DLA PIPER COMMENTS ON EDPB RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA (PUBLIC CONSULTATION REFERENCE R01/2020) – 21 DECEMBER 2020

About DLA Piper: DLA Piper is a leading global law firm with more than 180 data protection and privacy lawyers across our global offices in more than 40 countries. Our lawyers have advised more than 500 organisations on the interpretation and practical application of GDPR.

The *Schrems* II ruling of the CJEU has created significant legal uncertainty for multinationals subject to the GDPR and for their international group companies and suppliers. We are grateful to the EDPB for seeking to address this uncertainty by publishing the draft recommendations 01/2020. We also welcome the opportunity to comment and have set out our comments below.

1. Overly restrictive approach to supplementary measures

We welcome the recognition in the draft recommendations that supplementary measures may be contractual, technical and organizational in nature. We believe these are indeed appropriate categories of supplementary measures. We also welcome the suggestions and examples given in annex 2.

We do, however, have the following comments in this respect.

1. We would suggest to also consider recognizing any self-regulatory or voluntary schemes providing additional protections such as sector-specific codes of conduct or other schemes.

2. While the draft recommendations recognize the abovementioned three categories of supplementary measures, for the use cases which are most relevant for businesses, they consider that *only* technical measures – and moreover, extremely strict technical measures – are appropriate.

   This approach is overly and disproportionately prescriptive; it should be left to exporters to identify the appropriate supplementary measures in view of the nature of the transfer (see section 2 with regard to the legal requirement for a risk-based approach). Exporters should have the possibility to assess the supplementary measures in a more comprehensive, holistic way without being constrained to the technical measures dictated in the draft recommendations, particularly where the legal basis for the proposed highly prescriptive approach is at the very least open to interpretation.

   A risk based approach is in our opinion entirely consistent with the CJEU decision that acknowledges an assessment on a case-by-case basis (§ 134) and with GDPR.

3. While we welcome the fact that the draft recommendations provide for certain use cases to improve understanding of how the draft recommendations will apply in practice, these use cases (and in particular use cases 6 and 7) are unrealistic and disproportionate, particularly when coupled with the proposal that all personal data *however innocuous* should enjoy the full protection and associated costs contemplated in the draft recommendations. Taking an extreme example falling within use case 6, transferring contact details in the clear of sales representatives which are accessible globally on public websites hosted on servers in the EU to servers hosted by a processor in the US to improve technical performance of the website is according to use case 6 "*incapable of … an effective technical measure to prevent … access [by public authorities] from infringing on data subject rights*". This is notwithstanding that the data is freely available online to intelligence services via the EU hosted website and given its innocuous nature likely of no interest to them whatsoever. Effectively prohibiting such transfers would also cause significant detriment (financial and mental distress) to the sales personnel who are unable to share their contact details in the US.

4. For multinational companies it is not realistic nor feasible to avoid access to personal data in the clear from third countries. Many multinational companies with global reach often have strongly integrated businesses using common tools for HR, sales & marketing, finance, etc. which inevitably require an exchange of data across the globe and access to personal data in the clear. Furthermore, the draft recommendations do not address the practical and technical realities that usually at least some meta data needs to be unencrypted in order to provide an online service (for example connection information, session state, IP addresses, and basic subscriber data).

5. Save in very limited edge cases personal data transferred from the EU to third countries is unlikely to be of any interest to public authorities. Outlawing these transfers – which in effect is what use cases 6 and 7 seek to do – conflicts with a core underlying principle in GDPR and European jurisprudence that the interpretation and application of legal requirements should be proportionate. The use cases therefore have a questionable legal basis and in our view are not required either by *Schrems II* or by GDPR. They go further than the legal standard of care and will likely cause very significant cost and harm to the many businesses impacted by the draft recommendations, disproportionality impacting the Charter rights and freedoms of those businesses (see section 6 below).

2. Lack of risk-based approach

We respectfully request the EDPB to accept that subjective factors such as the likelihood of risk of harm to the data subject (which is directly linked to the likelihood of access to the personal data by a foreign surveillance authority) can be taken into account by exporters when assessing their transfers.

