21 December 2020

City of London Law Society Data Law Committee

Submission to the EDPB on its Recommendations on

Measures to Supplement Transfer Tools

The City of London Law Society ("**CLLS**") represents approximately 17,000 London City lawyers through individual and corporate membership including some of the largest international law firms in the world. These law firms advise a variety of clients from multinational companies and financial institutions to government departments (UK and otherwise), often in relation to complex, multijurisdictional legal issues. The CLLS responds to a variety of consultations on issues of importance to its members through its' 19 specialist committees.

This letter has been prepared by the CLLS Data Law Committee (the "**Committee**").

We welcome the opportunity to respond to the European Data Protection Board's ("**EDPB**") public consultation on its recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "**Recommendations**"). This submission is not confidential and we have no objection to it being published on the EDPB's website.

Unless otherwise stated, references to Articles, Recitals and Chapters are to articles, recitals and chapters in the GDPR and references to paragraphs are to paragraphs in the Recommendations.

1. BURDEN OF THE RECOMMENDATIONS

1.1 We welcome the level of consideration which has gone into the Recommendations, however we are concerned that the potential burden on entities, in relation to some of the elements of the Recommendations, is substantial.

1.2 To some extent, this will depend on the nature of the entity:

Large Entities

1.2.1 For large global entities operating across multiple jurisdictions, Step 1 of the Recommendations (paragraphs 8-13) imposes an onerous degree of investigation, most particularly with regard to onward processing (paragraph 10). Such large entities can and do have highly outsourced service provision involving personal data, with such processors utilising various sub-processors themselves, and so on. Creating a map of destinations (paragraph 12) for all personal data, regardless of risk profile, creates an administratively burdensome process for such entities. Indeed the suggestion at paragraph 9 that organisations 'build on' their GDPR requirement to have in place records of processing activities would appear to go beyond the requirements of the GDPR (i.e. the legal requirement is

to have a record of such activities and not a higher, built on, compliance level), nor is it clear practically what further mapping is expected by the EDPB.

1.2.2 Furthermore, given processors can be changed quickly depending on a range of factors (e.g. improved service offering from an alternative, more secure data storage, operational factors, changes in the law), the obligation at paragraph 12 to undertake such activities prior to a transfer could arguably be read as requiring that, in the event of a sub-processor / sub-sub-processor etc. change, that data transfer should be suspended until verification could be undertaken. Such an obligation will have material, negative consequences for conducting effective business.

SMEs

1.2.3 For smaller or medium-sized enterprises ("**SMEs**"), Step 1 will not likely be as burdensome, although with the caveat that where major technology vendors are utilised, the expectation on SMEs to be able to verify the onward transfers to such vendors' sub-processors and beyond, in compliance with the Recommendations, is a time and cost-intensive task which may be prohibitive to many SMEs.

1.2.4 Additionally, the expectation on SMEs in relation to the supplementary measures may well be impossible to fulfil given the potential cost implications, regardless of the risk profile of the personal data involved. For example Use Case 3, regarding data transiting through a third country, expects that 'state-of-the-art' encryption and measures to prevent active and passive attacks which can be considered 'robust' against public authority cryptanalysis are utilised, which is itself 'flawlessly implemented' and all backdoors are ruled out. This is a very high bar for all entities, but particularly SMEs, and in the context of onward transfers.

1.2.5 Furthermore, many of the ongoing requirements on entities highlighted throughout the Recommendations (e.g. the requirement to publish regular transparency reports (paragraph 129)) will be particularly burdensome on SMEs.

1.2.6 It is also not clear how some obligations in the Recommendations will impact SMEs. For example, the requirement to maintain records of processing activities does not apply to entities with fewer than 250 employees (Article 30(5)), however the Recommendations comment that entities 'build on' this (discussed at section 1.2.1 of this response) does not address this nuance for SMEs.

1.3 While it is understood that the Recommendations are a set of logical considerations in light of the Schrems II judgment from an academic point of view, we are of the view that such

considerations should be grounded in practical applicability in relation to the particular personal data transfer, *including* the risk profile of the data transfer.

