EUROPEAN DATA PROTECTION BOARD CONSULTATION RESPONSE

Submission to the EDPB on its Recommendations 01/2020 on Measures to Supplement Transfer Tools

FEEDBACK PERIOD

10 NOVEMBER 2020 – 21 DECEMBER 2020

1. INTRODUCTION

1.1 We welcome the opportunity to respond to European Data Protection Board's ("**EDPB**") public consultation 01/2020 on its recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "**Recommendations**").

1.2 While this response focuses on the Recommendations (01/2020) we refer also in places to the Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (02/2020) (the "**Essential Guarantees Recommendations**").

1.3 Unless otherwise stated, references to Articles, Recitals and Chapters are to articles, recitals and chapters in the EU General Data Protection Regulation (2016/679) ("**GDPR**") and references to paragraphs are to paragraphs in the Recommendations.

1.4 Pinsent Masons LLP is an international law firm with a dedicated Informational Law, Cyber and Privacy practice including over 50 specialists internationally and has worked closely with European Data Protection Supervisory Authorities regarding data protection laws over many years. We have a range of clients across sectors and jurisdictions that regularly transfer personal data internationally. We act for Controllers, Processors and Sub-processors, ranging from multi-national corporations, national organisations to SMEs and start-ups, so bring an insight from various perspectives.

1.5 We offer the following feedback on behalf of ourselves and our clients and raise a number of questions to provoke thought which we do hope will assist as the document is finalised.

2. OUR FEEDBACK

2.1 Onward Transfers

2.1.1 Step 1 provides that when mapping transfers, onward transfers should also be considered by the original data exporter. Step 3 goes on to add that any assessment must include any onward transfers that may occur and that the "*more controller, processor or importers involved, the more complex your assessment will be*". This seems unduly onerous and impractical for original data exporters.

2.1.2 In our view, the recommendations in this context should clarify that an initial data exporter cannot be held liable for *all* onward transfers, but rather the (onward) data exporter conducting such onward transfers. The data exporter will perform its duties in completing an assessment, however it may not know the end destination of the data or indeed what safeguards are appropriate pursuant to article 46 or 47. The onward data exporter conducting the assessment will be best placed to understand how to safeguard the onward data transfer. The initial data exporter shall bind the data importer contractually using transfer tools (including any assessments required of the data importer as set out in the Recommendations), it follows that should there be an onward transfer by that data importer,

the same obligations would be flowed down resulting in a consistent approach and greater fairness in respect of liability.

2.2 **Practicality of Step 3 and a harmonized approach**

2.2.1 Almost of our clients have raised concerns as to the practicality of carrying out the assessment of third country laws required by Step 3 of the Recommendations. In particular, the assessment of the proportionality of national surveillance measures (for example) of a third country require a complex assessment of principles of EU law which go beyond solely data protection. The Recommendations in effect place a burden on exporters to conduct a fulsome and holistic review and comparative analysis of the laws, precedents and practice of relevant authorities in the third country, and of a making a quasi-judicial determination as to whether they risk, in combination, undermining the safeguards provided for in transfer tools being relied upon. They are further being asked to assess whether that determination is altered by additional safeguards they may seek to impose.

2.2.2 Such review, analysis and determination requires specialist knowledge and multi-jurisdictional advice. Notwithstanding the EDPB's high-level guidance in the form of its Essential Guarantees Recommendations. For organisations of any size – but particularly for small and medium size businesses, the practicalities and costs of this have not been accounted for, which is at odds with Recital 13 which specifically states that " *In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation*".

2.2.3 Clients are confused as to the extent to which they are entitled to rely on assessments carried out by the importers and – in turn - importers, quite rightly, state that they cannot opine on the proportionality of local law measures by reference to principles of EU public law. There is also no clarity as to where the line is drawn in respect of responsibility as to the assessments, simply that the exporter is ultimately accountable.

2.2.4 Greater clarity is needed on the nature of local "practices" that exporters can (or indeed should) take into account, and the extent, that may potentially impact on their analysis. It would seem that organisational or procedural steps outside of the 'letter of the law', as well as the known or generally accepted view of the practical application of the law in the context of transfers of personal data from the EU should be given some weight.

2.2.5 For smaller businesses with little bargaining power, this lack of certainty could lead to unreasonable or prohibitively unworkable costs (including legal negotiation), and ultimately stifle business development in the EU and international business. Equally, international businesses based in a third country may need to cease offering their services in the EU, because of the costs involved in creating a structure in Europe that complies with the Recommendations.

2.2.6 The inefficiency and variance in results and, range in potential additional safeguards that exporters will seek to include in transfer tools, that will occur by virtue of countless different exporters carrying out assessments of the law and practices in third countries seems counterproductive. Rather than meeting the goal of ensuring that essential equivalence of EU data protection laws accompanies exported personal data, imposing the burden on exporters of making those assessments and the need and nature of additional safeguards is likely to something that may result in very different outcomes for data subjects depending on the data exporter and circumstances of the transfer in question. There is a material risk of inconsistency, confusion and a lack of certainty of compliance for data subjects and exporters alike.