We believe this is clearly supported by the CJEU decision which acknowledges a case-by-case assessment (see section 1 above) and also consistent with the GDPR which *explicitly requires* a risk-based approach to data protection. Indeed, the protections offered by the GDPR to data subjects are not absolute but subject to a risk assessment and proportionality. In this respect we refer to:

- Article 24 which obliges controllers to implement **appropriate** technical and organisational measures "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons".

  The term "appropriate" inherently includes a proportionality and risk-based assessment.

- Article 25.1 which allows controllers to take into account the "risks of varying likelihood and severity for rights and freedoms of natural persons" when implementing by means of technical and organisational measures the privacy by design principle.

- Article 32 which provides for "appropriate technical and organisational measures [to be implemented] to ensure a level of security appropriate to the risk [of harm]".

- Article 34 which provides that personal data breaches shall only be communicated to the data subject if it is likely to result in a high risk to its rights and freedoms.

- Article 35 which provides for a data protection impact assessment in case a type of processing is likely to result in in a high risk to the rights and freedoms of natural persons.

There is no reason why the risk-based approach would not apply to Chapter V and by seeking to remove the right for exporters to take a risk-based approach to transfer impact assessments, the draft recommendations set a *higher* standard for personal data exported to third countries than for data hosted within the EU. Not only is this approach impractical and disproportionate; it is also based on a questionable legal interpretation which is at odds with the explicit legally binding articles of the GDPR.

It follows that as proportionality is at the core of the application of GDPR requirements, supplementary measures should be tailored to take into consideration whether surveillance authorities in the importing country are likely to be interested in the transferred data, including evidence whether they have previously made access requests to the data within scope of each transfer assessment. The very large majority of personal data transferred to third countries are likely not to be of any interest to public authorities. If there is strong evidence that the data is innocuous in nature (such as sales rep contact details) and unlikely to be of interest to intelligence services, then the bar for appropriate supplementary measures should be set much lower.

Also, adopting a risk-based approach will allow companies to focus their limited resources on their important, potentially (high)er risk transfers which is clearly in the best interests of data subjects. It is not realistic nor feasible for companies, in particular in terms of volume of work and required resources, to assess all their data transfers with the same level of detail and forcing them to do so will inevitably lead to a tick-box approach to compliance which has proven to be a very ineffective approach to risk management.

3. Overly narrow interpretation article 49 derogations

We also respectfully request the EDPB to reconsider the narrow proposed interpretation of the derogations in article 49 to occasional and non-repetitive transfers. We consider that this interpretation not only conflicts with the explicit language of article 49 but also conflicts with the ruling of the CJEU itself. Furthermore the narrow interpretation is unnecessary given the "necessary" protection built into the derogations in article 49 will protect the rights and freedoms of data subjects.

Interpretation conflicts with article 49

The only derogation which is limited in its application to occasional and non-repetitive transfers is the derogation set out in the hanging paragraph of article 49(1) – ad hoc transfers based on compelling legitimate interests. None of the other derogations in article 49 are subject to this limitation. If the legislature had intended the limitations in the hanging paragraph to article 49(1) to have applied to *all* of the derogations then it would have been straightforward to change the drafting. They did not and as such none of the other derogations should be interpreted only to apply to occasional and non-repetitive transfers. There are several recitals in GDPR which may support a narrower interpretation. However, it is a well-established principle of law that when interpreting EU regulations the recitals to a regulation are not legally binding and in the event of a conflict between the recitals and the clear and explicit legally binding articles, the articles shall prevail. There is therefore no legal basis to limit the application of the article 49 derogations to "occasional and non-repetitive" transfers. Doing so also disproportionately impinges on the Charter rights and freedoms of the many businesses exporting personal data from the EU to third countries.