1.4 The 'one size fits all' nature of the obligations (rather than them being guidance for the interpretation of the GDPR) does not achieve a proportionate set of considerations for entities and we would suggest, as currently drafted, the Recommendations impose a set of obligations which are overly onerous and inflexible.

2. DIVERGENCE OF VIEWS ON ADEQUACY

2.1 The GDPR was introduced as a Regulation rather than a Directive with the intention of harmonising, across the EU, the position regarding the protection of personal data. However Step 3 of the Recommendations (paragraphs 28-44) would suggest that a high degree of divergence in analysis, and thus practice, will ensue.

2.2 This is particularly the case regarding the analysis of law or practice in a third country (paragraph 30). This can manifest itself in multiple ways, for example:

2.2.1 two independent exporters having different perspectives and considerations regarding a similar data set being transferred to the same importer in a jurisdiction;

2.2.2 different importers in the same jurisdiction having knowledge of, or access to, differing sources of information regarding the law and practice in that jurisdiction;

2.2.3 where there are settled sources of publically available information regarding the law and practice in a jurisdiction, different exporters and importers may analyse these sources differently, even with regard to similar data sets; or

2.2.4 where there are not settled sources of information regarding law and practice in a jurisdiction, for example where national security laws and/or practices are not published or made public, then different exporters and importers may make different assumptions regarding such circumstances.

Each of the example scenarios raises the real prospect of huge variance between different analyses, creating confusion regarding whether, in relation to the particular transfer of personal data, the recipient jurisdiction does provide sufficient equivalent protection and indeed what supplementary measures may or may not be required.

2.3 Such divergence will also create less clarity for data subjects who, should they request further information regarding the nature of a particular international data transfer, may be given different views in relation to similar circumstances, a result that is at odds with the original intention of the GDPR.

2.4 We would also note that the analysis being asked of private entities here is one which is very similar to that which competent bodies have been required to undertaken pursuant to the consideration of Article 45 adequacy decisions and which, to date, has only resulted in twelve extant decisions. Given the dedicated resourcing and substantial time afforded to competent bodies to undertake such analyses and determinations, placing such an obligation on private entities (and in particular SMEs) who have far fewer dedicated resources and for whom a data transfer may be marginal and ancillary to the business they undertake, is neither proportionate nor satisfactory for the entities involved or the data subjects, who would expect a settled, informed, and substantiated perspective from a competent body regarding the adequacy or otherwise of a recipient country's laws and practices. As such, we would request that the EDPB confirms whether reports produced by third parties on the condition of a jurisdiction's data protection practice (either commissioned by the data exporter or otherwise freely available) would satisfy the data exporter's diligence obligations, particularly given that this may be a suitable position for SMEs who would not necessarily otherwise have the resources to conduct such an analysis.

2.5 Furthermore, there appears to be no consideration of the fact that many countries have data protection laws similar to the GDPR, with perhaps the most pertinent example being a post-Brexit UK whose law would be the UK-implemented version of the GDPR. However the Recommendations do not refer to countries with similar legal positions as the EU in any way impacting the assessment of a recipient jurisdiction's national security laws. We would suggest that such consideration should be incorporated.

2.6 As already noted, introducing an element of risk consideration to the analysis being undertaken would be appropriate in that it would allow entities to make their recipient country adequacy considerations in the context of the risk to the particular personal data involved and the other circumstances of the transfer. This would be a practical and flexible solution rather than the position put forward in the Recommendations which can be viewed as something of a 'blunt instrument'.

3. SUPPLEMENTARY MEASURES

3.1 Where an analysis of the recipient jurisdiction's law and practice indicates that it does not provide sufficient equivalence, nor meet the EDPB's Recommendations on the European Essential Guarantees for surveillance measures framework ("**EEGs**"), then either: (i) the personal data should not be transferred; or (ii) supplemental measures should be put in place (paragraph 44).