2.2.7 It seems to us that this approach is only remotely practicable if the EDPB or similar body were to produce an analysis of third countries where the national surveillance or other relevant laws and practices cause a high risk to data subjects - effectively carrying out part of the review required by Step 3 of the process in the Recommendations. Facilitating a consistent appraisal would promote a harmonized approach, in the spirit of the GDPR.

2.3 **Risk based approach/Nature of the data**

2.3.1 One of the biggest concerns raised by clients as to the Recommendations is that they do not permit the analysis of the data in question so as to inform risk based judgments. Furthermore, they state that exporters must not "*rely on subjective factors such as the likelihood of public authorities' access to your data*".

2.3.2 Similarly, paragraph 17 of the Essential Guarantees Recommendations – quoting from the Schrems II judgment - states that "In order to find an interference [with fundamental rights] it does not matter *'whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference'*".

2.3.3 These statements seem to rule out sensible risk assessments on the basis of the nature of the data. For example, internal employee phone book information or HR appraisal files shared and accessible to employees of affiliated entities in a third country or similarly low level data could be restricted if the law in the third country allows a *theoretical* access to such data by third country public authorities.

2.3.4 This is reinforced by the Use Cases 6 and 7 in which the EDPB state that it cannot envisage a permissible scenario for unencrypted data to be processed in a third country in circumstances where there *may be the potential* for that data to be accessed by a public authority in a way that is excessive. This suggests that no contractual and organisational measures could be sufficient even where the likelihood of access by a public authority is remote or the data is of limited sensitivity. This seems to run contrary to the nature of the GDPR which in many areas relies on an assessment of the *nature* of the data to assess risk and engagement of particular provisions. We note the GDPR provisions relating to the appropriateness of security measures (Article 32), the obligation to notify a data breach (Articles 33 and 34) as well as the requirement to carry out DPIAs (Article 35) amongst other provisions, all of which require an analysis of the *nature* of the personal data in question in assessing the extent to which the relevant provisions are engaged.

2.3.5 It also seems to rule out sensible risk assessment of factors, such as reported precedents, legislation and practice, which may point to a low likelihood of access (or the exercise of access rights) by relevant authorities to data. It would seem unusual that exporters should not be able to consider a subjective application of such elements to their transfers.

2.3.6 We note also that adopting and allowing a risk based approach based on the nature of the data involved would mirror the European Commissions new draft SCC's, which include in their warranties that that the parties shall take account of "the *specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing;* ***the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred****."* [our bold][1]

2.4 **Transit**

2.4.1 Use case 3 of the Recommendations gives an example including data that may be "*geographically routed through a third country not providing an essentially equivalent level of protection*". This implies that a mere 'transit' may qualify as a 'transfer' for the purposes of Chapter V of the GDPR, thus creating onerous obligations which fall outside the intention and scope of the GDPR. Moreover, this suggests that when the data is in transit, the exporter must require encryption in all cases, even where it may be possible to adduce appropriate safeguards which protect that data. The recommendations should reiterate that mere transit does not constitute transfer for the purposes of the GDPR and to the extent the method of transfer is regulated by the GDPR, it is as a security mechanism for the

[1] 1 Clause 2(b)(i) of the draft new Standard Contractual Clauses issued by the European Commission 12/11/2020

purposes of Article 32 and that there is no requirement to carry out third country assessments in respect of jurisdictions through which personal data may route while 'in transit'.

2.5 **Practicality of Technical Measures**

2.5.1 We and our clients have concerns as to how realistic the encryption safeguards described in Use Cases 1 and 3 are. In particular, the requirement that encryption be "flawlessly managed" and keys retained under the sole control of the data exporter (or a provider in an adequate jurisdiction) is a high (and expensive) bar and does not take into account any other contractual, organisational or technical measures which may mitigate risk (including, also – per 2.3 point above - the sensitivity or otherwise of the data or likelihood of authority access).

2.5.2 There also appears to be an over heavy weighting in the examples towards encryption and technological solutions as the primary means of implementing additional safeguards. The examples given would likely require a considerable review of information security, cyber risk and governance structures for businesses trading in the EU, and seeking to establish and maintain the infrastructure required to support this, again creates the risk of an unreasonably high financial burden on business. Further, the prescriptive nature of such security safeguards do not account for technical developments which may ultimately hamper data transfers despite alternative more appropriate security measures.

We hope this is helpful. If you have any queries in respect of this response, please do not hesitate to contact Andreas Carney – a partner in our Dublin office - on Andreas.Carney@pinsentmasons.com or Jonathan Kirsop – in our London office - on Jonathan.Kirsop@pinsentmasons.com.

Pinsent Masons LLP
21 December 2020