Interpretation conflicts with the CJEU ruling in Schrems II

When considering whether it was appropriate to maintain the Privacy Shield Decision for the purposes of avoiding the creation of a legal vacuum, the CJEU concluded in its ruling that "*in view of article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum.*" (§ 202). The proposed narrow interpretation of article 49 in the draft recommendations is therefore not only at odds with the explicit language of the legally binding article 49, but also with the judgment of the CJEU itself. By interpreting article 49 *only* to apply to occasional and non-repetitive transfers, the draft recommendations if finalised in their current form will undoubtably create a legal vacuum for the large majority of perfectly innocuous data transfers.

A narrow interpretation of article 49 is unnecessary to protect the rights and freedoms of data subjects

There is also no need for such a restrictive interpretation of article 49 as each derogation (with the exception of the explicit consent of the data subject which sets the highest standard of protection) is

qualified such that the transfer must be *necessary*. When assessing whether a transfer is necessary exporters will be required to carry out a proportionality assessment *inter alia* taking into consideration the risk to the rights and freedoms of the impacted data subjects having regard to the nature of the personal data, the supplemental controls in place and how likely it is that public authorities will actually access the personal data.

The combination of a strict approach with regard to both supplementary measures and article 49 derogations leads to a *de facto* data localization requirement which is simply not supported by the GDPR or by the *Schrems II* ruling.

It is clear from both a literal and purposive interpretation of article 49 and by the CJEU's reliance on article 49 to conclude that no legal vacuum has been created by the invalidation of Privacy Shield that the law permits these derogations to be used in situations where no appropriate safeguards under article 46 are available, *including* for regular and systemic transfers. Exporters should be able to rely on those derogations under the conditions provided for by article 49 and no additional conservative interpretative restrictions should apply.

4. Difficulties in applying the EEG standard with regard to surveillance measures

Data exporters are recommended to assess the surveillance laws of the importing countries using the European Essential Guarantees standard.

Although we welcome guidance on how to assess the surveillance laws of third countries, we do have the following comments in this respect:

1. We believe that for most companies it will be unrealistic to perform these complex assessments because they lack resources (manpower, budget and specialist skills) and/or because they run a global business whereby data is transferred all over the world. We note that even with its very considerable resources and expertise, the Commission often takes years to carry out assessments leading to an adequacy decision. It is simply not practical to expect exporters to be able to carry out these reviews themselves without much more detailed guidance.

2. Each exporter is required to make its own assessment of the surveillance laws in third countries and whether or not they afford equivalent protection. As the Commission has demonstrated, adequacy assessments are far from an exact science and it is therefore inevitable that inconsistent assessments will be commonplace, increasing legal uncertainty and diminishing the protections afforded to data subjects. The same risk exists for assessments made by supervisory authorities of data transfers following a complaint or a notification of a transfer by a company. We would be grateful if the EDPB could clarify how it intends to ensure a consist approach to these complex assessments.

5. Absence of grace period

The draft recommendations do not provide for a grace period.

It is unrealistic and impractical to expect organisations to be able to carry out complex transfer mapping and transfer impact assessments overnight and to have alternative options readily available.

As such we urge the EDPB to introduce an enforcement grace period of at least 1 year from the date the recommendations are finalised.

6. Tension with other fundamental freedoms guaranteed by the Charter

The right to data protection is not absolute. This is expressly recognized in the recitals to the GDPR where it is stated that the right to data protection must be considered in relation to its function in society

and be balanced against other fundamental rights and freedoms, in accordance with the principle of proportionality. Furthermore, the recitals state that "the processing of personal data should be designed to serve mankind".

We believe that the conservative approach proposed in the draft recommendations disproportionately impinges on both the freedom to conduct business and the right to property by (i) limiting companies' ability to fully benefit from the globalization and digitalization (which inevitably entails international transfers of personal data) and to rely on non-EEA service providers, and (ii) by pushing companies towards substantial and costly investments to restructure their IT set up where the current set up would not meet the high threshold set by the draft recommendations. The draft recommendations, if adopted as such, create a real obstacle to the development of EU businesses around the world.

7. Clarification requested on impact of Schrems II on BCRs

We are grateful that the EDPB is considering whether any additional commitments may need to be included in BCRs as a result of the ruling. It would be helpful for the many organisations relying on BCRs if this guidance could be issued promptly given the significant legal uncertainty created by the ruling.

***