimal*	*Low*
5. Individuals submit deletion requests to IDF.	*Possible*	*Minimal*	*Low*

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Example		*Eliminated, reduced, or accepted*	*Low, medium, or high*	*Yes/no*
1.	IDF has ensured that law firms will only provide anonymised numerical information in relation to the diversity categories. IDF does not share these numbers (the 'raw data) with client signatories – only percentages rounded to the nearest whole	*Reduced*	*Medium*	*Yes*

	number – which minimises the risks of individuals be identified. No law firms will have access to other law firms' data in any form (neither actual numbers nor percentages), and strict access controls are in place to minimise the number of people from IDF and LSAC who can access the raw numerical data provided by law firms.			
2.	IDF has appropriate technical and organisational measures in place to protect data (such as strict access controls and encryption). IDF will process any data collected in line with high standards of physical and information security. IDF will ensure that no raw numerical data will be shared with client signatories or law firms. This minimises the amount of such data being collected and, in turn, reduces the potential number of individuals impacted in a potential data security incident. IDF has appropriate contracts in place with LSAC, the third-party processor and has carried out appropriate due diligence on LSAC to reduce the risk of a data processor security incident affecting this personal data. LSAC has appropriate technical and security measures in place to protect the personal data it processes on IDF's behalf, for example access controls, encryption, physical security, and information security policies. The online platform is SaaS and built on Microsoft Dynamics 365, Power Platform, and PowerBI, a Microsoft suite of tools where security is managed by Microsoft.	*Reduced*	*Low*	*Yes*
3.	IDF will have set retention periods (6 years post-participation) to ensure that personal data is not kept for longer than is necessary for the purpose collected. It will make sure that all individuals at IDF directly involved in this type of processing are aware of and adhere to these retention requirements.	*Reduced*	*Low*	*Yes*

4.	It will be clear to client signatories that the data is accurate as of 31 December of the previous year, but the participating law firms will be expected to complete the survey annually so that the information remains as accurate as possible.	*Reduced*	*Low*	*Yes*
5.	IDF will ensure that it carefully considers any deletion requests it receives and assesses whether any exceptions or exemptions apply under data protection laws on a case-by-case basis. If IDF considers that the information needs to be deleted, it will have procedures in place to remove the data which is reported to Client Signatories on the platform dashboard, or to delete the data entirely from the online platform.	*Reduced*	*Low*	*Yes*

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	**Jonathan Leonhart** Head of Operations 24 June 2021	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**Jonathan Leonhart** Head of Operations 24 June 2021	If accepting any residual high risk, consult the ICO before going ahead
Comments: For the reasons set out in detail in this DPIA, IDF does not consider that its data processing is high risk to the rights and freedoms of individuals. The UK MDS has been designed in the least privacy-intrusive way possible and IDF has appropriate technical and organisational measures in place to protect the limited personal data collected and comply with data protection laws in respect of such data.		

This DPIA will be kept under review by:	**Jonathan Leonhart** Head of Operations 30 October 2022	