3.2 In such a scenario, our understanding of the supplementary measures which are detailed at paragraphs 69-137 is that the only effective supplementary measure to facilitate an international transfer is to encrypt, pseudonymise, or otherwise render the data to be non-personal in nature so that the relevant personal data cannot be read by the importer. This is on the basis that the commentary in the Recommendations regarding: (i) contractual supplementary measures suggests that they 'should be combined with other technical and organisational measures' as contractual measures cannot bind a third party authority in the recipient country (paragraph 93); (ii) organisational measures suggests that they are 'needed to complement contractual and/or technical measures' and only contribute to ensuring internal consistency of processing and importer entities' risk awareness (paragraph 122); and (iii) technical measures states that they will be 'especially needed' where the law of a recipient jurisdiction would impinge on the contractual protections.

3.3 On this basis, the proposed technical protections would seem to essentially amount to there being no scenario where an importer in a recipient jurisdiction which is assessed as not providing an adequate level of protection could receive personal data which can be processed there, regardless of the nature of the personal data involved. Is this the EDPB's intention?

4. **USE CASES**

4.1 The Recommendations provide two use cases where no effective measures can be found from a technical perspective: (i) transfers to cloud service providers (paragraphs 88-89); and (ii) remote access to data for a business purposes (paragraphs 90-91).

4.2 Such scenarios are likely to be very commonplace, for example: in the former particularly for SMEs using global cloud-based platforms to undertake functions which are resource-prohibitive to support in-house; and in the latter for larger entities who are headquartered in one jurisdiction and have global operations across jurisdictions.

4.3 Given this, and in light of the comments at section 3.2 above regarding contractual and organisational measures being insufficient in themselves, the Recommendations appear to suggest that there is no available compliant process to facilitate an international data transfer in these Use Cases (i.e. they would appear impossible).

4.4 Is this the conclusion reached by the EDPB and, if so, given the substantial practical implications on business, are there any supplementary measures which the EDPB would consider sufficient in such scenarios?

4.5 Given the commonplace nature of these scenarios, we would suggest that the Recommendations provide for an alternative action organisations can take, for example applying to the competent supervisory authority to assess the transfer.

5. DATA LOCALISATION

5.1 For entities who are not able to meet the substantial obligations (as noted at section 1 above), the only alternative in order to continue operating (on the basis that the personal data collected and processed is that which is necessary and cannot be minimised to none) will likely need to localise data processing activities in the EU.

5.2 Such a decision may be impossible in relation to some activities if, for example, the services required are not performed by an EU-based entity, or otherwise could incur material cost expenditure as well as cause operational disruption.

5.3 The Recommendations may therefore be read as implementing a broader data localisation agenda by having such onerous expectations in place. We would note that this is not the intention of the GDPR and threatens to 'Balkanise' global data flows.

6. BINDING CORPORATE RULES

6.1 The Recommendations note that Schrems II also applies to binding corporate rules ("**BCRs**") and that the impact of Schrems II on BCRs is 'still under discussion' (paragraphs 58-60). Given we would anticipate further guidance being received on this in due course, there are some areas where it would be particularly useful to get clarity.

6.2 For organisations who have had their BCRs approved, will there be an expectation or requirement on them to perform a transfer impact assessment ("**TIA**") and then re-submit their BCRs for approval? If this is the case, then we would suggest that this is disproportionate and that a more moderate approach would be for the existing BCRs to remain valid and for organisations with BCRs to perform such TIAs as necessary and submit them to their lead supervisory authority, who can then approve or deny them.

6.3 Where future BCR applications are made by an organisation, inclusion of TIAs in this process will exacerbate the already length process. This is particularly so given that organisations who use BCRs generally have a large global footprint and, as a TIA will include an assessment of the laws of every importing third country, will be onerous both for the organisation to compile, as well as for the lead supervisory authority to assess.

7. ENFORCEMENT

7.1 Given the substantial expectations placed on entities by the Recommendations, and in particular the specific case-by-case analysis required in respect of every personal data

transfer, this would seem to place an extraordinary burden on regulators in order to enforce this position.

7.2 Our understanding is that a regulator would need to: (i) be appraised of the specifics of the data transfer (i.e. particular exporter, importer(s), data set(s), format of data, jurisdiction(s) etc.); (ii) undertake an assessment of the law and practice in the recipient jurisdiction on the basis (presumably) of the same information which the exporter had available in the context of the information at (i); (iii) consider the Article 46 transfer tool which was relied on and any supplementary measures; and (iv) determine whether, against the EEGs, the transfer was compliant.

7.3 This is a significant amount of work for a single data transfer, let alone the myriad transfers undertaken by entities on a daily basis. It is unclear that such an expectation on regulators in respect of international transfers of personal data is proportionate in relation to other elements of the GDPR over which they must also regulate and which, arguably, can be seen as posing a higher risk to data subjects.

7.4 Indeed, the logical conclusion given the substantial work required involving a single international data transfer must be that regulators will take a risk-based view in relation to which international data transfers they will audit and potentially take action regarding. If this is the case, then it seems appropriate to include an element of risk-based consideration for exporter entities.

8. ALIGNMENT WITH STANDARD CONTRACTUAL CLAUSES

8.1 Further to the conclusion reached at section 7.4 of this response and the discussion of the divergence of views regarding adequacy at section 2, we would suggest that the EDPB ensures alignment between the Recommendations and the draft new Standard Contractual Clauses which are currently the subject of consultation ("**Draft SCCs**") particularly in respect of the assessment of whether a transfer tool is effective in light of the transfer.

8.2 Paragraph 42 of the Recommendations suggests that an objective approach should be pursued (i.e. *can* national authorities access personal data?): "*you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards*". This is contrary to the approach in the Draft SCCs where clause 2(b)(i) advocates a subjective approach (i.e. *have* national authorities accessed personal data?): *"The Parties declare… they have taken due account in particular of the following elements:… 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".*

8.3 In this example, while the Recommendations suggest that an organisation should not consider practical experience with public authority access requests, the Draft SCCs suggest that an organisation should. We would suggest that the Recommendations and Draft SCCs are aligned in final form and that consideration of practical experience is an appropriate and proportionate consideration to include.

9. CONCLUDING COMMENTS

9.1 In light of the comments at sections 1 to 8 of this response, we are of the view that a degree of risk-based consideration should be integrated within the Recommendations.

9.2 Given that the Recommendations already place a large degree of independence on entities to assess the law and practice of a recipient jurisdiction, it would seem both proportionate and appropriate to enable entities to consider the actual and potential risk in relation to the various factors noted.

9.3 For example, while the Schrems II case provided detailed and reasoned conclusions regarding the transfer of personal data to the USA, in a White Paper released in response to the decision, the US Department of Commerce highlighted a range of factors not considered in the Schrems II case, including that the vast majority of personal data is of no interest to, and most likely outside the scope of, the USA's security laws.[1]

9.4 Such commentary and analysis is integral to informing the considerations of a particular transfer of personal data as, if the data will not be sought by a public body, the potential harm to the individual is limited.

9.5 Given that the intention of the GDPR is to reduce the harm, both potential and real, to data subjects in respect of their personal data, a full consideration of the personal data in question should be undertaken, and this should therefore include risk-based consideration.

9.6 Including within the Recommendations a degree of risk-based consideration will enable entities of all sizes to be able to adopt appropriate and proportionate supplementary measures where necessary which will enable a more flexible, practical, and coherent approach to the international transfer of personal data.

9.7 Finally, given the substantial obligations envisioned by the Recommendations (and in particular the analysis of recipient jurisdictions' data protection position), we would suggest that the absence of a transition period is impractical. Organisations will need time to consider the final form Recommendations and ensure necessary compliance with, and

[1] Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*, White Paper September 2020, https://www.commerce.gov/sites/default/files/2020- 09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

implementation of, them. Indeed, a transition period would also align with the position proposed for the Draft SCCs. As such we would suggest that a transition period is incorporated into the final form Recommendations.